10.6326/NDJ.202403_39(1).0001

我國關鍵資訊基礎設施平戰防護之運用

A Study on the Utilization of ROC Critical Information Infrastructure Protection in Peace and Wartime

董慧明 (Hui-Ming Tung)

國防大學中共軍事事務研究所副教授

摘　　要

全民防衛動員準備的目的，在於透過動員程序，充分運用各種資源，強化平時整體防禦能力，並能支援軍事行動與應對緊急情況。另關鍵資訊基礎設施是指對國家安全、民生、經濟具重要性的資訊系統，其安全與可靠性攸關國家穩定。因應當前複雜多變的安全環境，臺灣必須建立跨部門聯防機制，以確保關鍵基礎設施的防護，並且在行政動員和軍事動員準備兩個子系統中，能夠有效地轉換與運用。

本文關注我國關鍵資訊基礎設施在平時與戰時間的靈活轉換議題，透過對中央政府部門、國軍、民間單位的法規制定與實務運作觀察，提出以下建議。第一，政府應提升通信網路的數位韌性，增進中央指揮體系的訊息傳遞效能，維持必要的國際聯繫，並確保能夠向公眾傳遞訊息。第二，國軍在動員準備業務方面，應著重資訊科技人才動員，提升資訊戰力，並促進與民間單位的合作。第三，民間單位亦應提升設施的防護力和轉換能力。透過完善的法規、政策與協調機制，以及技術和資源的投入，確保關鍵資訊基礎設施在平時與戰時得以順利轉換運用。

關鍵詞：國土安全、關鍵資訊基礎設施、全民防衛動員準備法、數位韌性、社會韌性

Abstract

Comprehensive national defense mobilization preparation aims to strengthen overall defense capabilities during peacetime through mobilization procedures, optimizing the utilization of diverse resources. This implementation will ensure robust support for military operations and effective response to emergencies. Critical information infrastructure refers to information systems crucial to national security, public welfare, and the economy, with their security and reliability directly impacting national stability.

Taiwan must establish inter-departmental joint defense mechanisms to safeguard critical infrastructure in response to the complex and dynamic security environment, The study focuses on the flexible conversion of national critical information infrastructure between peacetime and

wartime scenarios. The following recommendations are proposed through critical observations of regulatory frameworks and operational practices within the administration Government, R.O.C. Armed Forces, and civilian sectors.

First, the government should enhance the digital resilience of communication networks, improving the efficiency of information dissemination within the government command structure. This decision ensures the maintenance of essential international connections and the ability to convey information to the public.

Second, in mobilization preparation, the military should emphasize the mobilization of information technology talent, enhancing information warfare capabilities, and fostering collaboration with the private sector.

Third, the private sector should also enhance their facilities' protective capabilities and conversion capacities.

Through refined regulations, policies, coordination mechanisms, and investments in technology and resources, ensuring the smooth transition and utilization of critical information infrastructure during both peacetime and wartime can be achieved.

Keywords: Homeland Security, Critical Information Infrastructure, All-out Defense Mobilization Readiness Act, Digital Resilience, Social Resilience

壹、前　　言

關鍵資訊基礎設施(Critical Information Infrastructure, CII) [1] 被視為現代國家發展體系的神經中樞，確保其穩定運作不僅攸關國家經濟和社會繁榮，亦與全民國防、國土安全有著密切關聯。[2] 在資訊及網路應用服務無所不至的年代，包含大數據(Big Data)、雲端運算(Cloud Computing)、物聯網(Internet of Things, IoT)以及人工智慧(Artificial Intelligence, AI)等數位技術因已嵌融於人們日常的生活、工作，由此衍生與國家金融、能源、交通、衛生等各領域之關鍵基礎設施(Critical Infrastructures, CI)安全防護、運用議題也變得至關重要。這些設施一旦失效、失能或遭到破壞，勢必直接衝擊國家的整體安全。反之，當政府必須及時因應天然災害或緊急事件，亦須建立一套可行、有效之平戰時轉換機制。從「全民防衛動員準備」角度而論，這項工作涵蓋了政府、國軍與民間單位三個層面的權責劃分、協調分工，以及公私民協力三大部分，相關法規的制定與完備

1 是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。其中，重要資通訊系統或調度、控制系統，分別包括政府與民間之市內、長途、國際通信、行動通信、衛星通信、國際海纜、數據通信，以及無線廣播電視、有線廣播電視之通訊、傳播設施，以確保能源、水資源、交通、金融、醫院、政府機關、科學園區等功能正常營運。見〈國家關鍵基礎設施安全防護指導綱要〉，《行政院國土安全政策會報》，2018年5月18日，<https://ohs.ey.gov.tw/File/EF5E72C88077DE72>（檢索日期：2024年1月6日）

2 汪毓瑋，《國土安全（下）》（臺北市：元照出版，2021），頁699-712。

問題至為關鍵。

再以關鍵資訊基礎設施安全防護與轉換運用的重點而論，包括有線、無線網際網路、行動通信、固定電信、衛星通信、光纖海底電纜、廣播電視等各類型網路皆為關鍵資訊基礎設施的核心，[3] 且鏈連著政府機構行政體系、電子政務系統；軍事和國防通信、指揮和控制；醫療服務與公共衛生；航空、鐵路、公路和港口等交通設施；電力、石油和天然氣等關鍵能源供應，以及銀行、金融服務、支付系統之財務數據和交易等各個環節。若是發生嚴重故障，導致服務中斷，同樣會立即對國家安全、社會秩序、公共利益、民眾生活造成莫大危害。可見關鍵資訊基礎設施的防護、運用正隨著涉及領域範疇愈來愈廣泛，其重要性也隨著受到威脅和攻擊的程度而同步增加，更是影響各國維持全球商業、科技、軍事競爭力優勢的關鍵。[4]

臺灣四面環海，國土面積有限，一旦發生大規模戰爭或軍事衝突，境內地面通信網路、國際海底電纜，以及重要的網路節點極易遭外力破壞。以臺灣、馬祖間的海底電纜在過去幾年間曾多次發生斷纜造成通信中斷為例，[5] 如何建立國內、國際通信網路功能復原量能，抑或是增加備援手段來保障通信網路韌性，建立確保政府、國軍、民間單位仍能維持通信管道暢通，已成為包括臺灣在內，各國皆迫切強固的重點工作。進一步審視近年國際間發生的烏俄戰爭、以哈衝突，更可印證現代戰爭或軍事衝突往往在短時間內猝然發生，而通信網路等關鍵資訊基礎設施定是敵方鎖定的首要打擊目標。為了確保政府在應急、應變期間仍能透過多重通信技術與管道維持國內外聯繫暢通與政務正常運作，尤須加強軍民用通信網路的數位韌性。

通信網路不僅是關鍵資訊基礎設施的樞紐，同時也是其他關鍵基礎設施的運作命脈。考量當前國際戰略環境、臺海安全局勢以及各種潛在的安全突發事件極易讓社會和經濟陷入動盪不安，我國國家安全環境已呈現複合式態樣與混合型式的威脅態勢。國家安全不再僅僅關注軍事因素，經濟安全、環境、資通網路等對安全的影響範圍日益擴大。對此，本研究基於對我國現行法規制度的析察，借鏡外國經驗，以及思索以國家通信網路為根基之關鍵資訊基礎設施在平時與戰時的轉換、運用更佳作法，深入探討政府、國軍、民間單位的聯防、分工機制，確保關鍵資訊基礎設施得到更好的防護與運用。

貳、關鍵資訊基礎設施的平戰轉換運用

我國關鍵資訊基礎設施的平戰轉換運

3 Julia Brackup, Sarah Harting, Daniel Gonzales, Brandon Corbin, *Alternative Futures for Digital Infrastructure Insights and Considerations for the Department of Defense* (Santa Monica, CA: RAND Corporation, 2023), pp. 10-22.

4 Matt Pottinger, David Feith, "The Most Powerful Data Broker in the World is Winning the War Against the U.S.," *The New York Times*, November 30, 2021, <https://www.nytimes.com/2021/11/30/opinion/xi-jinping-china-us-data-war.html>（檢索日期：2023年12月2日）

5 黃琮淵，〈NCC擬修法，破壞海纜致災最重罰1億元，近5年故障中斷逾20次〉，《中時新聞網》，2023年3月30日，<https://www.chinatimes.com/newspapers/20230330000467-260110?chdtv>（檢索日期：2023年12月2日）

用涉及到許多層面的考量，例如安全防護技術、業務項目監理政策、法律，以及經濟、社會的產業體系運作等。這些基礎設施在平時就扮演著重要角色，而在戰時更攸關作戰的勝敗和國家的存亡。因此，如何保護這些基礎設施免受敵方攻擊，又能在必要時將這些基礎設施轉換為戰略資源，是國防安全與國土安全兩個領域皆須共同關注的重要課題。

各種公開資料顯示，關鍵資訊基礎設施正面臨如駭客入侵、網路間諜、網路恐怖主義、網路戰爭等多重威脅。其造成的危害不僅是資料洩露、系統損壞或功能中斷，也會影響到其他相關聯的基礎設施，甚至引發更大規模的災難。[6]因此，必須有健全的防禦能力，能夠及時偵測和回應任何異常或攻擊，並且能夠快速恢復正常運作。另一方面，關鍵資訊基礎設施亦須有良好的轉換能力，能夠在平時與戰時之間靈活移轉。這意味著，在平時，這些基礎設施需要遵循相關法規和標準，保障用戶的權益和隱私，並且提供高效率和高品質的服務。而在戰時，這些基礎設施則須能夠支援國家的軍事行動和戰略目標，例如提供情報、指揮、通信、控制等功能，並且能夠抵抗或反制敵方的干擾或破壞。

要實現此轉換與運用目標，需要建立一套完善的制度和機制，包括法律、政策、規範、協議等。這些制度和機制亦須能夠符合平時與戰時的界線和條件的界定，規範各類基礎設施在不同情況下的功能和責任，協調各類基礎設施之間的協調與合作，以及監督和評估轉換的效果和影響。此外，還需要有一套涵蓋人員、設備、程序等有效的執行和管理體系。這些體系須能執行和落實相關的制度和機制，並且能夠適應不同的情況和需求，以及應對不同的挑戰和風險。

一、美國的經驗

揆諸各國對關鍵基礎設施防護的政策與作法，美國在國土安全和防禦方面具有豐富的實踐經驗，成為本研究可借鏡的主要國家。美國曾遭受恐怖攻擊，擁有多場實戰經驗，無論是在國防與國土安全理念、功能、架構設計，抑或是政策、法規、合作模式等方面，為我國關鍵資訊基礎設施提供了平戰轉換運用有益參考。其中，以2001年的「911恐怖攻擊事件」為時間節點，美國對強化關鍵基礎設施防護的經驗已逾20年，包括一系列公布的戰略、法律、規劃、行政令、總統令，支撐著全國包括資訊基礎設施在內之安全防護與轉換運用機制。

首先，為確保關鍵基礎設施的可用性、安全性和快速恢復性的目標，美國已經建立了政府與關鍵基礎設施運營者之間的資訊共享和責任共同承擔的合作模式。在此合作模式之下，亦強調加強立法設置、增加研發投入和宣傳教育等一系列措施，以提升各方對關鍵資訊基礎設施防護的認識與能力。例如：隸屬美國國土安全部的「網路安全暨基礎設施安全局」(Cybersecurity and Infrastructure Security Agency, CISA)會以公布關於網路事件資訊共享指南(Guidance on Sharing Cyber Incident Information)的形式，為利益相關者提供明確的指引和相關資訊。[7]

6 樊國楨、韓宜蓁，〈美國關鍵基礎設施防護法案與資訊安全管理技術控制標準化〉，《國防雜誌》，第30卷第4期，2015年7月，頁99。

這種當政府蒐獲特定威脅情報，便會及時通知相關的基礎設施運營者，進行協同防禦的作法，有利於更全面地掌握潛在威脅，並且迅速應對，防範安全事件的發生和造成損害。

審視美國國會通過和由總統簽署施行的《國土安全法》(Homeland Security Act of 2002)、[8]《國土安全總統命令》(Homeland Security Presidential Directive, HSPD)、[9]相關關鍵基礎設施保護法令與執行規定(CIKR protection-related legislation, Executive Orders)與國家策略(national strategies)，[10]以及《關鍵基礎設施保護法》(Critical Infrastructure Protection Act)、《關鍵基礎設施資訊法》(Critical Infrastructure Information Act)等法案，[11]亦為相關工作的法律制度提供了支持，強調政府在促進民間公司企業與政府之間合作方面的角色。此外，為了強化防禦能力，不斷加強網路安全技術的研發，用以改進對抗網路攻擊的手段，保障系統的穩健性亦為政府與民營部門和學術機構合作的重點項目，[12]而定期舉辦安全研討會、製作安全教育影片，更是加深社會大眾對參與及理解關鍵基礎設施防護政策的重要手段。

其次，對關鍵基礎設施實體與行業進行明確的界定與責任劃分，亦可從美國的相關法規中見其律定。例如：依據2013年美國發布的第21號總統令《關鍵基礎設施安全和彈性》(Critical Infrastructure Security and Resilience)，確定了16項的關鍵基礎設施防護範圍（如表1所示）。透過明確定義關鍵基礎設施的範疇，美國正在逐步建立一個以國土安全部為主要負責政府部門、以風險評估和管控為指導原則、以公私合作和訊息共享為基礎的關鍵基礎設施保護體系。[13]

在轉換運用層面，則可關注美國負責

7 "Guidance on Sharing Cyber Incident Information," *Cybersecurity and Infrastructure Security Agency*, April 7, 2022, <https://cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf>（檢索日期：2023年12月2日）

8 "Homeland Security Act of 2002," *U.S. Department of Homeland Security*, September 1, 2022, <https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf>（檢索日期：2023年12月2日）

9 包含：「國土安全數位圖書館館藏」(Homeland Security Digital Library Collection)、「關鍵基礎設施識別、優先順序排序和保護」(Critical Infrastructure Identification, Prioritization, & Protection)、「國家防範」(National Preparedness)、「信號情報活動」(Signals Intelligence Activities)4個行政部門文件。見"Presidential Directives," *U.S. Department of Homeland Security*, August 18, 2022, <https://www.dhs.gov/presidential-directives>（檢索日期：2023年12月2日）

10 Franklin D. Kramer, Robert J. Butler, *Cybersecurity: Changing the Model* (Washington D.C.: Atlantic Council, 2019), pp. 5-9.

11 "Critical Infrastructure Information Act," *U.S. Department of Homeland Security*, January 27, 2022, <https://www.dhs.gov/sites/default/files/publications/CII-Act_508_0.pdf>（檢索日期：2023年12月2日）

12 "DOD Announces Release of 2023 Strategy for Operations in the Information Environment," *U.S. Department of Defense*, November 17, 2023, <https://www.defense.gov/News/Releases/Release/Article/3592788/dod-announces-release-of-2023-strategy-for-operations-in-the-information-enviro/>（檢索日期：2023年12月2日）

13 例如：經營美國國防、情報、安全和基礎設施工程的「帕森斯公司」(Parsons Corporation)正與美國網路司令部(U.S. Cyber Command)合作，提供J9網路專案執行辦公室(J9 PEO Cyber)和聯合網路作戰架構整合辦公

表1　美國關鍵基礎設施行業防護範圍

項　次	關　鍵　基　礎　設　施　行　業	權　責　管　理　單　位
1	化工行業	國土安全部
2	通信行業	
3	水壩	
4	應急服務行業	
5	信息技術行業	
6	商業設施	
7	關鍵製造業	
8	核設施行業	
9	政府設施	國土安全部和總務管理局
10	交通運輸行業	國土安全部和交通部
11	金融行業	財政部
12	國防工業設施	國防部
13	能源行業	能源部
14	農業食品行業	農業部和健康與公眾服務部
15	醫療保健和公共衛生行業	健康與公眾服務部
16	供水與廢水處理行業	環境保護局

資料來源："Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience," *Cybersecurity and Infrastructure Security Agency*, February 12, 2013, https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf

軍事動員的國防部，以及職掌國家動員的聯邦、州、地方政府中各相關部、署、局、委員會等單位所形成的三級指揮與協調聯繫。基於美國憲政體制，發布國防動員令的第一級決策權掌握在美國總統，而國會則掌有宣戰之同意權。第二級的國家安全會議則設有「緊急準備與動員計畫政策協調」機制，必須對第三級的軍方與政府各部門動員執行機構進行相關工作的指揮與協調。其中，美國國防部以「國防資訊系統局」(Defense Information Systems Agency, DISA)職掌國防企業能力和安全性、作戰和基礎設施、整合與創新、雲端運算，以及「網戰司令部」(Cyber Command)掌管各軍種網路空間防禦資源，提升機密資訊的互通、共享以及對網路空間攻擊的快速反應能力最為重要。透過負責網路保護、國家任務、作戰任務、技術支援部隊的執行，與隸屬國土安全部之「聯邦

室(Joint Cyber Warfighting Architecture Integration Office)相關服務。見"Parsons Awarded $91 Million Cyber Capabilities Contract," *Parsons Corporation*, November 9, 2023, <https://www.parsons.com/2023/11/parsons-awarded-91-million-cyber-capabilities-contract/>（檢索日期：2023年12月2日）

應急管理署」(Federal Emergency Management Agency, FEMA)，以及下轄之各階層應急管理局、應急管理辦公室，構建軍政體系鍵連的關鍵資訊基礎設施動員體制。此外，為確保機制運作，亦制定相關法規為依循（如表2所示）。

美國對於國家安全議題的重視，以及現行各種政策、制度，已激發許多國家積極投入建立堅實的全民防衛體系、提升高效的資通網路韌性，以及精進政府在應急或戰時的指揮體系效能。對臺灣而言，更是要在肆應中共敵情威脅和安全環境變遷中，完備相關運作機制，維護國家安定。

二、我國的作法

我國「全民防衛動員」制度除了動員實施階段由國防部承總統依憲法發布之緊急命令，主責全國動員或局部動員外，在動員準備時期區分「行政動員」與「軍事動員」兩個子系統。其中，行政動員準備由中央各機關及直轄市、縣（市）政府負責執行；軍事動員準備由國防部負責執行，中央各機關配合辦理。相關準備事項亦須由中央各機關，以及直轄市、縣（市）政府納入年度施政計畫推動實施。

由於動員的實施是由「預防與準備」以及「積極的危機管理處理」概念所產生的。故動員機制被視為一種轉換和控制的機制，其功能在於將政府體制從平時轉變至戰時或非常時期，使國家的戰爭潛力由隱性和潛在轉變為明確和實際，同時對全國的人力、物力、財力等整體力量進行統一的控制、調整和分配(如圖1所示)。

(一)政府行政體系

以中央各機關及地方政府為主體，各地方政府擔負實際執行責任。其中，根據行政院各相關動員準備業務部會的指示，地方政府須制定應變計畫，評估地方的防衛需

表2　美國國家與資通信動員相關法規

類　　型	法　規　名　稱
動員法規	總動員法 國家緊急狀態法 戰爭授權法 國防部組織法 國防資源法 國防優先法
資通領域相關法規	資訊設備安全法案 關鍵設施保護計畫 網路空間安全資訊共享法案 網路空間戰略 網路安全國家行動計畫

資料來源：作者自行彙整

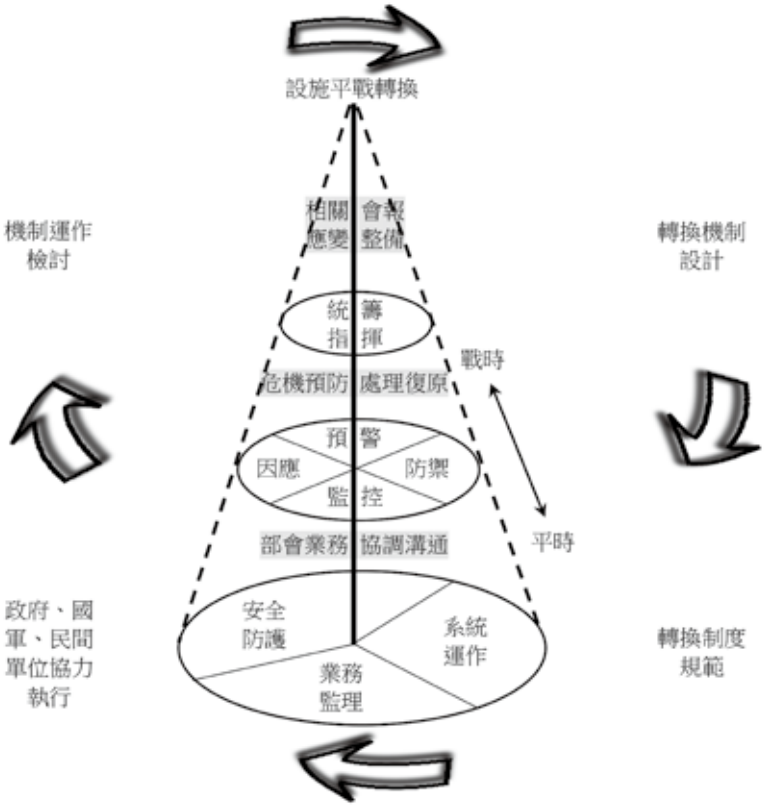

圖1　關鍵資訊基礎設施平戰轉換運用示意圖

資料來源：作者自行繪製

求，以及當地資源、民力等進行動員準備，確保當地能夠迅速有效地參與動員工作。同時，中央各機關亦應負責提供指導、協助、和整體規劃，以確保全國各地的動員工作協調一致。例如在建置視訊會議、網路電話與廣播電視直播系統方面，中央政府機關須加強突發事件現場影像傳輸、語音通訊、視訊會議等應急通信能力建設；地方政府亦須按照政府指揮體系要求，於平時建立、維管並測通聯繫和傳輸訊息所需之電信、資訊網路，確保在戰時或重大災害發生時的通聯暢通。

(二)國軍軍事系統

為強化對關鍵資訊基礎設施的防護和應對能力，國軍的軍事動員會著重在資訊科技人才的動員、資訊戰力的提升，以及對關鍵資訊基礎設施進行防護三個方面。目前國軍為強化資訊科技人才兵力結構，除了在軍事教育中建立相關領域人才培育管道，並充實資通電主戰部隊執行國軍電子戰、通信資訊網路架設、建立實時監測系統等任務所需，在守備、後備部隊方面，則藉由「強化全民國防兵力結構調整方案」，將國內網路安全、資訊系統防禦等方面具有專業知識的優秀的資訊科技人才，透過徵募併行兵役制度納入動員對象。[14] 這些專業人才在國家動員期間，可被指派參與防禦策略的制定、軍民用網路安全攻防，以及強化關鍵基礎設施的防護措施。為了驗證應對能力，平時亦會藉實戰演練，針對模擬的關鍵資訊基礎設施攻擊進行應變，以檢驗軍事系統的應變能力。[15]

(三)民間電信、資通、廣播電視經營業者

目前國內的通訊體系主要依賴4家整合性固網業者，以及3家行動業者來提供全國通訊網路；在國際通訊方面，則建置有14條連接外部的海底纜線。至於外（離）島地區，設有10條國內海底纜線，同時借助微波技術進行通訊。這些通訊網路不僅是通訊領域的重要基礎設施，更聯繫著其他關鍵基礎設施正常運作。

為了強化數位韌性，政府要求民間電信業者在動員時必須盡可能地維持和保障通信網路的穩定性。資通業者則須協助政府機構和國軍進行強化網路安全、提供即時監控系統，以及支援防範資訊戰的技術和設備等資訊安全的防禦和應對措施。廣播電視業者在動員期間亦被要求提供相關的應急通知和資訊。包括參與政府的公共事務宣傳，向民眾傳達重要訊息，並在需要時協助傳遞緊急通告和指示。對此，民間業者需與政府機構和國軍進行密切協調，確保各項動員準備方案與行動符合整體動員計畫。透過確保通信網路的運作、加強資訊安全、支援媒體宣傳，以及制定應急計畫等方式，發揮著關鍵的支援和協助作用，確保整個國家在需要時能夠有序應對。

14〈強化全民國防兵力結構調整方案說明〉，《中華民國國防部》，2023年1月10日，<https://www.mnd.gov.tw/Publish.aspx?u=NewUpload/202301/強化全民國防兵力結構調整方案-詳細說明_582413.pdf&fid=43404>（檢索日期：2023年12月2日）

15 周力行，〈第三作戰區關鍵基礎設施防護演練，蔡總統：共同提升臺灣耐災韌性〉，《軍聞社》，2023年7月26日，<https://mna.gpwb.gov.tw/news/detail/?UserKey=872b33b4-5853-4d78-82a2-f96e56e08401>（檢索日期：2023年12月2日）

綜合以上所述，我國關鍵資訊基礎設施平戰轉換運用機制的最高決策權由總統擁有，並由行政院作為統籌辦理動員準備事項之主責單位。其中，院長、副院長分別擔任「全民防衛動員準備業務會報」、「國土安全政策會報」之召集人，而國防部部長除兼任動員準備業務會報執行長，承召集人之命，綜理會報事務，亦為兩大會報之委員。在平時，屬於國土安全範疇之「關鍵資訊基礎設施」業務由行政院國土安全辦公室負責辦理各項幕僚作業，負責協調各機關、地方政府，以及相應的民間機構。進入應急、應變或戰時，國防部將擔負更為核心關鍵的角色與職責。包括動員指揮、資源調配、情報協同等，以確保國家能夠快速且有序地應對各種挑戰。因此，為確保統籌與調度機制順遂，國防部與行政院國土安全辦公室之間的相互協調配合，攸關政府部會間各項業務主管機關之平戰轉換時的權責、權限交接，也直接影響地方政府、民間機構之間與中央政府的有效協同配合。

此外，國防部與數位發展部、國家通訊傳播委員建立密切的工作協調、訊息共享、資源整合，亦為落實平戰轉換的關鍵，目的在確保在平時至戰時轉換過程中的無縫對接和高效運作。其中，國防部、數位發展部之間的工作聯繫是實現關鍵資訊基礎設施安全和功能轉換的基礎。國軍負有捍衛國家安全第一道防線職責，指揮、管制、通信、資訊、情報、監視和偵察系統(C^4ISR)須維持暢通；另數位發展部於平時就職司關鍵資訊基礎設施的資訊化發展和資通安全，在同樣為國家安全優先設想下，兩部之間的合作不僅能夠提供國軍實際的安全需求和情報支持，透過資訊科技創新應用和資通安全政策引導，則能增進關鍵資訊基礎設施安全韌性的提升。而在國防部、國家通訊傳播委員會之間的合作關係方面，則有賴於國家通訊傳播委員會主責監理國內電信衛星、廣播電視等行業之豐富經驗和資源，能夠與國防部共同聚焦於軍、公、民營通信網路系統的互通聯繫，特別是必須確保各作戰區內的命令傳遞、戰情統合匯整，以及與警消、海巡等機關構聯，強化在危急環境任務中的作戰效能及支援能量。

無論是會報機制的協調配合或是由國防部各業管聯參部門與相關部會建立協調聯繫管道，所有機關和部會、部門之間的協調和分工不僅僅須在平時進行，更重要的是要在戰時或緊急情況下及時應對。此一由平時轉到戰時的權責交接機制，往往須根據不同情況和需求進行靈活調整。因此，維繫關鍵資訊基礎設施的正常穩定運作，仍有賴包括國軍在內之公私民協力夥伴關係(Public-Private-People Partnership, PPPP)的靈活性與適應性，確保整體動員準備工作高效執行。在此過程中，聯防核心思維，加上平戰結合的務實作法，以及統籌協調分工關係，皆是不可或缺的要素，尤其是在關鍵資訊基礎設施的平戰轉換和運用政策制定及配套作法方面。

參、政府主要部會權責與分工

政府基於民國92年7月28日召開的「行政院全民防衛動員準備業務會報91年度工作檢討會」，決議建構以全民防衛動員準備體系作為備援主軸之國土安全機制，規劃包括災害防救、民防、緊急醫療、反恐等範疇，以強化全民防衛動員準備系統的協同作用，提高處理各種緊急危機的效能。[16] 此外，政府亦於2018年9月公布首部《國家資通安全

戰略報告》，透過整合國家安全會議「國家資通安全辦公室」、行政院「資通安全處」以及「國家通訊傳播委員會」組成國家資安防護鐵三角機制，並著眼於國安、資安、通安等層面，保護國家與社會的整體安全，以及和友邦進行國際聯防及情資分享。[17] 在此運作機制下，我國掌理關鍵資訊基礎設施工作的主責部門是「數位發展部」，其設施平時、戰時的轉換運用則納入「全民防衛動員準備」制度。為釐清政府相關部門權責與分工，聚焦關鍵基礎設施防護、全民防衛動員準備、關鍵資訊基礎設施安全，以及電信、衛星與廣播電視管理，說明其統籌、協調、分工關係。

一、行政院國土安全辦公室：關鍵基礎設施防護

國土安全辦公室為行政院院本部之業務單位，其職掌是按照國土安全政策會報決議、配合國家安全系統，處理關鍵基礎設施防護業務事項，確保國家安全和資訊基礎設施的完整性和穩定性。又因國土安全辦公室扮演關鍵基礎設施防護相關工作之協調、指導、監督等重要幕僚角色，其「防護」業務的核心在於有效防禦各種安全威脅，尤其是針對關鍵資訊基礎設施的物理、數位層面攻擊，必須持恆增進包括設施防火牆、入侵檢測系統、加密通信等技術手段，以及設置安全監控、定期演練等管理措施，確保防護工作可行、有效。基此，審視國土安全辦公室的主要職責包括：

第一，檢視與稽核安全防護計畫書與工作：國土安全辦公室應檢視並稽核主領域協調機關的安全防護計畫書與工作，並送行政院核備。[18]

第二，指導防護演習計畫：在關鍵基礎設施防護演習方面，行政院國土安全辦公室提供指導手冊，要求擬訂演練計畫、辦理說明會議，並詳實記錄演練過程，以作為未來修訂防護計畫的參考。[19]

第三，協調國土安全政策：參與國土安全政策會報，並協調反恐及關鍵基礎設施防護，包括制定基本方針、工作計畫、演習訓練、安全監控、通報應變機制。[20]

第四，定期舉辦防護演習：行政院國土安全辦公室定期舉辦國家關鍵基礎設施防護演習，強調專業職能的發揮。[21]

16〈全民防衛動員準備機制介紹〉，《嘉義市政府警察局第二分局》，2006年3月21日，<https://wn1.ccpb.gov.tw/download/index.php?mode=dl_file&data_id=75&file_rename=5rCR6ZiyNl8xNzA2MDYwNjU5MDM=.doc>（檢索日期：2023年12月2日）

17 林正義，〈美國與中共網路戰略及其對臺灣可能的影響〉，《國防雜誌》，第35卷第4期，2020年12月，頁42。

18〈國家關鍵基礎設施安全防護指導綱要〉，《行政院國土安全政策會報》，2018年5月18日，<https://ohs.ey.gov.tw/File/EF5E72C88077DE72>（檢索日期：2024年1月6日）

19〈關鍵基礎設施防護演習指導手冊〉，《行政院國土安全辦公室》，2021年4月9日，<https://ohs.ey.gov.tw/File/91A85FC21D277A1>（檢索日期：2024年1月31日）

20〈國土安全辦公室組織與職掌〉，《行政院》，<https://www.ey.gov.tw/Page/66A952CE4ACACF01>（檢索日期：2024年1月31日）

21 林裕洋，〈專訪國家資通安全研究院副院長林盈達〉，《CIO Taiwan》，2024年1月，<https://www.cio.com.tw/interview-lin-yingda-vice-president-of-the-national-institute-of-security-studies/>（檢索日期：2024年1月31日）

為能保障關鍵基礎設施之資訊系統於戰時環境下的持續運作能力，在平時、戰時功能轉換方面，尚須側重於戰時緊急通信系統、備份資料中心、遠程控制和管理機制等運作無虞。故在相關運作機制方面，亦須在「國土安全網」應變體系下，[22] 與國防部、數位發展部、國家通訊傳播委員會保持良好的業務合作關係。確保關鍵資訊基礎設施能夠快速、有效地轉換功能，充分支援臺澎防衛作戰和應急所需，發揮提供與支援國家安全和國防戰備整備之功能與服務。

二、國防部：全民防衛動員準備

「全民防衛動員準備」制度緣於民國31年3月29日《國家總動員法》之「國家總動員綜理業務」。民國81年政府宣布終止動員戡亂時期後，改以《全民防衛動員準備實施辦法》作為國家動員準備工作法規依據。惟因該實施辦法位階僅為行政命令，其涉及人民權利、義務之事項屢遭質疑，嗣於民國90年11月14日公布《全民防衛動員準備法》，成為我國策訂各種動員準備分類計畫與結合政府各項動員準備事項之最根本法源依據。[23]

據此，行政院依法成立「行政院全民防衛動員準備業務會報」，由國防部擔任秘書單位，負責協調各部會之間的行政、軍事動員準備，同時主導國家動員實施工作。透過資源共享、訊息流通、協同作戰等方面的順暢聯繫，及時支援和緊急應變。在此體制下，「國防部全民防衛動員署」承擔著關鍵角色，擔負協調橫向跨部會合作機制，制定後備軍事動員計畫等相關準備工作，[24] 確保全民防衛動員體制順利運作。

「全民防衛動員準備」是我國的國防動員準備的機制。目的在整合、準備包括人力、物力、財力、技術和軍事能力等國家資源，強化平時整體防禦能力，並能應援軍事行動與緊急情況。圖2明確顯示我國全民防衛動員準備的運作機制，凸顯其多方面的涵蓋範疇和相互協同特性。

其次，為能確保「全民防衛動員準備」事項順利運作，除與民國91年3月1日施行之《國防法》密切相關，[25] 其他包括：《行政院全民防衛動員準備業務會報設置要點》、《國防部全民防衛動員署組織法》、《全

22 黃正芳，〈建構我國國土安全五大應變體系國土安全網之探討〉，《國防雜誌》，第27卷第2期，2012年3月，頁6、23。

23 郭憲鐘，〈全民防衛動員準備法相關問題之研析〉，《立法院》，2001年1月1日，<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6586&pid=84257>（檢索日期：2023年12月2日）

24〈建置臺灣民間自主緊急應變隊中程計畫（113年至118年）〉，《內政部消防署》，2023年6月12日，<https://www.nfa.gov.tw/cht/index.php?act=download&ids=18117>（檢索日期：2023年12月2日）；中華民國112年國防報告書編纂委員會，《中華民國112年全民國防報告書》（臺北市：國防部，2023），頁104。

25 包括《國防法》第3條：「中華民國之國防，為全民國防，包含國防軍事、全民防衛及與國防有關之政治、經濟、心理、科技等直接、間接有助於達成國防目的之事務」。該法第5章亦設「全民防衛」專章，其第24條：「總統為因應國防需要，得依憲法發布緊急命令，規定動員事項，實施全國動員或局部動員」；第25條：「行政院平時得依法指定相關主管機關規定物資儲備存量、擬訂動員準備計畫，並舉行演習；演習時得徵購、徵用人民之財物及操作該財物之人員；徵用並應給予相當之補償」；同條第2項：「前項動員準備、物資儲備、演習、徵購、徵用及補償事宜，以法律定之」皆為兩部法規重要的關聯之處。見彭錦珍，〈我國國防政策合法化之研究—以《國防法》制定為例〉，《復興崗學報》，第80期，2004年6月，頁155。

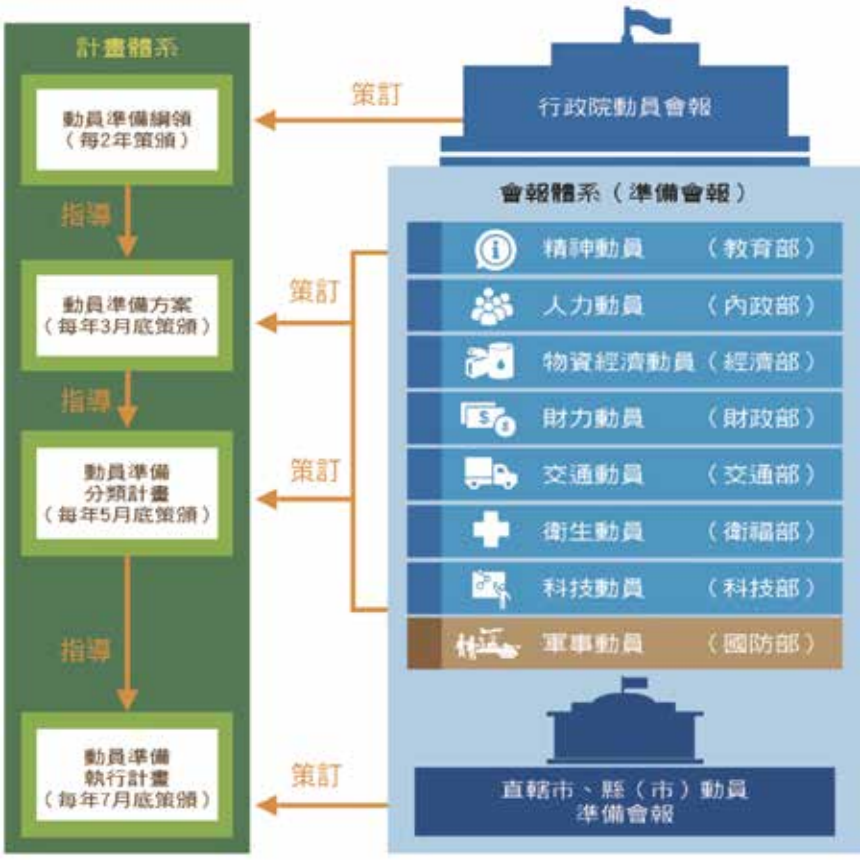

圖2　中華民國全民防衛動員機制運作示意圖

資料來源：中華民國110年國防報告書編纂委員會，《中華民國110年全民國防報告書》（臺北市：國防部，2021），頁76。（註：2021年7月科技部升格國科會）

民防衛動員實施階段物資固定設施徵購徵用及補償實施辦法》、《推動全民防衛動員準備事務獎勵及慰勞辦法》、《結合民防與全民防衛動員準備體系及協力組織執行災害整備及應變實施辦法》、《動員實施階段軍事人力統籌分配辦法》、《動員實施階段國軍機動運輸及軍品運補交通管制辦法》、《戰備各階段公民營通信設施支援軍事管制運用辦法》等相關法規的制定亦涵蓋了臺灣全民防衛動員準備工作的原則、目標、組織、職責、措施、資源、監督和獎懲等內容。目的在將國防動員從一個被動的、應急的、戰時的概念，轉變為一個主動的、預防的、常態的運作機制。

再以各階段動員之定義與任務面向而論，全民防衛動員準備為「全民國防」的具體實踐，須透過動員程序，以充分運用政、經、軍、心、科技等總體力量來強固國防，各動員階段與任務如表3所示。其中，「科技動員」在支持全民防衛動員準備過程亦為保障關鍵資訊基礎設施順利運作之重要機制。2021年7月，由科技部升格的「國家科學及技術委員會」成為我國最高科研事務最高權責機關，包括主導與投入資通安全防護、應變通信系統建立等和資訊戰力相關之先進科技研發，對於確保國家在平時、戰時或緊急情況下的通信、指揮控制和訊息傳遞效能極為重要。

三、數位發展部：關鍵資訊基礎設施安全

關鍵基礎設施是指「在一個國家中為

表3　我國各階段動員之定義與任務

動員階段	定　　義	任　　務
動員準備	指平時實施動員準備時期。	結合施政作爲，完成人力、物力、財力、科技、軍事等戰力綜合準備，以積儲戰時總體戰力，並配合災害防救法規定支援災害防救。 ●行政動員準備：由中央各機關及直轄市、縣（市）政府負責執行。 ●軍事動員準備：由國防部負責執行，中央各機關配合辦理。
動員實施	指戰事發生或將發生或緊急危難時，總統依憲法發布緊急命令，實施全國動員或局部動員時期。	統合運用全民力量，支援軍事作戰及緊急危難，並維持公務機關緊急應變及國民基本生活需要。

資料來源：〈全民防衛動員準備法〉第2條，《全國法規資料庫》，2019年6月19日，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=F0070013&kw=全民防衛動員準備法>（檢索日期：2024年1月6日）

維持國家安全、民生、經濟而提供的基本產品或服務，包含維持國家最基本的經濟、民生、政府運作與國家安全息息相關的實體和以資訊電子為基礎的運作系統」。[26] 我國依功能屬性將關鍵基礎設施區分：能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等八大主領域，各有不同的主管機關，[27] 並且對應於公民營的電信、能源、銀行、財金、交通、供水及防救災等系統。其中，支持關鍵基礎設施所需之資通系統即為「關鍵資訊基礎設施」，亦是重要防護範圍。[28]

另依據《資通安全管理法》第3條第7項，關鍵資訊基礎設施是指「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」。[29] 其保護與管理由我國行政院「國土安全政策會報」和「資通安全會報」負責推動，前者負責實體防護，後者負責資通安全。有關於關鍵基礎設施的指定與分級，是由中央目的事業主管機關指定關鍵基礎設施提供者，報請行政院核定，並依據其影響程度分為不同的資通安全責任等級和資通安全事件通報等級。[30]

另在政策推動與執行方面，則是由民國111年8月27日成立之「數位發展部」作為資通安全防護和強化的主責機關，掌管資訊、電信、傳播、資安及網際網路五大領域安全事項。該部所屬「資通安全署」，以及監督

26 行政院科技顧問組，《關鍵資訊基礎建設保護政策指引》（臺北市：行政院，2011），頁1。

27〈國家關鍵基礎設施安全防護指導綱要〉，《行政院國土安全政策會報》，2018年5月18日，<https://ohs.ey.gov.tw/File/F31BBE04AD8B9E98>（檢索日期：2024年1月6日）

28〈國家資通安全發展方案（110年至113年）〉，《行政院國家資通安全會報》，2021年2月，頁7，<https://cc.ncku.edu.tw/var/file/2/1002/img/1302/776559884.pdf>（檢索日期：2023年12月2日）

29〈資通安全管理法〉，《全國法規資料庫》，2018年6月6日，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297>（檢索日期：2023年12月2日）

30 同註15。

之「國家資通安全研究院」為國家資通安全政策研擬、規劃及執行的重要單位。此外，「韌性建設司」、「資源管理司」則分別職掌通訊傳播事業基礎設施防護與資通訊動員準備相關業務，以及通訊傳播與數位資源之整體規劃、整備、分配、核配、補償及管理。[31] 這些與關鍵資訊基礎設施平戰轉換直接相關業務規劃以及由該部主管《電信事業資通安全管理辦法》、《關鍵電信基礎設施指定及防護管理辦法》、《無線電頻率使用管理辦法》、《資通安全事件通報及應變辦法》、《資通安全責任等級分級辦法》等法規，成為我國關鍵資訊基礎設施安全防護與功能轉換運作之重要制度依循。

四、國家通訊傳播委員會：電信、衛星與廣播電視監理

「國家通訊傳播委員會」於民國95年2月22日成立，作為我國電信通訊和廣播電視等訊息流通事業的最高主管機關，為受行政院監督的獨立機關，主要職責是規劃通訊傳播政策、制定通訊傳播法規、審核通訊傳播事業執照、監督通訊傳播事業經營、處理通訊傳播申訴、維護通訊傳播秩序、推動通訊傳播教育等。[32] 相較於數位發展部專責於國家數位產業發展與資通安全防護，國家通訊傳播委員會主要是對這些業務項目扮演「監理」職能，亦即數位發展部是「踩油門」的角色；國家通訊傳播委員會則是「踩煞車」。[33]

由此審視國家通訊傳播委員會主管的法規，例如《通訊傳播基本法》第14條「遇有天然災害或緊急事故或有發生之虞時，政府基於公共利益，得要求通訊傳播事業採取必要之應變措施」；《電信法》第25條「電信事業對於發生天災、事變或其他緊急情況或有發生之虞時，為預防災害、進行救助或維持秩序之通信；陸、海、空各種交通工具之遇險求救及飛航氣象等交通安全之緊急通信；為維護國家安全或公共利益，有緊急進行必要之其他通信等，應予優先處理」；《電信管理法》第22條「為預防或因應災害防救或動員準備，各相關主管機關依其主管法律規定，得指定電信事業採取確保通信之必要措施或設置應變相關設施」，以及《衛星廣播電視法》第26條「遇有天然災害或緊急事故，主管機關得指定衛星廣播電視事業播送特定之節目或訊息」皆為我國電信、衛星與廣播電視在平戰轉換時可參酌的法規依據。另為保障國家在天然災害及緊急事故發生時仍能本於保障公眾的生命安全和財產安全考量，對訊息通報、應變程序、緊急救援等應急處理有所規範，《有線廣播電視法》、《有線廣播電視法施行細則》、《有線廣播電視系統經營者天然災害及緊急事故應變辦法》亦為該會主管之重要法規。

肆、現存問題與解決之道

一、先做好「聯防機制」設計，再強化「設施防護」

31〈數位發展部處務規程〉，《全國法規資料庫》，2022年8月8日，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0010154>（檢索日期：2024年2月7日）

32〈國家通訊傳播委員會組織法〉，《全國法規資料庫》，2022年5月4日，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=P0000008&kw=國家通訊傳播委員會組織法〉（檢索日期：2023年12月2日）

33 徐子苓，〈數發部成立！一文看懂成立背景、政策目標〉，《自由時報》，2022年8月27日，<https://ec.ltn.com.tw/article/breakingnews/4039483>（檢索日期：2023年12月2日）

當前的安全挑戰日益複雜，單一機構難以應對各種戰爭、災難和網路攻擊，再加上關鍵資訊基礎設施因涉及實體和資通安全兩層面，建立高效的「聯防機制」成為保障全民防衛動員成功的不二法門。無論是安全防護或是平戰轉換，這種機制應涵蓋政府、國軍、資通業者、相關企業公司等各關鍵基礎設施的運營者，並廣泛整合民營業者中與國家安全密切相關的行業，透過跨部門的合作和資訊共享，方能完善資通安全體系運作。

實現聯防的核心挑戰在於建立高效的跨部門協作機制。以全民防衛動員準備機制下的政府部門功能而論，又以國防部和數位發展部、國家通訊傳播委員會在電信、資訊、廣播電視等資通電基礎政策、法規的相互配合與協調最為關鍵。以我國現行由數位發展部主管之《無線電頻率使用管理辦法》為例，無論是在平時、戰時，皆為確保國家無線電通信暢通，確保各頻段無線電頻率核配、使用、共享管理之重要法規。惟檢視「無線電頻率干擾處理」專章內容，可見軍用和非軍用干擾之受理機關仍為「國家通訊傳播委員會」，可依法進行干擾來源查測及排除。[34] 可見政府部門間依據各自權管權責，依法建立跨部門協調與合作機制，為提高國家靈活、迅速地抵禦各種複合安全威脅能力的關鍵。進一步整合民間單位等多方力量的聯動安全網路，其整合性和分層次的防護體系定能有效增進全民防衛動員的平戰轉換與運用成功機率。

另考量行政院國土安全辦公室雖然在國家安全體系中扮演重要角色，但其主要職責主要集中在國土安全相關業務的推動與精進，特別是在關鍵基礎設施防護業務之外，該辦公室尚肩負我國反恐預防與應變整備工作職能在身。現階段就其業務幕僚單位特性，以及受限於編制與人力資源配置，實難涵蓋在全民防衛動員準備制度運作下的關鍵資訊基礎設施全面協調與整合。因此，在平戰轉換實際運作層面，仍有賴國防部、數位發展部、國家通訊傳播委員會在職能、職掌層面建立務實、有效的協調與合作機制，並且攸關中央政府部門、國軍、民間單位建構聯防機制。

此外，聯防機制的設計也須納入明確的指揮結構和充分的訊息共享。政府在這方面的作用是提供有效的協調，確保不同部門之間、中央與地方之間，在行動上保持一致性。藉由進行定期的跨部門演練和培訓，以應對可能發生的各種危安情境，提升整體應變能力。另為了應對跨國威脅，聯防機制亦應融入國際體系。[35] 透過與其他國家建立安

34 該辦法第42條第1項「軍用通信之干擾申訴，由國防部受理、查測及排除。未能查明干擾信號之來源時，得洽商國家通訊傳播委員會進行查測，以斷定干擾之來源，並決定處理辦法」；同條第二項「非軍用通信及來自國外之干擾申訴，由國家通訊傳播委員會受理、查測及排除。未能查明干擾信號來源時，得洽商國防部會同處理」。見〈無線電頻率使用管理辦法〉，《全國法規資料庫》，2023年7月27日，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0060123>（檢索日期：2023年12月2日）

35 例如「北約」於2023年11月在愛沙尼亞舉行了一場網路安全演習，包括日本、韓國皆以正式參與者的身分參加。另負責新興安全挑戰的助理秘書長表示：北約希望與印太地區夥伴深化合作。見Elisabeth Gosselin-Malo, "NATO Deepens Cyber Coalition with Asian Partners," *C4ISRNET*, December 1, 2023, <https://www.c4isrnet.com/cyber/2023/12/01/nato-deepens-cyber-coalition-with-asian-partners/>（檢索日期：2023年12月2日）

全合作關係，共享情報、經驗和技術，才能精準、即時、全面地掌握和因應全球性資通安全威脅，形成有力的防禦網路。

在關鍵資訊基礎設施防護的技術和策略方面，只要確保聯防機制穩定運作，即可進一步強化「設施防護」，以確保各類型基礎設施的可靠性和安全性。在技術層面，著重發展先進的數位韌性技術，使關鍵基礎設施對於網路攻擊具有更高的防護力。同時，應加強對實體設施的實時監控，導入智慧感測裝置和監測技術，提高對潛在威脅的敏感度。

二、要實現「平戰轉換」須先做好「平戰結合」

鑒於外國關鍵資訊基礎設施防護經驗以及戰爭衝突的啟示，儘管我國在「平戰結合」方面已逐漸建立共識，並且取得一些進展，惟仍然面臨著挑戰和不足，尤其是在政府跨部門應對機制、資通安全體系、軍民合作等多重因素和層面必須持續精進。此外，相關政策、法規的與時俱進、完備制定亦為關鍵資訊基礎設施「平戰結合」的關鍵。

關鍵資訊基礎設施功能、效能的順利轉換，取決於各類型設施的基礎建設與備援方案，必須結合平時與戰時。隨著戰爭型態與安全環境的轉變，傳統的戰時和平時的界線變得日益模糊，軍隊和地方在國家資訊通信體系中的聯繫日益密切，「平戰結合」不僅是應對現代複合安全威脅的必然選擇，更是實現資源最大化利用、全面提高安全效能的有效手段。透過這種理念的落實，不僅能夠在平時確保社會運作韌性，亦能在戰時快速轉換，應對各種複雜情境。基此，除了建立安全防護協調機制，持續強化政府、國軍、民間單位等各方軟硬體建設的功能，亦為實現建立靈活、迅速、高效的平戰轉換目標之必要之舉。[36]

「平戰結合」的關鍵便是要在平時就能建置國家因應緊急事件或天然災害的應變能力。針對關鍵資訊基礎設施，必須考慮三個方面的結合。第一，結合資訊化建設和網路空間防禦建設；第二，結合網路空間的戰時應對於平時網路安全工作，實現戰備與備戰用途的互相促進；第三，結合網路戰備效益與社會效益、經濟效益。其中，戰備效益是平戰結合的前提，經濟效益是基礎，社會效益是必然的結果。在實踐中，必須妥善處理三種效益間的關係，確保戰略目標實現。

以歐盟的作法為例，為了做好關鍵資訊基礎設施平戰結合工作，除了制定相關戰略或政策文件，亦針對能源、數位基礎設施、交通和航太部門等關鍵基礎設施進行壓力測試。其中，歐盟於2018年建立了網路防禦政策架構(Cyber Defence Policy Framework, CDPF)，確定了發展網路防禦能力和共同安全與國防政策(Common Security and Defence Policy, CSDP)通信保護和資訊網路等優先事項。[37] 2023年11月14日，歐盟的「歐洲防衛局」(European Defence Agency, EDA)更新了2023年《歐盟能力發展優先事項》(The 2023 EU Capability Development Priorities)，強調必須增強網路安全和資訊作戰能力，同時

36 李彥璋，〈國軍應對網路攻擊之法理框架〉，《國防雜誌》，第37卷第3期，2022年9月，頁68-69。

37 "European Parliament Resolution of 7 October 2021 on the State of EU Cyber Defence Capabilities," *European Commission*, October 7, 2021, <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0412_EN.html>（檢索日期：2023年12月2日）

明確提及將關鍵基礎設施的保護和復原能力納入軍事能力發展的首要目標。[38] 歐盟亦與「北約」(North Atlantic Treaty Organization, NATO)於2023年3月啟動關鍵基礎設施復原能力工作組，目的即在促進對彼此工作的相互認識，分享最佳實踐，並確定協同作用和進一步的合作領域。[39] 在網路防禦方面，歐盟亦持續進行多個專案研究。包括歐洲國防工業發展計畫，即有關於情報、安全通信和網路防禦的相關專案，並且專注於對技術、設備、服務、數據和數據處理的防禦能力提升與管制。[40]

可見，要實現「平戰轉換」，須針對「平戰結合」制定明確的策略。首先，在國家層面，建立戰時應對體系，確保資訊系統能夠在瞬息萬變的戰爭環境中迅速轉換。其次，加強國軍與民間單位合作，在機密保護原則下，建立設備共通、共用與資訊共享機制，確保資訊基礎設施在平戰關鍵時期的無縫切換。再者，促進防禦技術的研發，使其能夠適應不同的場景，實現平戰結合的靈活應對。

三、中央政府機關、國軍、民間單位的統籌與協調機制

在資訊網路技術快速發展的今天，保護關鍵基礎設施的物理空間安全同樣重要。其中，中央各機關主管的動員準備方案涵蓋多個層面，由不同部門主導，包括精神動員、人力動員、物資經濟動員、財力動員、交通動員、衛生動員、科技動員、軍事動員等。儘管這種區分明確，惟這些動員準備業務範疇，如何在「國防安全」、「國土安全」範疇找到協調機制的均衡點，仍有賴政府部會之間，甚至與民間單位、相關協力團體持續建立共識。以全民防衛動員準備機制運作現況而論，各方以「全民國防」理念作為鏈結並無疑義，惟在實際運作過程，涉及到的人力、物力、財力往往是任務執行最現實的考量因素。特別是在業務績效競爭壓力下，平時的民防、災防、動員準備、全民國防教育、國土安全等業務，往往成為消極甚至冷門的工作。這也導致每每在國家發生天災、人為重大危安事件時，即易出現政府行政體系無法充分協調合作導致危害擴大的憾事結果。

又如在實際運作中可見，儘管中央政府機關、國軍皆制定許多關於關鍵基礎設施防護、全民防衛動員準備工作可資依循的法規或程序辦法，惟在地方政府層級，或因業務整併或人力精簡因素，而將原本的動員業務移至民政部門兼辦，遑論在鄉、鎮、市層級更因人力、專業與經費有限，更是難以落實。[41] 因此，如何強化各層級間的統籌與協

38 European Defence Agency, *The 2023 EU Capability Development Priorities*, November 14, 2023, <https://eda.europa.eu/docs/default-source/events/eden/phase-iii/factsheets/cdp-factsheet---eda---14-nov-2023.pdf>（檢索日期：2023年12月2日）

39 "EU-NATO Task Force on the Resilience of Critical Infrastructure," *European Commission*, June 29, 2023, <https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf>（檢索日期：2023年12月2日）

40 "European Parliament Resolution of 7 October 2021 on the State of EU Cyber Defence Capabilities," <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0412_EN.html>（檢索日期：2023年12月2日）

41 例如：《全民防衛動員準備法》第12條：「縣（市）政府得視需要，指定所轄鄉（鎮、市、區）公所指

調機制，例如：建立跨機關合作平臺，提供各級政府機關、國軍和民間單位之間即時溝通和訊息分享之用；強化舉辦跨機關全民防衛動員演練和模擬活動的實況內容，以測試和改善各機關之間的協調應變能力；建立關鍵資訊或緊急事件通報聯絡人網路，並設立清晰的通報流程和準則；建立蒐集、存儲和分享各類訊息之共通資訊系統、訊息分享標準，及時提供可靠數據，支持決策和因應行動；以及進行資訊網路技術整合與跨機關人才交流，提高應對緊急情況的整體效能和安全性，皆是可再深思熟慮的方向。

另聚焦關鍵資訊基礎設施的平戰轉換實體建設，除須保障和運用臺灣與金門、馬祖、澎湖等外（離）島地區海底電纜在通信聯繫、網路安全、緊急應變與國防安全等方面需求的可靠性和穩定性外，亦可謹慎評估我國衛星通信系統的強化作法。審視我國「數位發展部」提出的「應變或戰時應用新興科技強化通訊網路數位韌性計畫」，[42] 可知該計畫主要是為確保戰時或大規模災害發生時，政府指揮體系仍可透過衛星通信與國內外保持聯繫。因此，該部計畫在政府指揮中心、22個縣市政府、3個國外站點、700餘個重要基礎設施場域（如學校、醫院等）、70餘個偏遠地區基站建置非同步軌道衛星(Non-synchronous Orbital Satellites)通信平臺，作為陸地網路中斷時的備援，確保政府緊急通信與重要服務，提高網路抗破壞與恢復能力，並且提供視訊會議、網路電話、直播系統等政府緊急通信需求，以及部分民眾寬頻上網等服務。非同步軌道衛星具有頻寬大、成本低、涵蓋廣、抗干擾的優勢，未來若能根據實際需求，逐步擴增站點數量，提升傳輸內容容量，即具有強化政府指揮體系緊急通信能力，維持重要節點的基本網路服務等網路數位韌性效益。[43]

進一步審視這項通信網路新興科技的運用與發展，其強化我國通訊網路的數位韌性，不僅包括本島、外（離）島，還將涵蓋偏遠地區，這將有效提升通訊網路在面對各種突發情況時的抗壓能力。其次，這項計畫的實施亦能提升應急或戰時政府指揮體系間訊息傳遞的韌性，確保快速、有效地傳遞命令和訊息。特別是在維持一定的國際通訊量能以及有效傳遞訊息方面，將有助於政府安定民心，凝聚社會向心力，對於維護國家安定具有重要意義，值得納入政府、國軍、民間單位共同參與合作與推動。

伍、結　　論

在當前複雜多變的安全環境中，保障關鍵資訊基礎設施的安全運行不僅關係著國家經濟發展和社會穩定，更是國家安全和防禦能力的關鍵所在。本文聚焦於我國在全民防衛動員準備體制下，關鍵資訊基礎設施在平戰時期轉換與運用的重要性。特別是藉由對我國政府、國軍、民間單位三方面在法規制

定單位及人員辦理動員準備業務」。見〈全民防衛動員準備法〉，《全國法規資料庫》，2019年6月19日，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=F0070013&kw=全民防衛動員準備法〉（檢索日期：2023年12月2日）

42 數位發展部，〈應變或戰時應用新興科技強化通訊網路數位韌性計畫〉，《行政院》，2022年8月，<https://www.ey.gov.tw/File/25AFCB901E407DD2>（檢索日期：2023年12月2日）

43 黃晶琳，〈低軌衛星台鏈，商機爆發〉，《經濟日報》，2023年11月20日，版A1。

定與實務運作的觀察，並且借鏡美歐國家對於基礎設施安全防護、平戰結合運作的制度性作法，更凸顯出聯防機制、平戰結合、統籌協調是平時做好設施防護、戰時實現無縫轉換的前提要件。

首先，關鍵資訊基礎設施作為現代國家發展系統的核心，其穩定運作與國家安全息息相關。無論是有線、無線資通網路系統、衛星通信，還是廣播電視，這些都是現代社會運作的關鍵元素。在平時，這些基礎設施的穩定運作對於確保政府和社會秩序尤為重要。而在戰時或緊急危難發生時，通信和資訊傳輸的速度、效能和準確性更直接影響到任務遂行的結果。基此，政府、國軍和民間單位之間的緊密合作和協調，是實現關鍵資訊基礎設施在全民防衛動員準備制度下平戰轉換運用的關鍵。

其次，在關鍵資訊基礎設施的平戰轉換和運用方面，我國可以借鏡美國的作法，建立國軍、政府與民間的協力夥伴關係，加強關鍵資訊基礎設施資訊共享和共同負責機制。透過彼此緊密合作、協調一致，共同建立有效能的跨部門、跨體系運作模式，並且持續完善與制定相應的政策和規範，方能在平時確保關鍵資訊基礎設施的安全，在戰時能夠順利地進行資通訊基礎設施的平戰轉換運用，進而在全民防衛動員準備機制中發揮重要作用，保障國家安全。

第三，為解決現階段我國關鍵資訊基礎設施的平戰轉換問題，本研究認為必須應建立高效的「聯防機制」，包括政府、國軍、民間資通業者等跨部門合作，以應對日益複雜的安全挑戰。在「平戰結合」作法方面，則建議可參考歐盟在平時與戰時結合資訊化建設和網路空間防禦的作法。更重要的是必須持續強化中央政府機關、國軍、民間單位的統籌與協調機制，尤其是在全民防衛動員準備方面，各層級間的協調仍需深化。

全民防衛動員準備不僅僅是單一的應變措施，更是整個政府施政的一部分。各部門的動員方案包含了精神、人力、物資、經濟、財力、交通、衛生、科技等多方面的內容，並結合政府各項施政計畫。這種全面性的規劃有助於蓄積平時全民總體戰力，並在應急狀況中有效支援應處。其次，政府在應急或戰時必須有效地向公眾傳遞政策訊息，維護社會穩定，凝聚民眾向心力。因此，持續評估與投入關鍵基礎設施的建設工作，建立包括利用傳統媒體和社群媒體平臺等完善的公共訊息傳播體系，多管齊下，方能保障政府訊息能夠及時、準確地傳達給公眾，並迅速回應社會關切事項。

透過本篇論文研究，因深入探討我國現行全民防衛動員準備、關鍵資訊基礎設施防護業務之法規制度，進而瞭解在安全環境變動不定，平戰界線更加模糊的今天，我國必須重視和不斷精進相關機制運作的完備與效能。其中，包括攸關關鍵基礎設施正常運作之核心資訊、通信網路的韌性，皆屬完善動員體制的重中之重。

最後，通信網路的韌性、政府指揮體系的效能、國際聯繫的順暢、公共訊息傳播的迅速，這些要素不僅在平時彼此緊密聯繫，更在應急或戰時形成強大的協同作用。只有在整合思維下相互支持，我國才能建構更加強大、反應更迅速的全民防衛體系，以確保國家安全與人民福祉。

（收件：112年12月6日，接受：113年3月6日）

參考文獻

中文部分

專書

汪毓瑋，2021。《國土安全（下）》。臺北市：元照出版。

期刊論文

李彥璋，2022/9。〈國軍應對網路攻擊之法理框架〉，《國防雜誌》，第37卷第3期，頁55-74。

林正義，2020/12。〈美國與中共網路戰略及其對臺灣可能的影響〉，《國防雜誌》，第35卷第4期，頁23-52。

彭錦珍，2004/6。〈我國國防政策合法化之研究—以《國防法》制定為例〉，《復興崗學報》，第80期，頁131-168。

黃正芳，2012/3。〈建構我國國土安全五大應變體系國土安全網之探討〉，《國防雜誌》，第27卷第2期，頁3-26。

樊國楨、韓宜蓁，2015/7。〈美國關鍵基礎設施防護法案與資訊安全管理技術控制標準化〉，《國防雜誌》，第30卷第4期，頁97-122。

官方文件

2013/12/11。〈電信法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0060001&kw=電信法。

2016/10/19。〈衛星廣播電視法施行細則〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=P0050014&kw=衛星廣播電視法施行細則。

2016/11/9。〈通訊傳播基本法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=P0010005&kw=通訊傳播基本法。

2018/5/18。〈國家關鍵基礎設施安全防護指導綱要〉，《行政院國土安全政策會報》，https://ohs.ey.gov.tw/File/F31BBE04AD8B9E98。

2018/6/6。〈資通安全管理法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297。

2019/6/19。〈全民防衛動員準備法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=F0070013&kw=全民防衛動員準備法。

2021/2。〈國家資通安全發展方案(110年至113年)〉，《行政院國家資通安全會報》，https://cc.ncku.edu.tw/var/file/2/1002/img/1302/776559884.pdf。

2022/5/18。〈衛星廣播電視法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=P0050013&kw=衛星廣播電視法。

2022/5/4。〈國家通訊傳播委員會組織法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=P0000008&kw=國家通訊傳播委員會組織法。

2022/8。數位發展部，〈應變或戰時應用新興科技強化通訊網路數位韌性計畫〉，《行政院》，https://www.ey.gov.tw/File/25AFCB901E407DD2。

2023/1/10。〈強化全民國防兵力結構調

整方案說明〉，《中華民國國防部》，https://www.mnd.gov.tw/Publish.aspx?u=NewUpload/202301/強化全民國防兵力結構調整方案-詳細說明_582413.pdf&fid=43404。

2023/6/12。〈建置臺灣民間自主緊急應變隊中程計畫（113年至118年）〉，《內政部消防署》，https://www.nfa.gov.tw/cht/index.php?act=download&ids=18117。

2023/6/28。〈電信管理法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0060111&kw=電信管理法。

2023/7/27。〈無線電頻率使用管理辦法〉，《全國法規資料庫》，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=K0060123。

中華民國110年國防報告書編纂委員會，2021。《中華民國110年全民國防報告書》。臺北市：國防部。

中華民國112年國防報告書編纂委員會，2023。《中華民國112年全民國防報告書》。臺北市：國防部。

行政院科技顧問組，2011。《關鍵資訊基礎建設保護政策指引》。臺北市：行政院。

報紙

徐子苓，2022/8/27。〈數發部成立！一文看懂成立背景、政策目標〉，《自由時報》，https://ec.ltn.com.tw/article/breakingnews/4039483。

黃晶琳，2023/11/20。〈低軌衛星台鏈，商機爆發〉，《經濟日報》，版A1。

黃琮淵，2023/3/30。〈NCC擬修法，破壞海纜致災最重罰1億元，近5年故障中斷逾20次〉，《中時新聞網》，https://www.chinatimes.com/newspapers/20230330000467-260110?chdtv。

網際網路

2006/3/21。〈全民防衛動員準備機制介紹〉，《嘉義市政府警察局第二分局》，https://wn1.ccpb.gov.tw/download/index.php?mode=dl_file&data_id=75&file_rename=5rCR6ZiyNl8xNzA2MDYwNjU5MDM= doc。

周力行，2023/7/26。〈第三作戰區關鍵基礎設施防護演練，蔡總統：共同提升臺灣耐災韌性〉，《軍聞社》，https://mna.gpwb.gov.tw/news/detail/?UserKey=872b33b4-5853-4d78-82a2-f96 e56e08401。

郭憲鐘，2001/1/1。〈全民防衛動員準備法相關問題之研析〉，《立法院》，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6586&pid=84257。

外文部分

專書

Brackup, Julia, Sarah Harting, Daniel Gonzales, Brandon Corbin, 2023. *Alternative Futures for Digital Infrastructure Insights and Considerations for the Department of Defense*. Santa Monica, CA: RAND Corporation.

Kramer, Franklin D., Robert J. Butler, 2019. *Cybersecurity: Changing the Model*. Washington D.C.: Atlantic Council.

官方文件

2021/10/7. "European Parliament Resolution of 7 October 2021 on the State of EU Cyber Defence Capabilities," *European Commission*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0412_EN.html

2022/1/27. "Critical Infrastructure Information Act," *U.S. Department of Homeland Security*, https://www.dhs.gov/sites/default/files/publications/CII-Act_508_0.pdf

2022/7/27. "Guidance on Sharing Cyber Incident Information," *Cybersecurity and Infrastructure Security Agency*, https://cisa.gov/sites/default/files/publications/Sharing_Cyber_Event_Information_Fact_Sheet_FINAL_v4.pdf

2022/8/18. "Presidential Directives," *U.S. Department of Homeland Security*, https://www.dhs.gov/presidential-directives

2022/9/1. "Homeland Security Act of 2002," *U.S. Department of Homeland Security*, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf

2023/11/17. "DOD Announces Release of 2023 Strategy for Operations in the Information Environment," *U.S. Department of Defense*, https://www.defense.gov/News/Releases/Release/Article/3592788/dod-announces-release-of-2023-strategy-for-operations-in-the-information-enviro/

2023/6/9. "EU-NATO Task Force on the Resilience of Critical Infrastructure," *European Commission*, https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf

European Defence Agency, 2023/11/14. *The 2023 EU Capability Development Priorities*, https://eda.europa.eu/docs/default-source/events/eden/phase-iii/factsheets/cdp-factsheet---eda---14-nov-2023.pdf

報紙

Pottinger, Matt, David Feith, 2021/11/30. "The Most Powerful Data Broker in the World is Winning the War Against the U.S.," *The New York Times*, https://www.nytimes.com/2021/11/30/opinion/xi-jinping-china-us-data-war.html

網際網路

2023/11/9. "Parsons Awarded $91 Million Cyber Capabilities Contract," *Parsons Corporation*, https://www.parsons.com/2023/11/parsons-awarded-91-million-cyber-capabilities-contract/

Gosselin-Malo, Elisabeth, 2023/12/1. "NATO Deepens Cyber Coalition with Asian Partners," *C4ISRNET*, https://www.c4isrnet.com/cyber/2023/12/01/nato-deepens-cyber-coalition-with-asian-partners/