國家資通安全戰略報告

資安即國安 2.0

打造堅韌、安全可信賴的智慧國家

TRUSTWORTHY

People Prosperity
Protection
People Prosperity

國家安全會議 NATIONAL SECURITY COUNCIL 國家資通安全辦公室

2021年9月

國家資通安全戰略報告

資安即國安 2.0

國家安全會議

序

「資安即國安」，面對鋪天蓋地、沒有煙硝的數位資訊戰，沒有人可以置身事外。

當虛擬進入我們的生活，成為現代社會的日常。資訊安全(Cyber Security) 不再僅限於高科技人員的獨門學問，也不只是政府層次的管理防範，而是我們每一個人，都肩負著資訊安全的重責大任。

在我總統的第一任期，全力推動「資安即國安」戰略。行政院成立資通安全處、國防部成立資通電軍、調查局建立資安工作站，立法院也通過《資通安全管理法》等。

我們從組織、法制，到公部門的資安人才，逐一替臺灣打下穩固的基礎。接下來，政府進階推出「資安即國安 2.0」戰略，我們努力在既有的成果之上，更加精進完備。

在 2.0 戰略中，政府規劃設立數位發展部、成立專責的資通安全署，我們要更完善精實防禦的機制，積極培養資安相關領域的人才，促進國際交流合作，並扶持國內的資訊安全產業，廣納民間產學的豐沛能量，共同建立起「堅韌、安全、可信賴的智慧國家」。尤其在後疫情的時代，疫情加速了萬物聯網的普及，虛擬世界遠比真實世界還要更大。

資安不再只是個人手機、電腦及網路銀行的資料安全，未來包含自駕車、智慧家電、線上線下交易的串聯等，都需要更穩健的防護系統。

可以預期，國內外各產業都會加入數位轉型的趨勢，隨著 5G 、AI、AIoT 在各領域的廣泛利用，政府也需要透過風險管理的角度，確保大家日常生活的安全。

臺灣位處在民主前緣，是國際資安攻防的一級戰區，網路威脅的樣態與時俱進、多元複雜，這是我們的挑戰，也是我們的機會。

資訊安全需要結合所有人的共同力量。讓我們一起化挑戰為機會，讓世界看見臺灣的優勢，我們不僅擁有自主防護的能力，也能與國際上的民主夥伴，一起打造國際級的資安場域，共同維護數位領域的自由與繁榮。

總統 蔡英文

2021 年 7 月 12 日

目 次

表 目 次

圖 目 次

第一章 背景

民國 107 年 7 月由本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), 規劃重點包括 : 對內凝聚政府推動資安政策量能 , 促進資安產業發展 ; 對外則倡議資安政策與宣導 , 同時促進國際交流合作。時至今日 , 由於主客觀環境變化 , 科技持續飛速演進 , 以及國人資安意識的普及進步 , 本會自民國 109 年啟動新一階段《資安即國安戰略 2.0 報告》的研擬 , 以打造堅韌、安全、可信賴之智慧國家為目標 , 在既有戰略 1.0 報告的基礎上 , 提高戰略思維層級 , 建構更全面的資安策略整體規劃 , 以強化守護臺灣資訊安全防護網 , 並維繫國家民主自由與產業核心競爭力的永續發展。

第一節 資安即國安戰略執行現狀

在資安即國安戰略 1.0 的三大目標下，原行政院資通安全辦公室業於民國 105 年升格為行政院資通安全處；另，確立國安、資安及通安的鐵三角架構及 4 年期「國家資通安全發展方案」，亦同步推動「資通安全管理法」立法完成，並修正國安相關法規。此外，國防部正式成立資通電軍指揮部，並修正國家情報工作法將資通電軍納入準情報體系，建構國家資訊安全緊急應變團隊，以對應與日俱增的境外敵對勢力駭侵量能，同時強化國內自主資安產業。

再者，本會已協同「資安旗艦計畫」及「前瞻基礎建設計畫」等公部門資源投入，成立國家通訊暨網際安全中心、建構國家及六都聯防體系，並成

立資安線上學院，同時強化工控資安人才培育，以落實八大關鍵基礎設施之各項資安防護工作。爰此，資安即國安戰略 1.0 已達成階段性目標(表 1)。

表 1 資安即國安戰略 1.0 重點效益

	資安即國安戰略 1.0
組織	成立行政院資通安全處
法制	實施資通安全管理法 修正國家安全法及國家情報工作法
人才	成立資通電軍
產業	強化自主資安產業

第二節　數位趨勢下全球與國內面臨資安複合挑戰

從國際資安情勢看來，目前全球常見五大資安威脅包括：一、社交工程搭配時勢議題作為攻擊主軸；二、進階持續性滲透（Advanced Persistent Threat, APT）類型攻擊轉為利用商用工具軟體與服務；三、供應鏈攻擊活動加劇；四、物聯網攻擊鎖定監視與網通設備；五、勒索軟體攻擊風險激增。均與我國主要遭遇到的問題一致 (圖 1)。

社交工程搭配時勢議題作為攻擊主軸

攻擊啟動從釣魚郵件開始，駭客以近期受關注程度高的政經議題為由施行攻擊，例如肺炎疫情，總統520就職等，鎖定特定相關機關進行攻擊。

APT類型攻擊轉為利用商用工具軟體與服務

駭客利用網路上現成的工具程式或商用軟體進行入侵攻擊，並滲透與掌控AD系統，利用政府導入政府共通組態基準(GCB)以合法的服務，透過GPO派送惡意程式進行橫向擴散。

供應鏈攻擊活動加劇

入侵系統委外廠商後，以其做為跳板，滲透客戶組織駭客藉由入侵特定軟/韌體開發公司或人員電腦，進行修改程式或下載連結等行為，造成大範圍的感染與擴散。

物聯網攻擊鎖定監視與網通設備

鎖定機關監視器與網通設備做為攻擊標的，以弱密碼/預設密碼配合已知弱點攻擊程式進行探測並入侵控制。

勒索軟體攻擊風險激增

由亂槍打鳥轉向特定目標，遭鎖定對象包含委外廠商、機關人員，機關之公文系統資料庫主機，對外服務網站，環控系統，檔案分享系統等，藉以癱瘓系統運作，中斷服務提供。

疫情讓資安風險大增 社交工程事件頻傳

2020/8/31趨勢科技統計，半年攔截880萬次COVID-19攻擊 - 趨勢科技發表2020年上半年資安總評報告顯示6個月內即攔截880萬次新冠肺炎相關威脅，其中近92%是經由垃圾郵件散布。

供應鏈攻擊鎖定 FireEye使用SolarWinds Orion

2020/12/08美國資安公司FireEye揭露其遭到國家級駭客的入侵，確認駭客已取得該公司紅隊滲透的工具 - 經調查因FireEye使用SolarWinds Orion平台有關，駭客將惡意程式碼放入Orion並被編譯成修補程式，開放給客戶下載使用，造成18,000個客戶受到感染。

勒索軟體轉向目標式攻擊 資安威脅遽增

2021/03-04宏碁、廣達先後傳出遭駭客入侵，分別勒索5,000萬美元贖金 - 駭客組織不只威脅到產線運作、勒索鉅額贖金，更趁機竊取商業機密，做為進一步要脅業者的手段。無獨有偶，2020/7 Garmin傳出疑似遇害而導致服務與網站一度中斷，5月初中油台塑，力成先後遭駭客鎖定攻擊。

APT攻擊串聯網通設備或 商用軟體漏洞發動攻擊

2021/03/02微軟宣布旗下Exchange Server(電郵系統與行事曆)有漏洞 - 可入侵企業伺服器，偽裝管理員進行設定，得以遠距操控伺服器，目前調查背後的組織為中國的駭客團體Hafnium，手法為租借美國虛擬私人伺服器運作。

物聯網資安設備弱點威脅升高

2020/6/10 IoT裝置驚爆漏洞，恐引發資料外洩與DDoS攻擊 - 通用隨插即用協定來發現其他裝置並與之互動的物聯網設備及區域網路裝置，存CallStranger安全漏洞，可藉此漏洞竊取資料，發動分散式阻斷服務攻擊。

資料外洩、個資、商業機密全都露

2020/11 Prestige Software雲端配置錯誤，造成Booking.com，Expedia與Agoda等客戶的房客資料外洩 - 提供架站服務的Website Planet近日揭露，Prestige Software雲端配置錯誤造成多家住房網房客資料外洩，約有10萬名房客的信用卡資訊，受害者遍及全球。

資料來源：行政院資通安全處

圖1 全球重大資安威脅型態與案例

更令人憂心的是，伴隨全球數位化技術應用演進，帶動組織型駭客及國家支持型的網路攻擊複合化，頻繁刺探委外廠商與供應鏈公司。攻擊手段從以鎖定弱點（如供應鏈、產品）、數據分析的精準打擊目標人物到混合爭議訊息操作輿論（資金、認知），對國家安全、社會安定及民心士氣帶來新形態的威脅(表 2)。

表 2 鎖定弱點攻擊態樣與案例

弱點	態樣	國外案例	國內案例
供應鏈	委外廠商	資安大廠	委外公司
產品	硬體、 軟體、服務	IT 網管與網路 監控平臺業者	資通設備、 商用系統、雲端服務
資金	外包、 股權結構	事務所	委外公司、 資通訊廠商
人	釣魚郵件、 滲透、國籍	COVID-19 郵件	學研單位、醫療院所 （開發與維運）
認知	爭議訊息	社群媒體遭利用 影響各國大選	利用戰機失事事件 發布假訊息稱戰機投共

有鑒於此，茲將國內目前所面臨之嚴峻資安威脅與議題挑戰歸納為資安人才不足、外部新型態資安威脅及國內資安產業發展三大面向(圖 2)，並分別說明如次。

壹、資安人才不足

現今政府與產業各界均面臨資安人才不足的窘境，前者受限於公務人員選才制度，致資安人才招募不易，而專責資安職缺與任務日增，專職資安人員的空缺仍多，其中又以關鍵基礎設施之相關事業單位缺少資安人才為最迫切。從供給面來看，許多在校修讀資訊/資安相關科系領域的優秀人才，在強大的就業磁吸效應與跨國企業提供優渥的待遇條件影響下，並未選擇進入資安領域的職場工作；至於針對在職者進行跨領域別的資安能力培育則更加不易。在此種種狀況下，國內整體優質資安人才無論質與量提升的努力空間仍大，且整體的聯合防禦能量仍有待進一步提升。

貳、外部新型態資安威脅

近年來境外網駭攻擊與日俱增，除針對政府機關與關鍵基礎設施以外，更擴大發動包括竊取供應鏈廠商機敏情訊及國人個資等駭侵。由於匿蹤為網路重要特性之一，使得國家級攻擊的溯源困難重重，課責與究責機制亦尚不足。而過往國內做法多採取被動防衛，無法有效防範網路犯罪與國家級的外部威脅。

參、國內資安產業發展

完善的國家資安防禦有賴於建立繁榮的資安相關產業生態系，除了健全的留才、攬才與育才機制外，還必須能建立供需互倚蓬勃發展的產業環境與市場。然而國內各界將資安設計思維帶入產品設計仍不普遍，企業建立完善資安防護作為的意識不足，致國內資安產業與

市場整體需求動能有限,難以推升國內資安產業發展並吸引優質人才,長期恐將造成整體防禦能量不足的危機持續擴大。

衝擊議題

圖2 整體資安衝擊與議題分析

第三節　主動式防禦趨勢興起

歐美等先進國家近來為因應日益嚴峻的組織型或國家型駭客攻擊，均已提出主動式防禦策略，聚焦如何強化事件歸因、有效阻斷攻擊並減少攻擊後的災損。所謂主動式資安防禦機制係以資安威脅情報、數據及資安分析為後盾，讓政府與關鍵基礎設施的資安防護團隊，可根據攻擊者的駭侵行為，快速主動應變，包括鑑識潛在入侵者，清除後門與惡意程式，並主動阻斷攻擊來源，重新配置資安防護縱深，以增強組織事件應變能力，達到「早期預警、緊急應變、持續維運」的目標(圖 3)，更進一步可建立國際間的聯防機制。

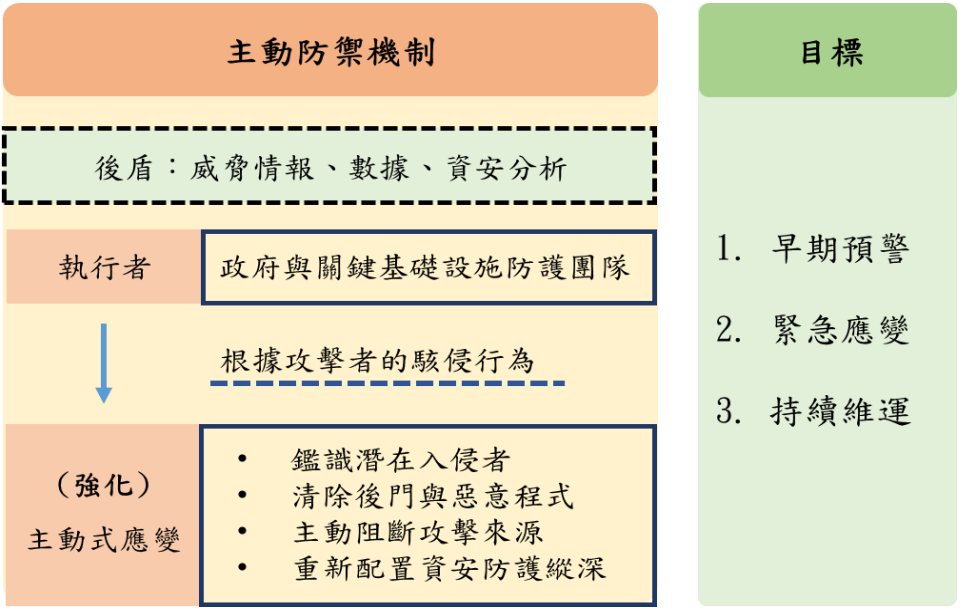


圖 3 數據驅動的主動式防禦發展趨勢

第二章《資安即國安戰略 2.0》重要內涵

現今境外勢力為干擾我國民主發展及打擊我國經濟發展與繁榮，日益加強網路攻擊力度、系統性散佈爭議訊息、入侵我高科技產業，遂行竊密與破壞。為有效因應情勢、守護國內民主自由與經濟發展，部署《資安即國安戰略 2.0》升級國內整體資訊安全防護網已刻不容緩。

第一節 資安即國安戰略 2.0 願景與目標

資安即國安戰略 2.0 在戰略 1.0 實施的基礎上，將以「打造堅韌、安全、可信賴之智慧國家」為願景(圖 4)，持續擴大並強化落實資安防護作為，完善資安防護體系，及提升資安應變能力。為因應前章

所述外部資安威脅與議題等挑戰，茲訂定對應的三大主軸與目標，包括：

目標一：充實資安卓越人才（People）

目標二：強化人民家園安全防護、鞏固資安外交網路防禦（Protection）

目標三：促進產業繁榮發展（Prosperity）

第二節　資安即國安戰略 2.0 推動策略

近年來供應鏈安全、零信任(Zero Trust)與主動式防禦的前瞻資安概念均為先進國家所倡議，加以國內面臨的資安風險急遽攀升高居全球前列，職是之故，本會參考先進國家策略並提升戰略思維，在「打造堅韌、安全、可信賴之智慧國家」願景及戰略 2.0 之三大目標下擬定五大推動策略「TRUST」。

茲說明如下：

- 策略一：Talent - 培育資安卓越人才，建構聯合作戰機制
- 策略二：Resilience - 提升防護韌性
- 策略三：Unity - 促進資安國際合作，建構國內外聯防體系
- 策略四：Security - 發展精實防禦機制，打擊網路犯罪
- 策略五：Technology - 產業落實資安、驅動資安產業

各目標策略與做法茲分述於下節。

圖4 資安即國安戰略2.0願景與目標

第三節　資安即國安戰略 2.0 推動做法

壹、充實資安卓越人才：培育資安卓越人才，聯合作戰機制

一、強化資安能力，培育資安卓越與實戰人才

過往在資安即國安戰略 1.0 下推動跨域資安人才培育各項計畫，主要由教育部推動新型態資安暑期課程培育在學資安人才，並建立虛擬的資安研訓院培育資安跨域在職人力，同時國防部也成立資通電軍指揮部，培育資安戰力。然而此一培育模式因現今資安防護需求急遽升高，已不足以快速因應補足政府與企業對於專職資安人力的需求，亟需增加資安高教師資，提高資安在學人才培育的質與量；並以公

私協力模式，打造國家級資安卓越中心，以實作代訓、擴大培育跨域資安人才，補足政府與產業所需的資安人力，強化國家資訊安全團隊，深化聯合防禦綜效，落實資安治理各項工作。相關做法如下(表 3)：

（一）完善資安高教環境：擴增師資員額，延攬國際頂尖師資，透過出國研習、跨域進修、引進產業專家等培養種子教師，帶動資安師資生態系統發展。

（二）於規劃成立之數位發展部下新設「國家資通安全研究院」，並成立「技術服務中心」與「資安卓越中心」，加速培育資安研發人才，並強化與民間資安專家及社群的合作，建立資安國家隊。

（三）設立防衛後備動員署，精進關鍵基礎設施資安協防機制。

表 3 資安人培 2.0 策略

資安及國安戰略1.0	單位培育對象	資安及國安戰略2.0
資安暑期課程	**教育部** 在學資安人才	**完善資安高教環境** • 於4年內擴增師資員額 • 延攬國際頂尖師資
虛擬資安研訓院	**數位發展部/經濟部** 資安跨域在職人才	**成立國家資通安全研究院** • 前瞻資安技術研發人才培育 • 招募民間專家組織國家資安戰隊 • 資安競賽以戰代訓培養實戰人才
資通電軍指揮部	**國防部** 資安戰士	**設立防衛後備動員署** • 培訓後備網路戰士 • 精進關鍵基礎設施協防機制

二、建構聯合作戰機制，推動公私協同治理

公私協力團隊主要由本會與行政院團隊共同推動，其中本會統籌法制、政策與前瞻技術領航團隊 。行政院協同新設之數位發展部 、調查局、刑事警察局、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)與民間關鍵基礎設施及企業密切合作。主要工作包括以下三項：建立各領域公私協同治理運作機制、增強人員資安意識與能力建構、公私合作深化平時情資交流與應變演練。

三、完備資安組織架構

（一）加速成立數位發展部暨資安相關部門

為因應境外敵對勢力，影響國家安全與民主發展，行政院於 110 年調整行政院的資安組織架構，將加速成立數位發展部，以專

責部會整合資訊、資安、電信、網路和傳播 5 大數位發展相關業務領域，提升各種資安危機處理的應變能力。而數位發展部尚未成立時，則預先部署強化國家資訊（國家發展委員會）與資安（行政院資通安全處）的整合協調機制及推動國家資訊/資安政策的落實。

（二）資安鐵三角升級至六塊基礎聯防

原資安即國安戰略 1.0 規劃的鐵三角機制，係由本會資安辦公室、行政院資安處及國家通訊傳播委員會共同建構，主要任務是維護國家安全、資訊安全及通訊安全；現為落實資安相關規範與措施，並有效因應資安事件調查應處之需求，進一步升級增納國防部資通電軍、法務部調查局，及內政部刑事

警察局，共同建構六塊基礎聯防體系(簡稱六塊基，圖５)，國家通訊傳播委員會則擔任關鍵基礎設施資安防護的主管機關。

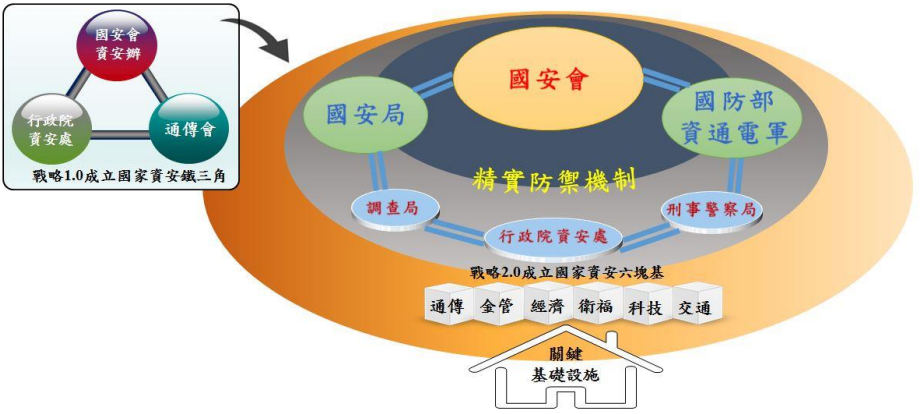


圖５ 六塊基礎聯防體系

貳、強化人民家園安全防護、鞏固資安外交網路防禦

一、提升防護韌性

主要任務如下：

（一）針對前述所提被鎖定的弱點，強化委外

供應鏈風險管理，並提升八大關鍵資訊基礎設施及六大核心戰略產業承受大規模網路滲透、高強度網路攻擊與破壞的能力，快速有效地應變聯防，並進行復原、事後鑑識與歸因。

（二）完成國家層級的資安風險評估，以釐清風險優先順序，有效配置資源，並研發關鍵技術。

（三）以往分散式的網路架構暴露多項弱點，致資安團隊陷入被動、疲於修補漏洞；未來政府將採資訊資源向上集中管理，整合機房與網路集中出口、機房能源效率改善、共用行政資訊系統，減少暴露在外、缺乏管理的破口。

二、促進資安國際合作，建構國內外聯防體系

經過資安即國安戰略 1.0 有效部署之後，國內已建立八大關鍵基礎設施與跨域的資安聯防系統，透過資安資訊分享與分析中心(ISAC)、電腦緊急應變團隊 (CERT)與資訊安全監控中心 (SOC)的通報與聯防體系，有效地降低境外勢力對我國的網攻衝擊。未來更將透過資安即國安戰略 2.0 進一步深化國際情資分享、擴大國際參與，聯合理念相近國家夥伴、鞏固友邦發展數位資安外交(圖 6)。藉由擴大國際參與、整合國內外情資來源及分享，搭配日後「資安卓越中心」所建構的國際級資安培訓場域，進行跨國資安演練，從雙邊資安固邦至多邊資安聯防進行合作，提升我國在網際

空間的聯防能力，創造屬於臺灣的資安外交模式。其重要做法如下：

（一）深化國際情資分享，發展前瞻研究及技術應用，整合國內外情資來源，促進國際合作。

（二）協同理念相近國家進行多邊資安交流，建立常態及制度化的資安聯防機制，並積極參與區域聯防及早期預警體系；同時整合產官學研代表，組成資安專業團隊，以發揮公私合作能量。

（三）以雙邊合作為基礎，繼續強化資安外交固邦方案，提供有資安需求的友邦資安技術協助，發展數位外交，執行合作專案推促我資安產品，帶動產業發展；並

運用資安科技優勢，爭取以專業參與政府及非政府間多邊資安組織或倡議。

圖 6 資安國際合作策略 2.0

三、發展精實防禦機制，打擊網路犯罪

下一代資安防禦必須參考國際主動防禦趨勢加以精實化，方能制敵機先。為部署精實防禦，國內資安團隊將加速整合國內外各種數據，迅速追溯資安威脅源頭、檢測、分析、破解並制止惡意網路活動，緩解漏洞和病毒攻擊的威脅及爭議訊息散播的混合挑戰，發展網路治理的模式，並建構精實防禦機制，防護八大關鍵基礎設施與六大核心戰略產業，有效因應國家型網路攻擊(圖 7)：

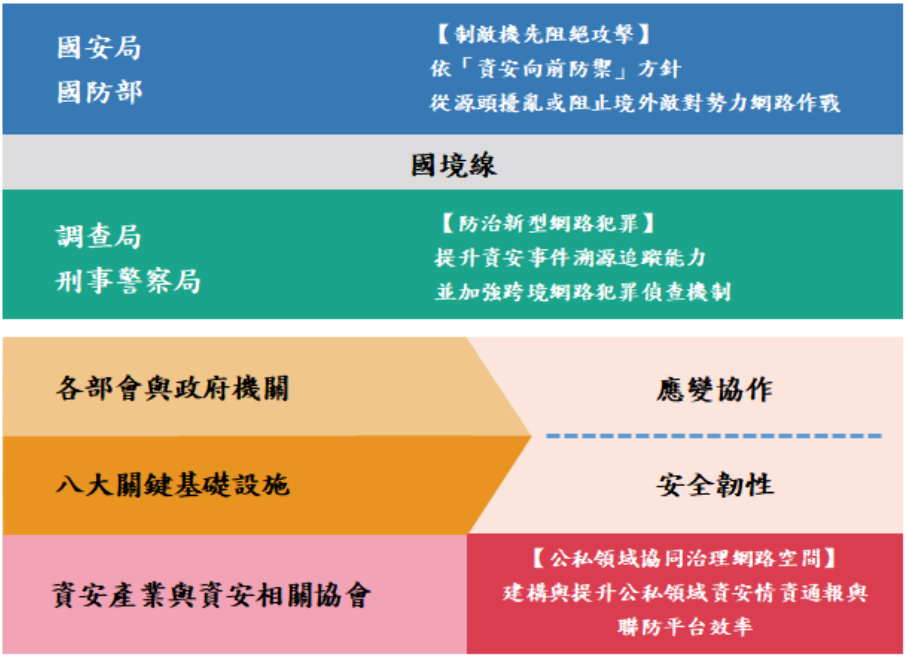


圖 7 精實防禦

（一）資通安全管理法已於民國 108 年頒布實施，相關的子法與施行細則亦已開始施行，惟各相關單位仍需時間具體部署防護措施，因此當務之急必須持續落實資通安全管理法及其相關的規

定與配套措施，並適時檢討以符合國際資安防護趨勢。

（二）提升科技主動偵查、網路溯源分析能量，制敵機先阻絕攻擊，政府團隊將以「資安超前防禦」為方針，應用新興資安技術，強化新型網路犯罪偵防能量、提升資安事件溯源追蹤能力及加強跨境網路犯罪偵查機制，防制網路犯罪並降低駭侵情事擴大。

（三）完善網路法規，建立並落實各相關單位的標準程序，發展真正權責分明的網際框架與安全查核制度。

參、促進產業繁榮發展：產業落實資安，驅動資安產業

根據經濟部統計，至民國 109 年國內資安產業總產值已達新臺幣 552 億元，共計有廠商家數約 340 家，從業人數約 9,000 人。與民國 108 年相比，廠商營運普遍持續穩定成長(圖 8)。

圖 8 資安各類別產值

未來在資安即國安戰略 2.0 下，為加快我國數位國家及產業發展，將於「5+2 產業創新」的既有基礎上，加速發展國內資安產業，以保護「六大核心戰略產業」，期望打造自主防禦，且獲得世界各國信賴之資安系統及產業鏈；另接軌國際規範，加強國際合作，促進我國資安產業更加繁榮壯大，成為未來全球經濟發展中的關鍵力量。相關說明如下：

一、落實六大核心戰略產業資安導入

為因應國內數位轉型及智慧化需求，國家發展委員會已於民國 109 年規劃推動六大核心戰略產業全面導入資安，開發新領域資安國際解決方案，強化新興領域防護，建立供應鏈資訊安全體系，以確保數位國家發展(圖 9)。

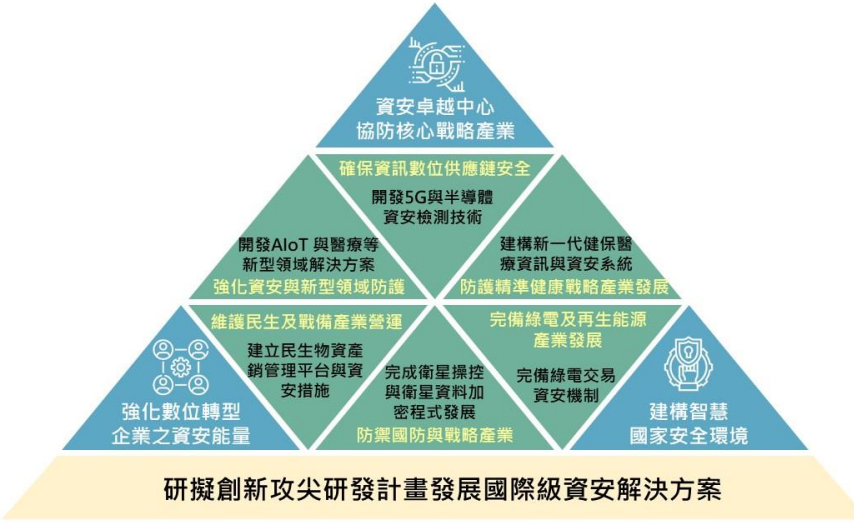


圖 9 六大核心戰略產業資安導入

二、提升資安產業自主能力，發展新領域資安能量

由國發會主責，統合其他政府單位，提出創新與前瞻的研發計畫，以發展新興應用領域之國際級資安解決方案，讓國內成為亞太高階

資安人才及技術創新基地為目標。此外，透過培育資安卓越與實作人才策略，提升資安產業研發人才素質，並推動「資安卓越中心」及相關學研單位協助資安產業進行研發，以持續強化資安產品核心技術能量，發展國際級資安解決方案。

三、接軌國際規範

健全的資安防護與繁榮的產業生態系不能侷限於國內市場環境，國內資安產業必須擴大接軌國際技術規範、參與制訂規範的組織，直接面對國際的競爭，產品、服務或團隊得到國際認證或殊榮肯定，才能將國內資安產業提升到新的層次，也才能夠真正打造繁榮的生態系統，並孕育卓越人才，完善自我防禦。在資安即國安戰略 2.0 下，未來將鼓勵相關機構與企業積極參與前瞻科技技術相關活動與工作

（如：國際標準訂定，積極與國際夥伴交流合作，參與新的技術參考架構開發等）。

表 4 資安即國安戰略 1.0 與 2.0 比較表

	資安即國安戰略 1.0	資安即國安戰略 2.0
組織	成立行政院資通安全處	1. 加速成立數位發展部暨相關資安管理部門 2. 政府機關六塊基礎團隊堅實合作
法制	1. 實施資通安全管理法 2. 修正國家安全法及國家情報工作法	法遵的落實（關鍵基礎設施、委外與供應鏈、資料庫等）
人才	成立資通電軍	強化資安卓越人才培育 促進公私團隊協力互助
產業	強化自主資安產業	六大核心戰略產業資安部署

第三章 結語

綜上所述，自民國 105 年起執行的資安即國安戰略 1.0 已經達成其階段性目標，不論是行政院資安處位階的提升、資安管理法施行、資通電軍的成立，以及強化自主資安產業，皆已確立了資安及國安的戰略發展方向與基礎。接續的進階戰略 2.0，亦將在前期奠定的基礎上，開展在組織、法制、人才與產業四大構面的全面升級。茲綜整如下：

一、 在組織面，加速數位發展部成立的進程，同時也建立政府機關六塊基礎團隊堅實合作架構，擴大開展國際緊密接軌。

二、 在法制面，深化各界法遵的落實，進而全面提升關鍵基礎設施整體韌性，改善委外與供應鏈管理，強化資料庫防護等。

三、 在人才面，促進公私團隊協力互助，強化資安卓越人才培育，發展精實防禦機制，藉以提升資安防禦整體能量。

四、 在產業面，加速六大核心戰略產業資安部署，以資安做為數位國力發展基石，建構共存共榮的臺灣產業生態系。

值此全球邁入物聯網與全面 5G 時代之際，隨著科技飛速進步，資安威脅與日俱增情勢嚴峻，唯有持續提升國家資安能量，才能確保國家安全、產業發展與人民福祉。資安就是數位免疫力，打造堅韌、安全、可信賴的智慧國家，期勉政府與民間、產業一起群策群力，超前部署。

書　　名：國家資通安全戰略報告-資安即國安 2.0

著作權人 / 國家安全會議

發 行 人 / 國家安全會議 顧立雄秘書長

作　　者 / 國家安全會議 國家資通安全辦公室

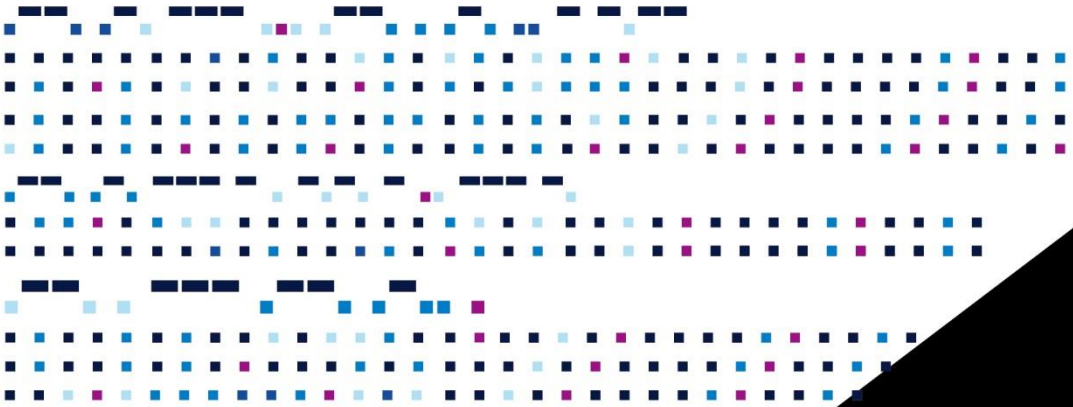
總 審 定 / 國家安全會議 李漢銘諮詢委員

中央研究院　李德財院士

出 版 者 / 國家安全會議 國家資通安全辦公室

出版年月 / 2021 年 9 月

People Prosperity Protection



打造堅韌、安全可信賴的智慧國家

People Prosperity Protection

ISBN 978-986-0724-45-5
00150
9 789860 724455

國家資通安全戰略報告

國家安全會議 NATIONAL SECURITY COUNCIL 國家資通安全辦公室