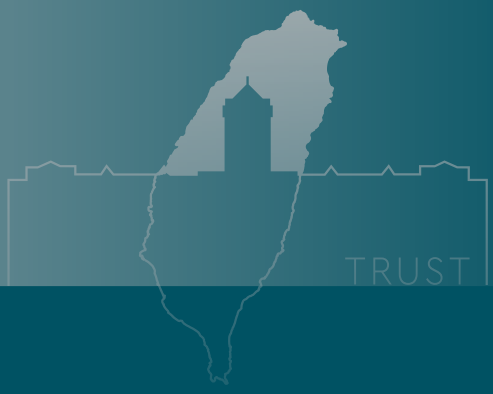
國家資通安全戰略2025
資安即國安

打造堅韌、安全、可信賴的智慧國家



國家安全會議 國家資通安全辦公室

2025年4月

國家資通安全戰略 2025 ——資安即國安

序

從近年來武漢肺炎疫情、俄烏戰爭、地緣政治衝突、美中貿易衝突及科技封鎖等全球重大事件的歷程和內容顯示，民主自由安全和資訊科技發展應用正走到關鍵的路口，無論對全球民主陣營和台灣都是重大危機與轉機。在多變的全球局勢中，數位領域的戰爭早已開始。世界上只有少數國家運用科技的方式與普世價值背道而馳，資訊科技被國家力量動員在內部運用於監控威脅人民，對外則用來攻擊侵犯其他國家主權，意圖癱瘓民主政府機關和基礎設施的正常運作，竊取國家機密及企業的智慧財產技術，奪取個人金錢資產，窺探並記錄個人隱私，進而發動複合型認知作戰，用冠冕堂皇的話術包裝顛倒是非的論述，輔以 AI 產製的影音圖文，混淆是非善惡認知，製造社會混亂與衝突對立。

台灣是自由民主繁榮的最佳典範，然而，自由和國家安全緊密相倚，國家安全根基搖搖欲墜的自由是脆弱的，對資安的無知與輕忽更是最大的國安風險，邪惡境外勢力正在利用國人的善良和珍惜自由的價值觀，在沒有硝煙和流血的數位戰場中侵門踏戶，我們人人都身在其中。儘管多年來政府在推動資安上不斷努力，遺憾的是，隨著科技快速演進造成資安威脅形勢更加嚴峻，透過現有制度、組織、法律、規範已難以防範應對各類新興的資安問題，而無視、躊躇、退縮、姑息只會送出錯誤的訊息。漸進式的改變已難以因應迫切的危機，在此重要時刻，全球民主陣營先進國家紛紛提出新的戰略規劃和組織規

範，動員產業、企業和公民整體力量協力合作以全面增強資安力量，《國家資通安全戰略 2025》的制定即植基於此，真正的威脅會在我們輕忽的時候來臨，只有預先做好充分準備才能嚇阻和遏止邪惡的擴張。

維護自由和安全的代價是必要的，《國家資通安全戰略 2025》中「全社會防衛韌性」、「國土防衛與關鍵基礎設施」、「關鍵產業與供應鏈」和「人工智慧應用與安全」四大支柱的制定，不只是為了進一步提升資安及國安能量，保護國人所珍視的民主自由安定繁榮，更是為了捍衛下一代的福祉，政府的作為至為重要。因此，必須敦促所有在政府機關、事業機構和設施的同僚更加勇於任事，積極貫徹實施執行；加強資安的規範不是對自由的管制，而是民眾自由與安全的護盾，確保數位國土安全的支柱。此外，在政府窮盡人才與科技來提升資安和國安實力之際，我們也必須提示國人，任何武器都不會比國民具備正確的資安意識更有效。個人和企業在生活上、營運中加強自我安全保護意識，就是增加國家打擊邪惡勢力的力量；網路上每一個人透過驗證、查證、提醒、拒絕和自制的對抗，都有助於提升資安國力來贏得每一場勝利。例如企業持續強化資安治理和營運韌性，不隨意使用有疑慮的資通訊產品裝置，個人不提供個資登錄並輕信有疑慮的社群媒體和軟體 APP，不散佈虛假訊息，不貪圖便宜和便利在有洩漏個資和足跡的網站購物。所有國人，請幫助身邊長輩、教育子女、提醒朋友，讓資安成為生活的重要議題，將自我防護意識內化成生活習慣，

進而形塑整個社會重視資訊安全的文化，這正是強化全社會防衛韌性的核心精神之一。

做為全球民主供應鏈的極重要一環，站在民主防線的最前緣，台灣一直是境外勢力意圖滲透攻擊的首要目標，資安措施與能量是先進民主戰略夥伴關心的焦點，同時也正是發展資安產業的最好機會；因此，我們要勉勵國人關切但不慌亂，小心而不懼怕；資安攸關個人身家財產甚至生命安全，必須要有正確敵我認知，不要讓蓄意破壞安定自由的勢力得逞，動搖我們的信念。《國家資通安全戰略 2025》不僅是全面規劃部署國家社會更前瞻資安作為、落實與全球民主先進國家戰略夥伴共同合作來對抗現今的邪惡威脅勢力，更是為了確保國家、社會、產業和每一個人安全的未來。維護全體國人最珍視的自由繁榮開放且安全的價值，正是國安的真正目的，也是維護資安的意義，今天就是開始。

總統 賴清德

2025 年 3 月 28 日

目次

前言——漸進式改變難以應對迫切危機

背景

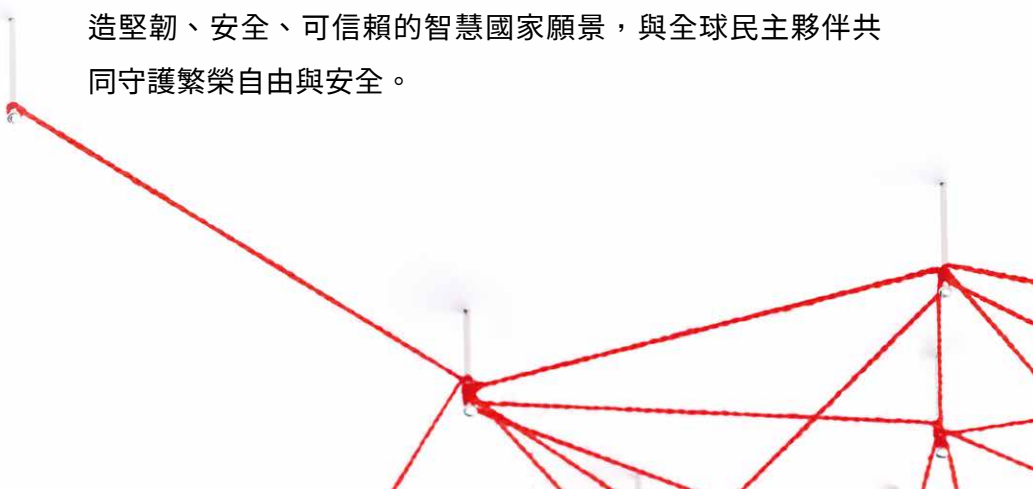
隨著全球數位化程度加深、新興科技逐漸普及，資通訊安全（以下簡稱資安）已位列全球前十重大風險（世界經濟論壇 World Economic Forum 2024），並成為國家安全的關鍵環節。對資通訊系統的駭侵與攻擊不僅構成國安重大威脅，也呈現出灰色地帶衝突的特徵，持續對區域和平與穩定造成挑戰。

2022 年俄烏戰爭爆發，針對關鍵基礎設施的網路攻擊成為大規模實體軍事行動的前奏。同年，時任美國眾議院議長的裴洛西（Nancy Pelosi）女士訪台，導致全台公私部門遭受網路侵擾；駭客藉由電子看板散播恫嚇言論，也試圖癱瘓各項應用服務，凸顯出資安防護對維護國家社會正常運作的重要性。2023 年，微軟公司揭露代號伏特颱風（Volt Typhoon）的國家支持型駭客組織，企圖掌控關島的關鍵基礎設施，其背後的意圖引發美國高度警戒。2024 年，美國再度揭露代號鹽颱風（Salt Typhoon）的駭客組織，入侵全美至少 9 家電信業者，企圖監聽時任總統候選人的川普（Donald Trump）等高層政治人物，並竊取國安資料。同年中東地區發生的呼叫器及對講機遙控爆炸，以及資安業者 CrowdStrike 的軟體更新意外導致全球數百萬台電腦當機等事件，暴露出高度複雜且相互依賴的資訊通信供應鏈所潛藏的風險。另一方面，人工智慧（Artificial Intelligence, AI）的急速發展，不僅帶來各類創新應用，也顯著加重了 AI 驅動的資安威脅。這些威脅包括透過自動化技術提高攻擊效率並

擴大攻擊規模、利用生成式 AI 製造更擬真的影音、圖像與文字內容迷惑目標或進行社交工程攻擊；甚至 AI 系統自身的弱點，也成為駭客鎖定的新興目標，帶來前所未有的風險。至於發展中的量子運算，其強大的運算能力將在未來對目前廣泛運用的公鑰密碼技術構成致命威脅，進而可能導致大規模的國家機密外洩與個人隱私暴露。這些案例與新興科技發展趨勢在在顯示「資安即國安」的本質與威脅的急迫性。

現今，中國在網際空間的各種行動正引發國際社會高度戒備。根據資安業者的分析報告與媒體揭露的訊息推估，來自中國的網路攻擊活動已遍布全世界。美國、英國、日本等國，都相繼傳出關鍵基礎設施與研究機構遭到鎖定與滲透的消息。這些行為不僅威脅區域安全，更挑戰全球秩序，印證了資安威脅無國界且不受現有法制架構約束的特徵。而我國所面臨的威脅尤其嚴重，國家安全局在「2024 年中共網駭手法分析」中指出：我政府網際服務網去（2024）年每日平均侵擾數為 240 萬次，較 2023 年日平均侵擾數 120 萬次增加逾 2 倍。其中多數為中共網軍所為，雖多已有效偵阻，惟仍凸顯整體網駭侵擾態勢愈趨嚴峻。另國安情報團隊去年掌握我國政府及民間網駭案件計 906 案，相較 2023 年 752 案，增長比率逾二成，其中以政府機關比率最高，占整體總數逾八成。經分析中共網軍駭攻目標，以通訊傳播領域（主要為電信業）、交通及國防供應鏈增長最為顯著，顯見該等領域已成為中共新興網駭重點。

基於各類資通安全威脅日益嚴重，2018 年國家安全會議（以下簡稱國安會）提出我國首部資安戰略報告《國家資通安全戰略報告——資安即國安》（以下簡稱資安即國安戰略 1.0），促成行政院資通安全處的成立及《資通安全管理法》的頒布實施；資安即國安戰略 1.0 著重於對內凝聚政府政策推動能量，對外倡議資安政策與促進國際合作。2021 年國安會推出資安即國安戰略 2.0，強化公私協力、提升防護韌性，並建構主動式防禦能量、擴大國際合作；同時，促成數位發展部成立，建構緊密合作的六塊基礎聯防體系。而隨著全球局勢變遷與新興科技發展，各類資安威脅與風險急速增長，民主夥伴國家紛紛投注更多資源，並加速調整政府組織與培育人才積極應對；我國位處地緣政治樞紐，所面臨的國家級駭侵情勢更加嚴峻，漸進式改變已難以應對迫切危機，亟需全面變革，大幅提升資安防衛能量與韌性，才能守護國家民主自由和產業繁榮的成果。爰此，國安會為更確保並強化國家安全，在既有基礎上提出《國家資通安全戰略 2025》規劃，扣合賴總統國家希望工程「創新經濟·智慧國家」的願景，推動五大信賴產業及全社會防衛韌性建設，希冀以前瞻思維打造堅韌、安全、可信賴的智慧國家願景，與全球民主夥伴共同守護繁榮自由與安全。



▼

威脅情勢與問題探討（如圖 1 所示）

㈠ 急遽升高的外部威脅

首先是國家級的資安威脅。國家支持的駭客組織所造成之威脅與日俱增，關鍵基礎設施與政府單位則是被鎖定的主要目標。這些駭客組織資源豐富、手段縝密、善於隱藏，且往往利用資通訊供應鏈入侵，大幅提升偵測與防禦的難度。他們通常長期潛伏在受駭者的網路環境中，伺機竊取敏感資訊，並等待適當時機展開進一步行動；例如在特定時間點外洩機密資料並引導媒體報導，以打擊政府威信。

其次是新興科技的挑戰。AI 技術的快速發展，正深刻影響資安格局。AI 的強大運算與分析能力，使駭客能更快速發現資安弱點、自動化攻擊流程，甚至生成高仿真釣魚郵件與社交工程手段，突破傳統防禦機制。另一方面，儘管量子電腦尚未商用，但其潛在的運算能力將顛覆現有的加密技術。未來，量子運算可能輕易破解目前廣泛使用的公鑰加密演算法，導致通訊系統、金融交易及國家機密的安全性面臨前所未有的挑戰。隨著技術競賽加劇，未來如何應對 AI 驅動的智慧攻擊與量子運算威脅，已成為全球資安戰略中的核心課題。

第三是網路犯罪持續猖獗。網路犯罪活動對個人、企業及國家安全構成多重威脅。尤其是勒索軟體攻擊屢屢升級，駭客將受害者的重要資料加密後索取巨額贖金，甚至威脅公開敏感資訊，造成巨大的經濟損失與信任危機。同時，網路詐騙手法層出不窮，從假冒企業電郵到釣魚網站，駭取個人

隱私資料。更令人關注的是智財間諜活動，駭客組織滲透企業與研發機構，竊取關鍵技術等營業秘密，對產業競爭力與國家利益造成難以估算的損害。

㈡ 亟待解決的內部挑戰

資安應變的目標、能力與韌性必須不斷提升。《資通安全管理法》推行至今，公部門及關鍵基礎設施已建立一定的防護基礎，但在面對日益複雜的威脅時，仍需投入更多資源強化防護與持續運作之韌性；事前盤點與防護、事中通報與應變、事後改善與情資分享等法遵與資安治理措施，更須全面落實。此外，為有效應對涉及國家安全的重大資安議題，跨部會的統籌協調與協同作業機制需要持續優化，確保資安應變能更具韌性與效率。

再者，隨著我國與戰略夥伴之間的鏈結與互通需求持續升高，資安已成為穩固合作基礎的關鍵要素。有效保護資料外洩、防範內部威脅、精進人員安全查核，以及建立政府部門間安全且可信任的通聯管道，都是不可忽視的重要議題。而透過與國際公私部門夥伴的合作，精進資安情資的分享與應用，能進一步強化我國資安防護能力，為深化戰略夥伴關係提供堅實保障。

最後，主動防禦亦是資安防護的核心策略。主動防禦目的在於提高駭客入侵成本，達到有效嚇阻效果，相關的措施包括透過資料蒐集與情資分析預先阻絕攻擊，結合持續威

脅狩獵（Threat Hunting）主動識別潛藏在網路深處的進階式威脅；透過追蹤溯源的技術、公私協力與國際合作，揭露駭侵手法及來源，對駭客進行歸因與究責；並視事件嚴重程度，及時採取必要的作為與措施。全面落實主動防禦，需要明確的戰略目標、專業的技術能力，以及充足的資源投入。主動防禦的落實，不僅是當前應對資安威脅的關鍵，更是未來數位韌性的基石。

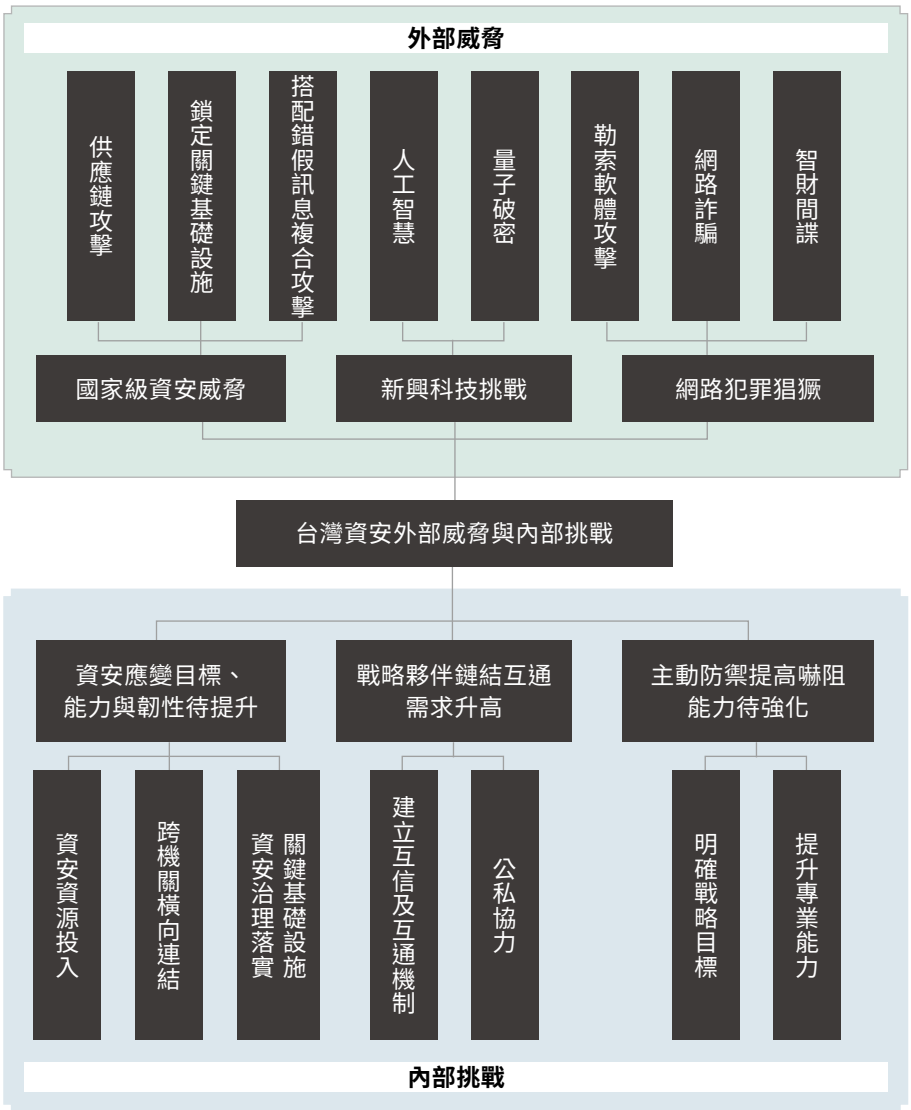


圖 1、台灣資安外部威脅與內部挑戰

▼

戰略構想

㈠ 國家前瞻發展需求

本戰略規劃與當前政府施政方針一致。賴總統在就職演說中特別強調，面對中國的各種威脅滲透，必須展現守護國家的決心，提升全民保家衛國的意識，健全國安法制，強化民主韌性。在經濟上將全面推動半導體、人工智慧、軍工、安控、次世代通訊五大信賴產業。賴總統並於就職滿月記者會進一步宣布成立「全社會防衛韌性委員會」，不僅推動擴大民力的訓練與運用，還涵蓋能源及關鍵基礎設施的安全，以及資通、運輸及金融網絡的穩定，以強化國防、民生、災防、民主四大韌性，打造強而有力的民主社會，全面守護國家安全。

此外，台灣是全球民主供應鏈的關鍵，必須促進產業 AI 化，運用 AI 來提升國力與軍力。行政院卓榮泰院長在施政報告中，亦揭示國家希望工程內容，包含創新經濟，智慧國家；打造韌性台灣，維護安全與和平。

㈡ 前期戰略延續性

對應《資通安全管理法》頒布實施、資通電軍指揮部及數位發展部的相繼成立，自 2018 年由國安會提出資安即國安戰略 1.0 與資安鐵三角機制，到 2021 年接續的資安即國安戰略 2.0 與六塊基礎聯防機制，都為維護國家資通訊安全提出前瞻戰略規劃，並建立一套統合網路情勢監控、資安事件應處及情資分享的國安聯防體系。

如今，在前期建立的堅實基礎與架構上，為因應日新月異的資安威脅，有必要投入更多資源，提升資安戰備能力，並加入全社會與重要關鍵產業共同防衛的思維。以持續實現打造堅韌、安全、可信賴的智慧國家願景。

㈢ 因應全球局勢與前瞻科技發展布局

世界經濟論壇《2024 全球風險報告》揭示全球風險與危機仍在持續升高，網路的不安全性、誤導資訊和錯假訊息、國際衝突等問題高居未來十年內全球風險的前列。俄烏戰爭、美中競爭推升了地緣政治不穩定性，而科技進步與 AI 發展也使得資安威脅隨之升級，資安即國安戰略必須隨著各種風險升高加強因應布局。

㈣ 資安是與戰略夥伴合作的基盤

台灣是「世界和平第一關的守衛」[1]，也是民主陣營最重要的防線，與先進戰略夥伴的協力合作至關重要。資通訊安全防護的戰略思維必須與先進戰略夥伴接軌同步，國防、政府機關與關鍵基礎設施的防護計畫、作為、系統設備及教育訓練等，也必須達到與先進戰略夥伴互通的標準，並與先進戰略夥伴的前瞻規劃與作為對焦，更加落實執行，才能提升互信，維繫緊密合作關係。

㈤ 各國威脅評估與網路戰略趨勢

本戰略在規劃過程中，除應對全球資安威脅的發展趨勢外，亦參考各國相關戰略、政策及法規，以確保其前瞻性並與國際接軌。以美國為例，在《2023 年國家資通安全

[1] 蔣渭水〈臨床講義〉。

戰略（National Cybersecurity Strategy）》中主張建立更安全、具韌性且符合美國與其盟友價值觀的網際空間，並強調將資安責任重新分配到更具能力的單位（如大型企業、供應商及雲端業者），而非讓中小企業與終端使用者承擔過多風險；同時，調整誘因促進長期資安投資，以建構更具防禦性與韌性的未來數位生態系統。因此，美國戰略提出五大戰略支柱，包括透過聯合網際防禦協作機制（Joint Cyber Defense Collaborative）等公私協力方式，強化基礎設施資安防禦能力；透過執法、經濟制裁及國際合作，全面打擊並瓦解資安威脅行為者；透過立法規範，確保供應商落實安全設計（Secure by Design, SbD）原則，包括對物聯網（IoT）設備設定強制性安全要求、更安全的軟體開發標準，並提升軟體供應鏈透明度；投資研發先進資安技術，包含 AI、工控系統（Industrial Control System）、雲端、後量子密碼（Post-Quantum Cryptography）與推動導入零信任架構（Zero Trust Architecture, ZTA）；以及深化國際夥伴關係等。

2025 年美國前總統拜登（Joe Biden）發布《加強和促進國家資通安全創新行政命令（Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity, EO 14144）》，進一步指名所有對美國的資安威脅中，以中國最為活躍與持續。2025 年甫就職的川普總統更提出五項資安優先事項，包括：強化政府資安；推動公私合作協同應對跨國網路犯罪及國家級威脅；重點防護電力、

交通、金融等關鍵基礎設施網路，並加強監管，確保遭遇攻擊後能迅速恢復；強化與盟國和國際組織合作，提升全球資安防禦協同作戰能力；以及提供資金援助及政策支持，鼓勵企業與研究機構開發先進的資安技術。

英國的《2022 年國家資安戰略（National Cyber Strategy 2022）》則圍繞五大策略目標：首先，強化全國網路生態系統，通過政府、學界與產業合作，培養多元化的網路專業人才並支持創新產業；其次，建立具韌性且繁榮的數位國家，降低網路風險，提升企業與公民的資通安全意識與防護能力；第三，領先發展關鍵網路技術，推進國家在科技競爭中的優勢，確保關鍵技術與基礎設施的安全性；第四，增強國際領導力，推動全球網路治理，促進自由、開放且安全的網際空間，同時加強國際夥伴的資安防禦能力；最後，偵測、打擊與遏制威脅行為，利用全方位手段保護國家安全，並在網際空間應對國家級網路攻擊與犯罪。另一方面，官方亦指出 2021 年最常見的資安威脅來自俄羅斯和中國。英國政府並認為，中國具備高度網路技術能力，且對英國的技術與商業機密展現高度興趣。英國評估，在未來十年內，中國的數位發展與全球影響力將是英國強化資安防護的重要考量因素之一。

澳洲於《2023-2030 資通安全戰略（2023-2030 Australian Cyber Security Strategy）》提出將以 2030 年成為全球資安領導者為目標，藉由六大「網路盾牌（Cyber

Shields)」保護公民與企業免受資安威脅，並強化韌性以快速因應與復原；實質內容包括強化公民與企業的防護能力、推動安全技術發展、建立世界級的威脅資訊共享與阻擋機制、保護關鍵基礎設施、發展本土資安能力與專業人才，以及提升地區和國際網路韌性與領先地位。該戰略透過三個階段實施：2023-2025 年鞏固基礎、2026-2028 年提升整體網路成熟度、2029-2030 年引領全球網路技術發展，同時推動公私協作與立法改革以實現願景。

歐盟自《網路與資訊系統安全指令（Network and Information Systems Directive 2, NIS2 Directive)》於 2023 年 1 月生效以來，持續加強其資安架構，推出多項重大法案與修訂，旨在應對日益複雜的資安威脅環境。NIS2 Directive 拓展了資安規範的適用範圍，強化關鍵基礎設施和重要部門的安全標準，並要求成員國提升通報機制和事件應變能力。《網路韌性法（Cyber Resilience Act)》則聚焦於數位產品的全生命週期安全，要求製造商對其產品的安全性負責，並確保弱點修復和軟體更新。《網路團結法（Cyber Solidarity Act)》倡導歐盟層級的威脅情報共享與跨境應變支援，強調成員國之間的合作以應對重大資安事件。而修訂版《資通安全法（Cybersecurity Act)》強化歐盟資通安全局（ENISA）的職能，並推動統一的資安標準認證架構，提升資通訊產品的可信度與安全性。此外，《人工智慧法（AI Act)》為全球首部專門針對 AI 技術風險的立法，對 AI 系統進行分級管理，確保

高風險應用符合透明、問責與安全的要求。這些措施共同構成了歐盟全面且協調的資通安全與數位治理體系，為未來的數位轉型與網路韌性奠定堅實基礎。

綜前所述，國家級威脅日增，且與地緣政治的發展形勢緊密相關，各國逐漸將其視為主要的國家安全挑戰。美國、英國、澳洲和歐盟等主要國家和國際組織的網路戰略均展現出一些共同趨勢：首先，這些戰略強調保護關鍵基礎設施的安全性與韌性，應對國家級威脅（特別是 APT 進階持續性威脅攻擊）[2] 的能力被視為重中之重。其次，面對 AI、量子運算等新興科技帶來的風險與機會，各國均投入資源加強技術研發和風險管理。第三，針對資通訊供應鏈及業者，各國陸續採取更嚴格的規範與責任要求，以確保整體網路生態系統的安全性與韌性。最後，國際合作和公私協力成為應對跨國資安威脅的關鍵，各國透過聯盟、合作架構和威脅情資共享等方式，建立聯防機制，共同應對國家級威脅的挑戰，推動全球資安的協同作戰能力。這些舉措顯示，各國正在加速建構更全面且具韌性的資安體系，以應對日益複雜的資安威脅局勢。

[2] Advanced Persistent Threat，簡稱 APT，是一種進階持續的網路攻擊形式，通常針對特定對象以精密手法滲透並躲避偵測、長期潛伏。APT 常採階段式行動，包括滲透、建立後門、擴張權限、橫向移動與資料竊取等。其主要目的包含竊取敏感資料、破壞或中斷系統運作，常見於國家支持的駭客行動，但也可能由資源充足的網路犯罪組織發動。

重要內涵
國家資通安全戰略２０２５

《國家資通安全戰略 2025》將全面部署並強化包括「全社會防衛韌性」、「國土防衛與關鍵基礎設施」、「關鍵產業與供應鏈」、「人工智慧應用與安全」的「資安四大支柱」，以「堅實資安治理機制及防護」與「戰略夥伴鏈結」為跨支柱準則，奠定「國家資安戰情協同應變中心」與「國家資通安全會報及資訊資安預算正規化」兩大基石，並結合六塊基礎聯防體系、跨部會協防體系、民間產業、學、研公私協力與國際合作做為堅實基盤，以期達成「打造堅韌、安全、可信賴的智慧國家」的願景（如圖 2 所示）。茲分述如下：

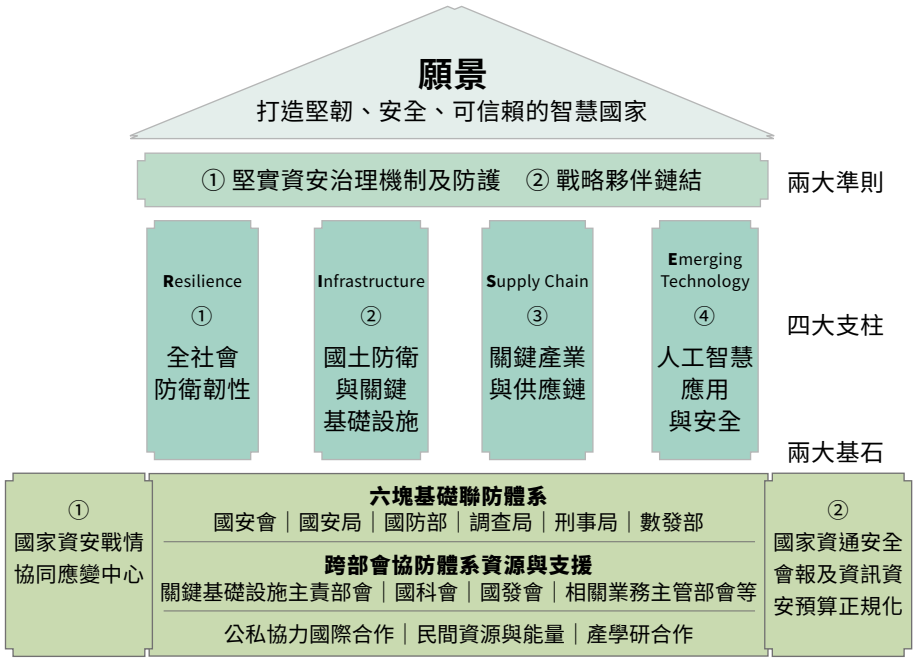


圖 2、國家資通安全戰略 2025 重要內涵

▼

跨支柱準則

㊀ 堅實資安治理機制及防護

資安治理是現代組織應對數位風險的基石。在美國國家標準暨技術研究院（NIST）於 2024 年正式推出的新版資通安全架構（NIST Cybersecurity Framework 2.0, CSF 2.0）中，特別新增「治理（Governance）」此一核心功能，以強調其在資安中的關鍵角色。治理的意涵在於建立清晰的政策與流程，確保資安目標與組織的業務需求相符，同時強化管理層的參與及責任。這不僅包括風險的識別與管理，也涵蓋資安文化的建立，確保從高層到基層都能有效落實資安措施。

此外，零信任架構（ZTA）已成為近年資安治理中不可或缺的一環。透過「絕不信任，永遠驗證」的理念，零信任架構要求對所有使用者、裝置與資源進行持續的身分驗證與授權，有效降低網路攻擊的影響範圍。

在瞬息萬變的威脅環境中，運作韌性則是資安治理的另一核心要素。韌性強調組織面對網路攻擊、運作中斷或其他不確定性時，能具備快速回應與復原能力。韌性的實現包括推動關鍵系統核心功能朝境外雲端備援轉型，加強基礎設施的異地備援與容錯設計，以及引導公私部門逐步過渡至後量子密碼技術，以因應未來其對加密技術的威脅。

因此，本戰略將「堅實資安治理機制及防護」列為跨支柱準則，從國家層次的高度推動組織落實資安治理、零信任架構導入及韌性強化。其主要目標為：

一、跨支柱推行零信任架構，強化公私部門機構的資通安全認知和文化。

二、落實資安治理，建立備援並有效保護公私部門資料。

三、發展後量子密碼之資安防護架構與管理，推動公私部門加速導入。

在關鍵策略做法上，首先，在加速各公部門及關鍵基礎設施落實全面資安治理與制度的過程中，應推動零信任架構的觀念，確保各單位對於資料處理、傳輸及儲存的安全性有更深刻的認知；從而擴大推動導入零信任架構，落實其三大核心原則——身分鑑別、設備鑑別及信任推斷，並協助公私部門機構訂定相應策略與執行方案，以建立更具韌性的安全機制。此外，必須發展驗證標準與指引，以確保零信任機制的有效性，並由公部門優先檢驗與調整，以提升整體防護能力。在產業發展方面，應積極輔導並促進資安零信任相關產業的成長，鼓勵更多解決方案的研發與應用，進而擴大引入創新技術來強化資安防護能力。

與此同時，應深化與國內外雲端服務業者的合作，擴大跨領域建立境外資料備份及核心功能備援，確保在面臨重大資安事件或災害時，政府與企業仍能維持關鍵業務運作。並應持續盤點、更新及修正數位治理及跨境（雲端）傳輸法規，以支援公私部門加速建立備援機制，確保關鍵資料的可用性。

而為強化資料保護及防範內部威脅，應制定相應政策法規並投注必要資源，確保機敏資訊得到適當保護；檢視現行資料加密相關法規與通訊傳輸設定，持續投入資源以落實資料加密儲存與安全傳輸，降低敏感資訊外洩或被竊取的風險。另隨著量子電腦技術的發展，傳統加密技術面臨破解風險，因此應透過產學研合作，推動公私部門重新檢視並調整現有資安架構，導入後量子密碼技術，以確保未來的資料保護機制仍具備長期的安全性與可靠性。

㈡ 戰略夥伴鏈結

國際合作是強化國家資安不可或缺的關鍵。資安威脅無國界，駭客組織與網路犯罪集團精於利用跳板、匿蹤網路與資通訊供應鏈進行滲透與攻擊，增加了在偵測、防禦與歸因上的挑戰。透過國際合作建立情資共享及聯防機制，可顯著提升對資安威脅的可視性，實現早期預警與快速應對；進一步推動事件歸因與共同究責，讓駭客組織及其行動透明化，從而提升其作業成本，達到有效嚇阻的效果。

資安合作不僅限於情資共享與聯防，更應包括協助其他國家提升資安能力。在全球經濟高度互賴的背景下，每個民主夥伴國家的資安能力提升，都能為整體防護提供助益。「幫助他人即是保護自己」的理念，正是資安國際合作的核心價值所在，並能為全球資安生態系建立更加堅實的基礎。

此外，資安是深化國際合作的根本，因為它是建立各國

互信的重要基石。面對地緣政治不穩定與對立升高的趨勢，各國必須攜手鞏固「民主供應鏈」，確保數位基礎設施與關鍵技術的安全性與韌性。台灣位於民主供應鏈的一環，且是全球資安的重要節點，更應積極參與資安國際合作，透過強化自身資安防護與技術創新，進一步成為區域與全球資安生態的核心貢獻者，發揮更大的守護效益。

準此，本戰略提出「戰略夥伴鏈結」作為另一跨支柱準則，主要目標如下：

一、以先進戰略夥伴為標竿，全面鞏固國防與政府戰備能力。

二、強化國際資安合作，擴大國際聯防。

三、協助戰略夥伴提升資安能量。

為達成前述目標，強化資安戰備互通性及可視性，具體策略做法為：強化與先進戰略夥伴的互信基礎，提升本戰略各支柱的資安戰備能力，使不同國家與組織間的協作更為順暢。而持續加強國際產官學交流，鼓勵國內資安團隊參與國際競賽與論壇，則有助於建立更緊密的事務性協作關係，不僅能促進經驗分享，還能擴大在全球資安領域的影響力。此外，應持續借鏡先進戰略夥伴的做法，推動民間資安人才與技術能力的蓄積，以強化整體資安實力。

在資料治理方面，應提升戰略夥伴間的資料互通分享機制，確保安全查核、實體安全、跨部門通聯機制及相關保密

作業規範皆符合對應的保密等級，厚植合作根基。同時，須強化與國際資安社群的鏈結，積極參與全球資安事務合作及演訓，藉此提升對境外資安情資的掌握度，強化聯防機制。並積極投入國際資安生態系的布局，爭取國際資源投入，進一步完善國內資安產業，確保與國際接軌。

最後，應持續透過主動分享資安防護、政策制定與推動的經驗，並積極協助戰略夥伴及友邦培育資安人才，提升其資安防護能力，深化雙邊與多邊的合作基礎。另為推動國內資安產業的國際化發展，須扶植本土企業，使其具備跨足國際市場的實力，並鏈結國際資源，使國內企業能夠前進全球市場，成為國際資安生態系的重要參與者，進而提升我國在全球資安領域的競爭力與影響力。

▼

四大支柱

支柱一：全社會防衛韌性

誠如賴總統揭示，「隨著全球疫情和俄烏戰爭的爆發，世界各國都在提升防衛韌性，包括北約或歐盟都制定了全社會韌性強化的指引。這顯示台灣並非特例，全社會防衛韌性是全球性的課題，而台灣持續提升全社會防衛韌性，也是國際社會的共同期待」。而資安正是全社會防衛韌性的重要組成，

特別是在數位時代，強化防護能力需要回歸以人為本的思維，其中包含兩個主要面向：一方面，資安是高度知識、技能與洞察力的結合，仰賴高階專業人才的投入，才能有效維護系統安全並驅動技術革新。另一方面，人始終是資安最大的風險來源。無論是因疏忽點擊惡意連結，還是因缺乏警覺而洩漏敏感訊息，都可能引發重大威脅。因此，持續的資安宣導，強化個人的資安意識至關重要，就像養成勤洗手、配戴口罩的防疫習慣一樣，簡單卻能有效降低病毒入侵威脅。而培養個人的警覺意識與網路使用習慣更有助於民眾面對錯假訊息和詐騙等複合式網路攻擊威脅。此外，全社會防衛韌性不僅仰賴個人層面的努力，更是一項公私協力的工作；政府與私部門需要攜手合作投注資源，共同建立一個具備韌性與防禦力的防護網絡，為數位時代的安全奠定堅實基礎。

本戰略因而將全社會防衛韌性作為第一支柱，主要目標為：

一、對應「全社會防衛韌性委員會」之成立，擴大民力的訓練與運用，厚實應變防禦量能。

二、提升全民資通安全與資料防護及辨識錯假訊息與認知作戰能力。

三、強化公私協力，完備資安防禦體系與韌性。

在擴大民力的訓練與運用方面，具體策略做法是優先建立資安菁英團隊，並與公協會、學會及相關機構合作，透

過定期交流、培訓與演練，確保資安專業人員之能力持續精進，提升整體防禦能量。並應積極擴大招攬國際資安人才，補足當前人才缺口，同時提升公部門及關鍵基礎設施領域的資訊資安人才待遇，以吸引並留任優秀專業人員。另一方面，應擴增公私部門間的資安人才流通管道及協力機制，促進跨領域資源共享，提升整體資安防禦效能。

在普及資安認知方面，則應提供台灣經濟骨幹各級企業完善的資安治理資源與基礎資安防護支援，協助企業建立完善的安全機制，以提升整體經濟體系的抗風險能力。為應對日益嚴重的網路犯罪與詐騙問題，則應推動公私協力及國際合作，加強對電商、社群平台等資料密集產業的安全監理，建立更完善的警戒、通報與查核機制，如數位鑑識與溯源技術的應用，確保相關風險能夠及時發現並迅速應對。亦應擴大推動兼顧便利性與隱私保護的個人身分辨識與驗證機制，以降低網路冒名詐騙的風險，提升線上交易與數位互動的可信度。

而為凝聚社會共識並推動資安發展，將定期召開全國資安高峰會議，凝聚共識、統合各界資安作為，及促進資安應用的發展與創新。同時，應落實公私部門的資安治理，事件應變與通報機制，以確保在面臨威脅時能有效應對。此外，落實盤點更新相關採購及預算法規，以營造更安全及有利的數位環境，支持產學研在前瞻技術的研發與應用，及確保資通訊產品在其生命週期內的安全性。

支柱二：國土防衛與關鍵基礎設施

關鍵基礎設施的資安至為重要，因為這些系統是維持社會運作的核心。油、水、電、通訊、交通、金融、醫療等基礎設施一旦遭受網路攻擊而中斷運作，不僅將導致社會停擺，對經濟活動、公共安全及人民生活造成難以估計的損害，還將進一步削弱國家的穩定性與公眾對政府的信任感。

在國防領域，資安的重要性體現在維護國軍作戰指揮與管控系統的安全性，確保設施設備、通訊與決策不受干擾。此外，資安能力更是國防戰略與作戰策略的重要延伸，國軍必須具備有效反制境外網路攻擊的能力，以防止敵方破壞國防系統、竊取敏感資料或癱瘓作戰能力。準此而言，資安是國土安全與國防效能的核心保障。

本戰略以「國土防衛及關鍵基礎設施」為第二支柱，主要目標包含：

一、全方位盤點國土防衛與關鍵基礎設施潛在資安風險並提出對策以強化關鍵基礎設施的安全及主動防禦能量。

二、落實資安治理，提升國防、民生、災防、民主四大領域資安防禦與韌性。

三、強化資安戰備，守護國家安全及區域和平穩定。

在具體策略做法上，首先應透過新設「國家資安戰情協同應變中心」全面掌握國家層級的資安風險，強化事件、人力的協同管理與應變機制，確保在面臨重大資安威脅時能迅速調集資源有效處置。再者，政府應明確制定資通安全戰備要求與戰略目標，涵蓋國防及執法部門，並集中資源提升情資蒐研、溯源及主動防禦能力，以建立更完善的資安戰備體系。同時，應全面盤點並列管重要機關組織與關鍵基礎設施的系統、網路及設備，依據風險等級進行分級分類，並建立定期檢視機制，確保管理、維護及升級規範的落實。為持續鞏固防禦能力，主管機關及中央目的事業主管機關應強化對關鍵基礎設施的監督責任，落實資安事件調查與課責機制，確保各單位對資安風險的應變能力達到既定標準。

在前述基礎上，國安與資安相關單位應與關鍵基礎設施的主責部會合作，在能源、通訊、交通、金融、醫療等領域的關鍵基礎設施分別制定並執行「資通安全行動方案」，強化其系統網路韌性。對於具系統相依性的關鍵基礎設施，尤應提高資安防禦規格，確保在極端狀況下仍能維持基本運作。另外，應將公部門及關鍵基礎設施的資訊資安經費正規化，加速資通訊設備的更新，以確保系統持續安全維運；並建立政府跨機關共同作業平台，重點強化緊急時期的運作韌性。

針對資安防禦能力的強化，則應成立專責資安防護團隊，透過定期培訓、演練來應對關鍵基礎設施突發事件，確保資安人員具備即時反應與解決問題能力。此外，應落實公

務機關、國防及關鍵基礎設施內部關鍵系統的技術檢測，並推動第三方資安實兵演練及桌上兵推，以測試及驗證資安防禦與應變機制。演練內容應涵蓋對資料外洩的因應措施，而桌上兵推則應由組織高階管理階層及資安長主導，確保決策層級對資安事件的應處能力得以提升，使政府及關鍵基礎設施提供者在面對各類資安威脅時能夠快速應變並有效防範，進一步強化台灣的國土安全與關鍵基礎設施防護能力。

支柱三：關鍵產業與供應鏈

國內包括五大信賴產業在內的關鍵產業是經濟繁榮發展的基礎，連同通訊、金融、醫療等維繫社會運作的核心服務產業，都需要確保資安、保護智慧財產並建立持續運作的韌性，因此對國家與經濟發展而言，關鍵產業及供應鏈安全都是資安防護的重點，特別是在供應鏈全球化的時代，防止各關鍵產業及其供應鏈遭受資安威脅侵害是維護國家與經濟利益的首要任務；對國際社會而言，強化關鍵產業資安更是鞏固「民主供應鏈」的重要環節，以確保全球合作基於安全可信賴的技術與產業生態。

此外，為了持續強化國內各關鍵產業及供應鏈的資安防護，扶植國內資安產業與新創企業的發展同樣重要。支持在地資安新創，不僅能提升自主技術能力，更能在國際間發揮關鍵影響力。資安產業的蓬勃發展，既能滿足本地需求，也能推動技術出口，促進產業升級，吸引更多資安人才的投入，為經濟帶來新的成長動能。唯有結合關鍵產業與供應鏈

資安推動及資安產業創新發展，國內的資安防護能力才能全面扎根，共同面對地緣政治與數位化的挑戰。爰此，本戰略的第三支柱為「關鍵產業與供應鏈」，主要目標為：

一、盤點並強化國內關鍵產業（如五大信賴產業及金融、通訊、醫療等資料密集產業）資通安全制度，鞏固民主供應鏈。

二、推動關鍵產業降低資通安全風險及持續營運管理（Business Continuity Management,BCM）。

三、擴大投資資訊資安產業並扶植新創。

為強化供應鏈安全，具體策略做法是與產業公協會及其領導企業合作，全面盤點關鍵產業、重要企業、供應鏈及其關鍵資源，建立風險管理清單，確保供應鏈的可視性與安全性。在此基礎上，亦應研擬符合各關鍵產業需求的「資通安全行動方案」，並逐步擴大推行範圍，以提升產業資安治理能力。此外，應完善政府採購及產品資安標章與認證制度，強化政府及關鍵產業供應鏈在軟硬體與服務等產品採購時的資安標準。透過健全的供應廠商及產品之標章與認證機制，確保供應鏈安全，並針對政府關鍵供應商及產品專案進行重點強化，從政府採購端優先降低供應鏈資安風險。

為提升關鍵產業的資安能力，則應促進企業之間的溝通交流，並透過定期人員培訓與重大弱點分享，提高資安意識與技術量能，確保資料安全。同時，鼓勵各關鍵產業及其供

應鏈（包括國防供應鏈），建立聯防機制，以強化資通安全的聯合防禦能力，強化整體應對資安威脅的韌性。另推動並落實關鍵產業企業的資安治理措施，並透過實兵演練來驗證企業的防禦與應變能力，確保其能有效應對資安事件。

在促進資安產業自主發展面向，應提升公私部門的資安規範要求，建立良性的資安產業發展環境。可透過定期審視並提供獎勵措施，如擴大資安投資之稅賦抵減項目（漏洞賞金計畫、接受第三方評鑑等）、強化政府採購契約要求及國內外資安業者評鑑等方式，促進企業強化資安治理，提升資安防護能力，進而帶動國內資安產業發展。此外，應擴大投資並輔導各類資訊資安新創企業，促進產業規模化與國際化發展，建立完整資安人力資源供需生態體系，強化台灣資安產業的競爭力，確保供應鏈在全球市場中的安全與韌性。

支柱四：人工智慧應用與安全

做為本戰略的第四支柱，人工智慧應用與安全的促進，應從技術、人才與制度三者並進。首先，政府須與民間攜手合作，投入更多資源研發 AI 資安技術與應用，共同應對新興科技快速演變的威脅；同時也須大規模培育資安與 AI 領域的專業人才，確保國內擁有足夠的技術與人力因應挑戰。建立並完善相關制度法規，有助於促進 AI 的安全應用與國際合作，將 AI 應用潛力最大化並降低相關風險。因此，本支柱的主要目標及策略做法涵蓋：

一、將 AI 技術應用於全社會防衛韌性、國土防衛與關鍵基礎設施、關鍵產業及供應鏈的資安防護，並打造產業生態系。

二、確保 AI 技術本身的安全性與可信任性。

為推動 AI 應用於資安領域並強化整體安全韌性，具體策略做法包括提升跨公私部門與產業在 AI 研發方面的合作，透過自動化資安治理與管理流程（如利用 AI 尋找弱點、提供問體解決方案），有效強化資通安全防禦能力。此外，可透過舉辦相關競賽的方式，促進技術研發與應用，鼓勵企業與研究機構投入資安 AI 技術的發展。同時，應建立資安科技園區，推動 AI 導入資安領域的相關計畫，增設育成機制，吸引國內外優秀資安企業與人才進駐，形成產業聚落，提升整體資安技術水準。

而為構建自主共榮且具競爭力的資安產業生態系，應以 AI 技術為核心，串聯資安產業上中下游資安服務廠商及資安需求端，包括關鍵產業、關鍵基礎設施及政府機關等，促使資安產業與市場需求緊密結合，建立良性循環，推動產業整體發展。在技術治理方面，應積極推動 AI 系統的安全設計（SbD）、安全性（Safety）及可信任性（Trustworthiness），確保 AI 技術從源頭即具備風險管理機制（Risk Management），降低潛在資安風險。

另一方面，應發展並接軌國際 AI 相關標準，鼓勵民間企業發展符合國際規範的合規技術，以奠定 AI 資安產業的長遠發展基礎。為確保 AI 技術的安全應用，應全面盤點現行法規，並推動人工智慧前瞻技術的普及與應用，發展完善的資安治理機制，確保在 AI 驅動的環境下仍能維持高標準的資通安全管理能力。尤其須強化對認知作戰及網路詐騙等風險的處置與追緝能力，以提升全社會的防衛韌性，確保 AI 技術發展不會成為資安風險的破口，而是成為提升安全性的關鍵動力。

▼

兩大基石

㈠ 建置國家資安戰情協同應變中心

為達成《國家資通安全戰略 2025》「打造堅韌、安全、可信賴的智慧國家」願景，鞏固四大支柱，應建置「國家資安戰情協同應變中心」，挹注充沛的經費人力等資源，以統合資安戰情之蒐集、分析、分享、聯防及重大資安事件之支援等協同作業。其重要任務包括：

一、製作國家資安風險地圖，以確實掌握國家層級資安風險。

二、擴大收攏全國公私部門、產業及國際資安監控情資，強化對資安威脅的可視性（Visibility）。

三、統籌並協處支援重大資安事件，訂定作業準則與工作規範，提升統合應變效能。

㈡ 強化國家資通安全會報及資訊資安預算正規化

強化現有行政院國家資通安全會報功能作為《國家資通安全戰略 2025》及政府資安事務的統籌督導角色，進一步活化會報職能，重要任務包括：

一、統籌督導跨部會資安事務，推動資安法規調適、並確實執行法遵事項。

二、確保政府機關及關鍵基礎設施具備充足資訊資安預算與人力編制，並考核部會及關鍵基礎設施資安防護的執行成效。

三、擴大納入私部門參與，促進公私協力。

▼

跨支柱基盤

㈠ 六塊基礎聯防體系《六塊基》

延續前期六塊基礎聯防體系，以國家安全為核心目標戰略，連結國家安全會議、國防部、國家安全局、調查局、刑事警察局、數位發展部六大機關，主要任務為確保資通訊安全相關基礎防護作為之規劃、執行與管理。其中，軍事部門資安與主動防禦由國防部主責；情報部門的資安防護及情資蒐研由國家安全局主責；數位發展部肩負強化政府數位韌性、落實資安法遵、提升產業資安及全民資安意識等重任；調查局及刑事警察局則為網路犯罪數位鑑識、溯源及執法的主力。

㈡ 跨部會協防體系《大聯盟》

配合《資安即國安》持續升級，增納重要政府機關及業務管理單位，包括其下轄機構法人、業管或監理之關鍵基礎設施、關鍵產業及其供應鏈（如圖 3 所示）。重要任務包括資源挹注、結合民間產學研能量、促進科研與產業發展；關鍵基礎設施之資安治理、預算分配、監督執行、重要資料與系統防護、推廣推動及超前部署、資安外交協力等。

㈢ 戰略夥伴國際合作

我國站在世界民主陣營的第一線，《國家資通安全戰略 2025》對外首重與先進戰略夥伴及理念相同之友邦國家攜手合作，並積極參與國際機構、資安專業社群及產學研等事務。透過公私協力與國際合作，將有效提升資安防護並擴大影響力。

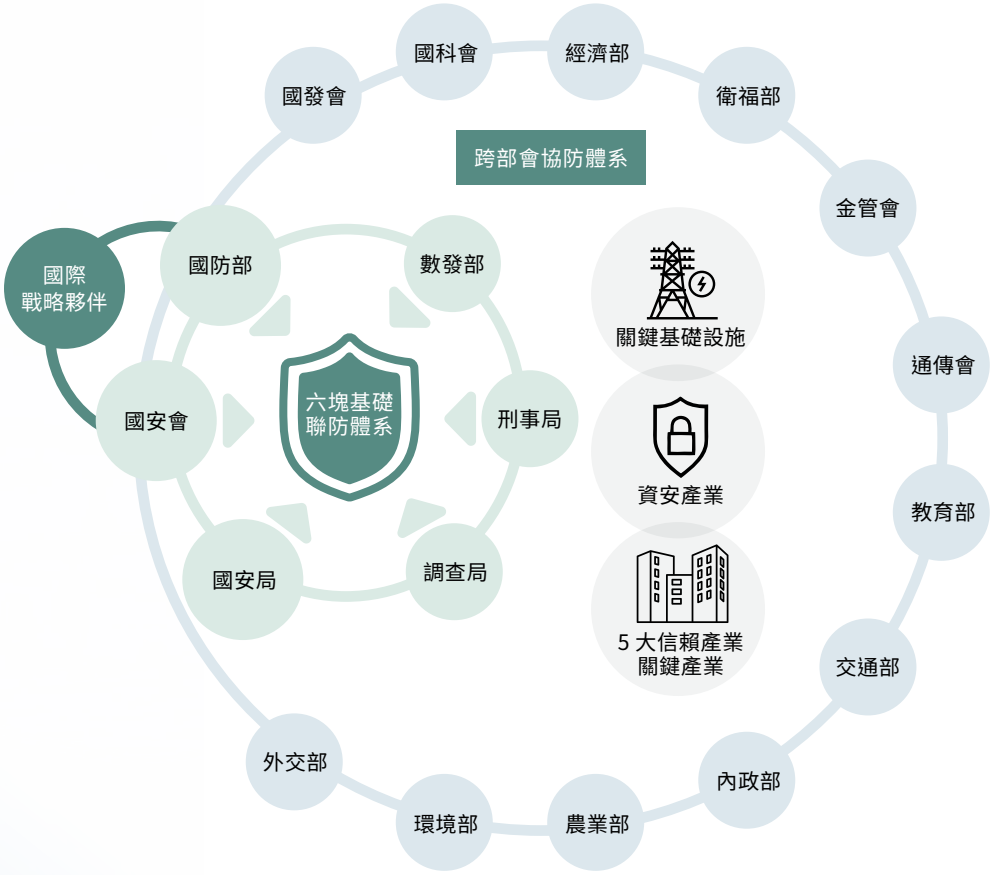


圖 3、跨支柱基盤與公私協力團隊

結語——打造堅韌、安全、可信賴的智慧國家

資安即國安，面對日益升級的資安威脅與挑戰，我國必須展現全民共同參與、全面投入資源與由上而下的決心，才能有效強化國家資安韌性，守護民主自由與產業繁榮。當前資安威脅早已不只侷限於技術層面，更是涉及國家安全、經濟與社會穩定、及政府運作的全面議題。國家級駭客組織、AI 驅動的複合式攻擊及供應鏈安全風險層出不窮，我國作為地緣政治樞紐與國際供應鏈的重要夥伴，處於全球資安戰線的最前緣，責無旁貸。

在此背景下，《國家資通安全戰略 2025》以「打造堅韌、安全、可信賴的智慧國家」為願景，提出以「全社會防衛韌性」等「四大支柱」為核心的策略佈局，包括零信任架構推行、主動防禦能力建構、國際聯防深化、人工智慧應用安全等關鍵措施。這些策略不僅需要技術、政策與法規的全面升級，更需要從政府到企業、從學界到民間的全社會參與，形成資安防護的共同體，凝聚每一份力量來應對未來的挑戰。

全民共同參與是資安防護的關鍵，政府應率先投入更多資源，展現由上而下的決心，加速變革。從威脅情勢掌握、政策與法規制定到資源分配與機制強化，政府將以資安治理架構的落實作為政策核心，提升公部門與關鍵基礎設施的防護韌性。同時，須深化與國際公私部門的合作，加強情資分享與聯防能力，讓台灣在全球資安生態中發揮更重要的角色。此外，必須大力培育資安人才、推動產業創新，做到資安自主，並透過誘因措施促使企業加強資安治理，形成產業自發提升的良性循環。

資安挑戰無國界，唯有全民上下一心、整合資源、全力投入，才能在全球數位競爭中確保台灣的安全與發展。我們需要以遠見與行動來應對資安威脅，以決心與策略守護國家的自由民主與產業繁榮，為全體國民締造一個堅韌、安全、可信賴的智慧國家。未來，我們將透過不懈的努力與變革，在國際資安舞台上站穩腳步，成為全球資安韌性的典範。

致謝

謹此向所有參與《國家資通安全戰略 2025——資安即國安》研擬工作的專家學者、公協會代表表達誠摯感謝，您們的專業意見與寶貴建議，爲國家資安政策進一步奠定更堅實之基礎，提升整體資安防護能量。

特別感謝名單：

吳宗成　國立臺灣科技大學資訊管理系特聘教授
吳明蔚　中華民國資訊軟體協會理事暨資安韌性促進會會長
李忠憲　國立成功大學電機工程學系教授
李倫銓　台灣駭客協會常務理事
李漢銘　國立臺灣科技大學資訊工程系特聘教授
李德財　中央研究院院士
沈柏延　中華民國資訊軟體協會理事長
林盈達　國立陽明交通大學資訊工程學系講座教授
金慶柏　台灣資安主管聯盟會長
夏　耘　國家資通安全研究院研究員
孫雅麗　國立臺灣大學資訊管理學系暨研究所教授
翁浩正　台灣駭客協會理事長
陳浩維　臺灣國際基金會創辦人
陳　曦　中國文化大學財務金融學系暨研究所助理教授
黃勝雄　財團法人台灣網路資訊中心董事長
鄭仲倫　台灣駭客協會常務理事
鄭欣明　國立臺灣科技大學資訊工程系教授
戴辰宇　台灣駭客協會理事暨總統府全社會防衛韌性委員會委員

（依照姓氏筆畫排序）

書　　名：國家資通安全戰略 2025 ——資安即國安
著作權人：國家安全會議
發 行 人：國家安全會議 吳釗燮秘書長
作　　者：國家安全會議 國家資通安全辦公室
總 審 訂：國家安全會議 李育杰諮詢委員
　　中央研究院 李德財院士
　　國立臺灣科技大學資訊工程系 李漢銘特聘教授
出 版 者：國家安全會議 國家資通安全辦公室
出版年月：2025 年 4 月
ISBN：978-626-7688-03-8
GPN：1011400332

國家安全會議
NATIONAL SECURITY COUNCIL

國家資通安全戰略2025

打造堅韌、安全、可信賴的智慧國家

國家安全會議
NATIONAL SECURITY COUNCIL

國家資通安全辦公室