

國家資通安全戰略報告

資安即國安

打造安全可信賴的數位國家



國家安全會議 國家資通安全辦公室
2018年9月

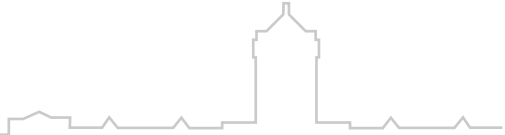
國家資通安全戰略報告



國家安全會議



序



資訊時代，數據就是資產，運作在自由、開放的網際空間中，創新了人類的生活方式，也開創了繁榮的契機。

同時，利益競逐與層出不窮的資訊安全問題也在邊界模糊的網路場域中應運而生，甚至產生資訊武器化的現象，是以世界各國多致力於網路治理研究、大力構築網路安全建設、設立專責機關、研定相關法規，並尋求國際協作，資安議題顯已超越科技範疇成為國家重要的戰略選擇。

我國因政經情勢特殊，經常面對網路竊資與攻擊的嚴峻考驗，我深刻體認網路空間的保護，攸關人民對政府的信任、經濟的發展與國家利益，就任之初即以國家層級思維，提出資安即國安戰略，並著手戰略的具體實踐。

自 2016 年 5 月執政以來，我們積極打造國家資安機制、建立國家資安團隊，並推動國防資安自主研發；行政院資通安全處、行政院數位國家創新經濟小組、國防部資通電軍相繼成立，並推動資安相關立法，期以建立安全、可靠的資通環境，達成數位經濟與國家發展的目標。

隨科技的躍進，資安能力必將成為國力的象徵與經濟的指標之一，故更需資安團隊、政府各部門、民間企業及非政府組織的協力合作。

今年國家安全會議提出了我國首部資安戰略報告，跨出複雜工程的初步，期盼報告的推出能強化全民資安意識、凝聚各界共識，為數位國家、創新經濟奠定堅實基礎。

總統

蔡英文

2018 年 7 月 24 日

目錄

第一章、資安即國安戰略的形成.....	6
第一節 國家智慧化面臨的資安挑戰.....	6
第二節 資安政策的重要內涵.....	11
第二章、資安即國安戰略願景、目標及方針.....	14
第一節 戰略願景與目標.....	14
第二節 戰略方針.....	16
第三章、資安即國安推動策略.....	18
第一節 打造國家資安機制，確保數位國家安全.....	18
第二節 建立國家資安體系，加速數位經濟發展.....	28
第三節 推動國防資安自主研發，提升產業成長.....	40
第四章、結語.....	50
第一節 持續優化國家資安機制.....	50
第二節 強化國家資安體系運作效率.....	51
第三節 完備資安自主產業生態體系.....	52
附錄、專有名詞英文對照表.....	54

圖 目錄

圖 1 以情報驅動之資安即國安戰略.....	12
圖 2 三乘三乘三的國家級資安戰略方針.....	15
圖 3 行政院國家資通安全會報新架構.....	21
圖 4 建立八大關鍵資訊基礎設施領域之聯防機制.....	24
圖 5 資安防護鐵三角運作流程說明.....	27
圖 6 國家資安聯防體系.....	28
圖 7 以情報驅動之國家資安聯防架構.....	31
圖 8 以「跨域試煉」為主軸之資安人才培育策略.....	36
圖 9 滿足國家安全防衛的資安產業自主研發策略.....	42

第一章、資安即國安戰略的形成

「資安即國安」戰略的形成，是以三大資安政策為主軸，包含將資安提升至國安層級、打造國家級資安機制與團隊及推動國防資安自主研發，並考量我國資安環境、戰略可行性及可執行性，由國家安全會議及行政院共同召集政府、產業及學研專家代表，召開相關策略會議擬定本戰略。

第一節 國家智慧化面臨的資安挑戰

隨著我國發展數位經濟及運用各種科技的過程中，各項基礎建設數位化、網路化及智慧化，卻仍發生重大資安事件，影響經濟與金融市場秩序。面對這些資安威脅，我國必須有「超前部署、預置兵力」的國家級資安戰略！

一、駭侵威脅程度升級至國安層級

（一）全球資安駭侵威脅情勢

1. 國家支持型：憑藉國家支持，攻擊其他國家政府組織單位，藉以竊取相關國家、國防及高科技機密。
2. 犯罪組織型：駭侵各國金融體系，利用釣魚郵件及勒索軟體等，要脅贖金或虛擬貨幣。
3. 理念宣傳型：置換政府單位網頁資料或散播虛假訊息，宣揚各式理念，影響政府施政或提高攻擊組織知名度。
4. 恐怖主義型：恐怖分子經由網際網路為平臺，達到特定意圖、訓練或動員激進分子進行攻擊。

（二）我國遭網路駭侵對象

檢討近年來國內資安事件駭侵層級，已升溫至攻擊政府體系與關鍵資訊基礎設施，以及關鍵民間產業，將影響國家安全，必須將資安防護升級至國安層級。

1. 政府體系：包含總統府、中央及地方機關（構）與相關單位等。
2. 關鍵資訊基礎設施：包含電信、金融、醫療、能源、水資源、交通及科學園區等。
3. 關鍵民間產業：擁有智慧財產權、商業機密，或影響產業數位化的關鍵企業與國防工業等。



二、強化國家整體資安防衛能力

面對駭侵威脅及層出不窮的資安事件，我國必須進一步提升國家整體資安防衛能力，加強資安機制、資安人才培育及資安產業自主研發，以突破資安防衛能力的困境：

（一）資安機制

1. 層級不足：政府資安相關單位原屬任務編組，於資安政策推動及事件協處上，因層級不足難以快速因應日趨嚴峻的資安威脅。
2. 法律未完備：目前網路空間尚未納入我國家安全法等領域，難以完整因應涉國家安全層級的資安事件，致資安機制出現缺口。



（二）資安人才

隨著數位經濟快速發展，致資安威脅程度亦加劇，使政府和產業對於資安防護及研發人才需求大增，凸顯現有資安人培質量的不足。

（三）資安產業自主研發量能

我國自主研發的資安廠商，因多數屬中小型企業，在研發資源有限情況下，難以投入足夠的研發能量於關鍵資訊基礎設施及物聯網等資安新興領域，進而影響數位國家發展的自我資安防衛能力。

第二節 資安政策的重要內涵

本戰略報告以情報驅動提出三大提升及三大整合策略，前者是基礎整備、產業量能和數位防衛能力的提升，後者包含資安人力、研究及產業的跨域整合，以提高資安機制效率、改善我國資安人力不足及產業自主研發能力疲弱等三大議題，進而達成三大目標及方針（如圖 1 所示）。



Cyber Security

以情報驅動提出資安即國安戰略

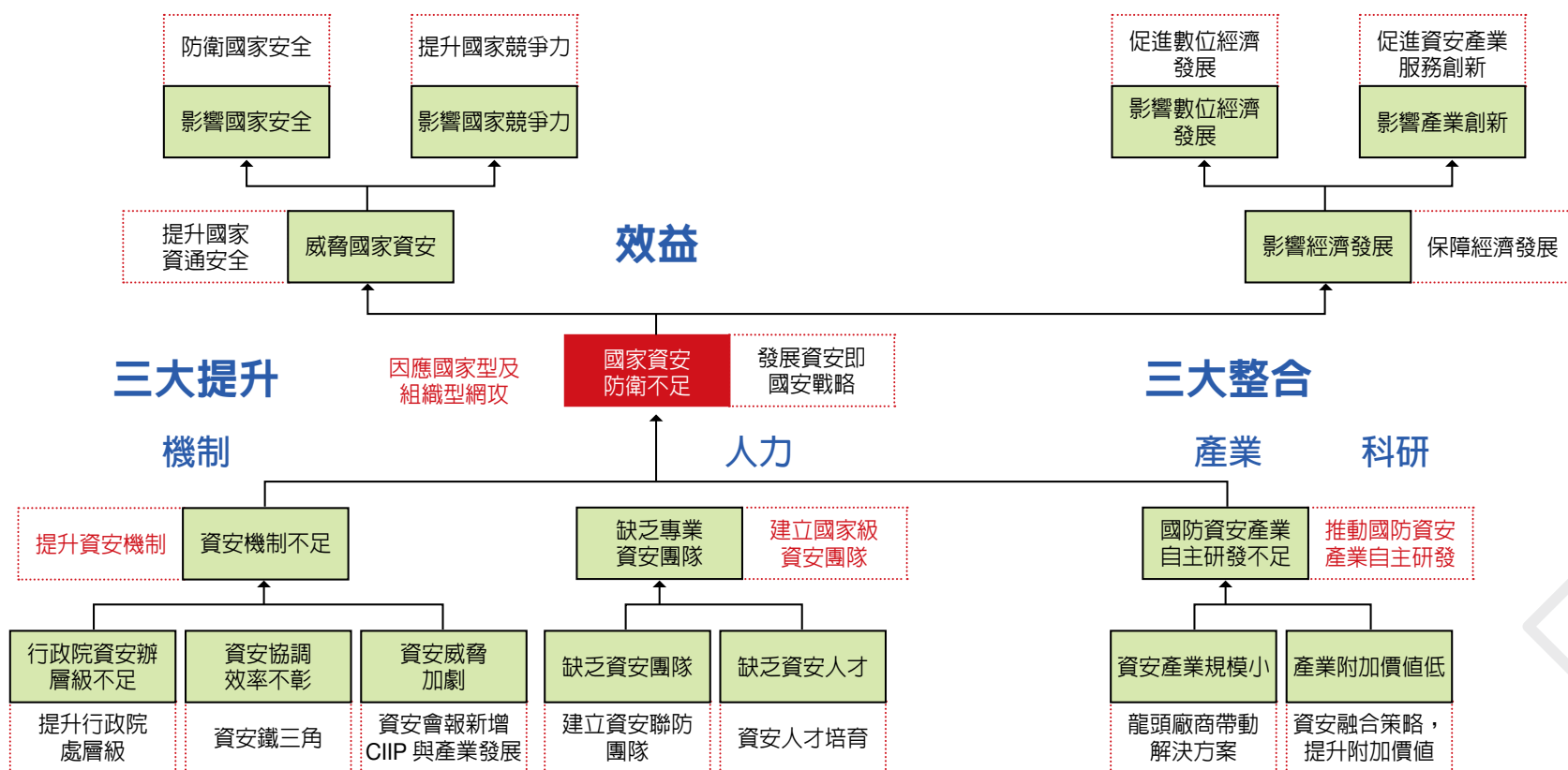


圖 1 以情報驅動之資安即國安戰略

第二章、資安即國安戰略願景、目標及方針

第一節 戰略願景與目標

依 2016 年 8 月資安即國安策略會議結論，訂定「打造安全可信賴的數位國家」戰略願景，國家安全會議國家資通安全指導小組第 13 次委員會議進而制訂三大戰略目標（如圖 2 所示）：

目標一：打造國家資安機制，確保數位國家安全。

目標二：建立國家資安體系，加速數位經濟發展。

目標三：推動國防資安自主研發，提升產業成長。

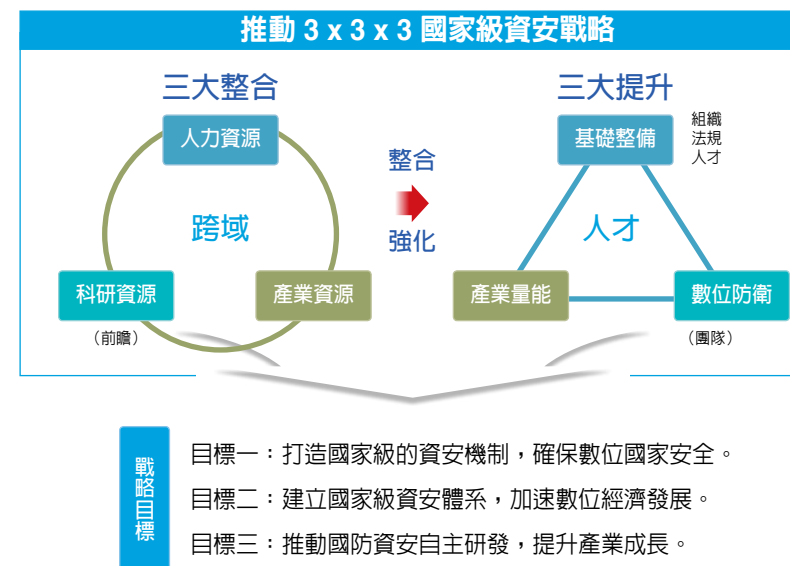


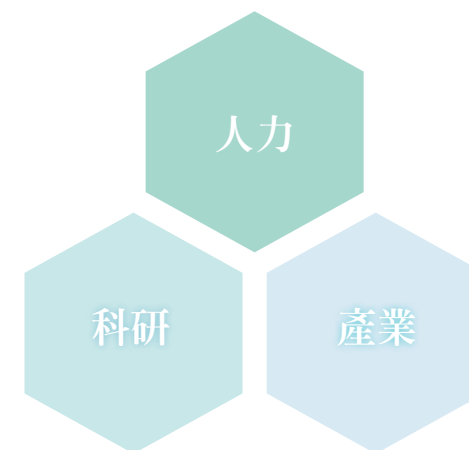
圖 2 三乘三乘三的國家級資安戰略方針

第二節 戰略方針

行政院國家資通安全會報第 30 次會議決議，規劃三乘三乘三的國家資安戰略方針。

方針一：以跨域為核心，整合人力、科研和產業資源。

方針二：以人才為核心，提升基礎整備、數位防衛和產業量能。





第三章、資安即國安推動策略

第一節 打造國家資安機制，確保數位國家安全

國家資安機制能夠有效運作的關鍵，在於資安組織的「專責與合作」及不斷完備資安相關法規。政府資安組織包含國家安全會議國家資通安全辦公室、行政院資通安全處及國家通訊傳播委員會，組成國家資安防護鐵三角，分別從國安、資安及通安等層面，保護國家安全及社會安全，建構國家整體資通安全防護網；並在「行政院國家資通安全會報」設立了「關鍵資訊基礎設施安全管理組」及「資安產業發展組」，以提高資安事件應變之組織層級、強化關鍵資訊基礎設施的安全及提升資安產業的合作量能。相關法規方面，持續完備與落實《資通安全管理法》、《個人資料保護法》等資安法規，並將網路空間治理概念納入《國家安全法》、《數位通訊傳播法》及《電信管理法》等法規修訂。

一、國家安全會議國家資通安全指導小組

國家安全會議為從事國家資通訊安全政策諮詢研究業務，加速建構國家資通訊整體安全環境，以及整合國家資通訊安全防護及反制能力，維護國家整體利益與數位國家安全，特設國家資通安全指導小組，並設網際防護體系、外館網際防護體系及網際偵蒐體系，分別由國防部、外交部及國家安全局主辦，並由國家安全會議國家資通安全辦公室擔任幕僚統籌統合協調各項工作與任務，指導小組重要工作如下：

- (一) 國家資通訊安全基本方針及規劃重點之研究，
- (二) 國家資通訊安全重要政策及措施之策劃與推動，
- (三) 國家資通訊安全相關事項防護、反制、偵蒐及應變作為之統合指導、協調及支援。

二、行政院國家資通安全會報

國家安全會議於 2000 年 5 月奉總統指示研提「建立我國資通訊基礎建設安全機制」建議書後，同年 8 月經總統核定並轉送行政院規劃辦理、研討相關規劃作業，於 2001 年 1 月第 2718 次院會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」，積極推動我國資通安全基礎建設工作，並逐年調整組織架構及相關任務。

近年來，資訊安全事件演變成組織型或國家型攻擊，影響社會穩定與國家安全甚巨。因此，行政院於 2016 年 8 月修正「行政院處務規程」，將原國家資通安全會報所屬任務編組的資通安全辦公室，改制為資通安全處，以更專責、專業方式推動並執行國家資通安全工作。同時，於網際防護體系下增設關鍵資訊基礎設施安全管理組及資安產業發展組，以提高資安產業自主量能，並強化關鍵資訊基礎設施的安全（如圖 3 所示）。

行政院國家資通安全會報組織架構圖

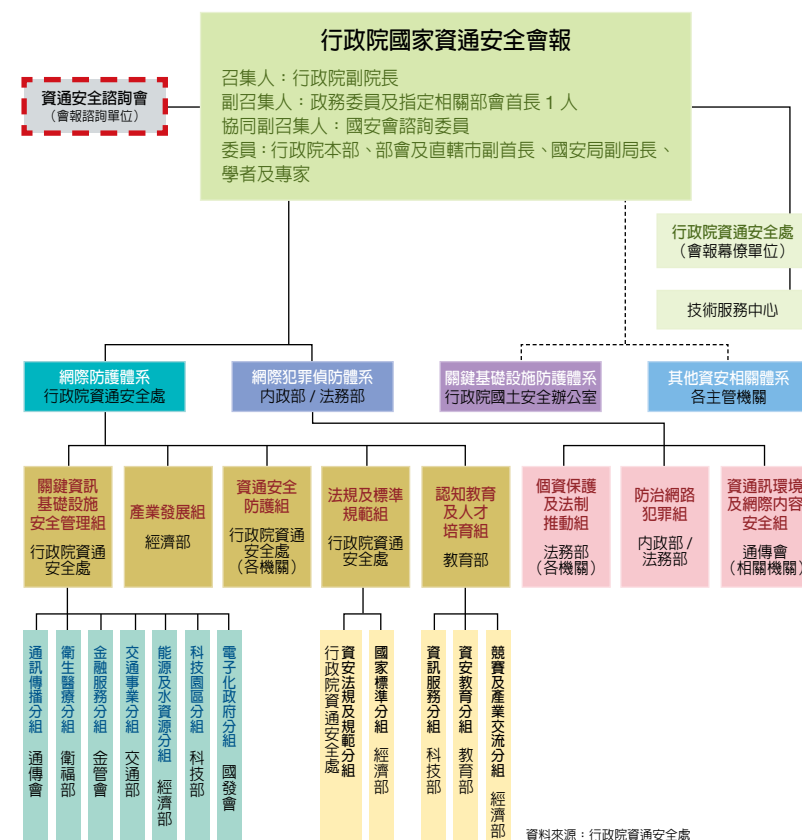


圖 3 行政院國家資通安全會報新架構

（一）行政院資通安全處

行政院資通安全處為行政院國家資通安全會報之專業幕僚單位，主責資安政策研議、法案審查、計畫核議、業務推動、督導及管考，主要任務包含：

1. 國家資通安全基本方針、政策及重大計畫。
2. 國家資通安全相關法規及規範。
3. 國家資通安全事件偵測及通報應變機制。
4. 國家關鍵資訊基礎設施安全管理機制。
5. 國家資通安全會報決議事項。
6. 資通安全相關演練及稽核。
7. 資通安全教育、訓練及宣導。
8. 資通安全國際交流及合作。



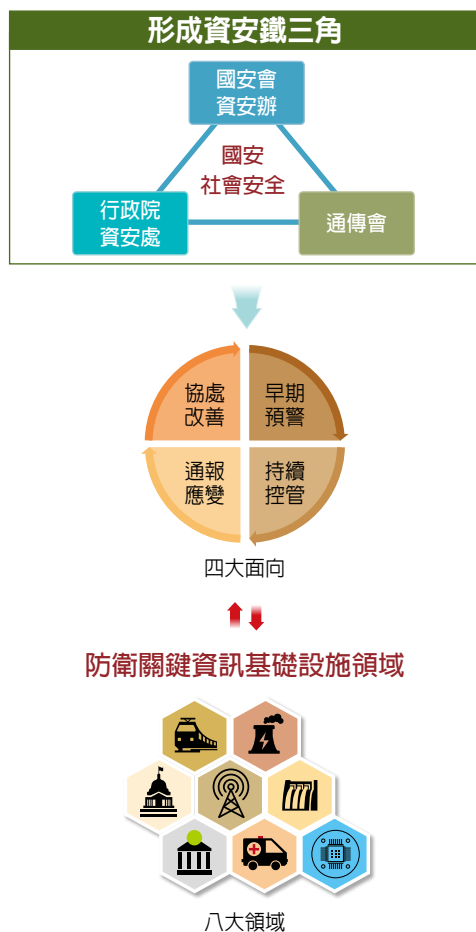
9. 其他有關資通安全業務事項。

（二）關鍵資訊基礎設施安全管理組

行政院國家資通安全會報增設關鍵資訊基礎設施安全管理組，使資安防護鐵三角連結相關部會，完善國家資安聯防運作機制、建立八大關鍵資訊基礎設施領域的資安緊急應變團隊、資安維運與預警中心，以及情資分享與分析中心，包含強化政府、高科技園區、能源、水資源、通訊、交通、銀行與金融、緊急救援與醫院八大關鍵資訊基礎設施的資安防護、風險評估機制及資安事件復原能力（如圖 4 所示）。

其中，通訊網路堪稱八大領域關鍵資訊基礎設施「持續營運」之神經骨幹，該通訊關鍵資訊基礎設施的資安防護由國家通訊傳播委員會負責，將強化早期預警、持續控管與維運、通報應變及協處改善等四大面向。





(三) 資安產業發展組

我國資安自主研發廠商屬中小型企業，缺乏足夠資源快速開發符合市場需求的資安解決方案或服務，造成我國資安產業鏈破碎化，使政府及企業的資安自主防護核心能量不足，也難以因應新興科技的需求。

為解決上述資安產業研發弱點，於國家資通安全會報設立資安產業發展組，由經濟部主責、國防部協同召集，對內凝聚國內資安自主研發廠商、資安創新創業及相關跨領域產業能量，以及投入高階人才自主研發，以提升國家自主資安防衛力量，對外則研擬並提出資安產業服務輸出策略。

圖 4 建立八大關鍵資訊基礎設施領域之聯防機制

三、資安防護鐵三角機制

由於資安事件態樣呈現多元，且被攻擊的目標，也從傳統的資訊設備不斷延伸到通訊和工業控制設備；被竊取的資訊不僅包括經貿與科技等智慧財產，更擴及國

家安全有關的外交、國防等機密。因此，有必要整合國安、資安及通安三方面之量能，形成防護三角機制，才能夠使資安事件的處理更全面、更快速且更有效，進而產生嚇阻作用（如圖 5 所示）。

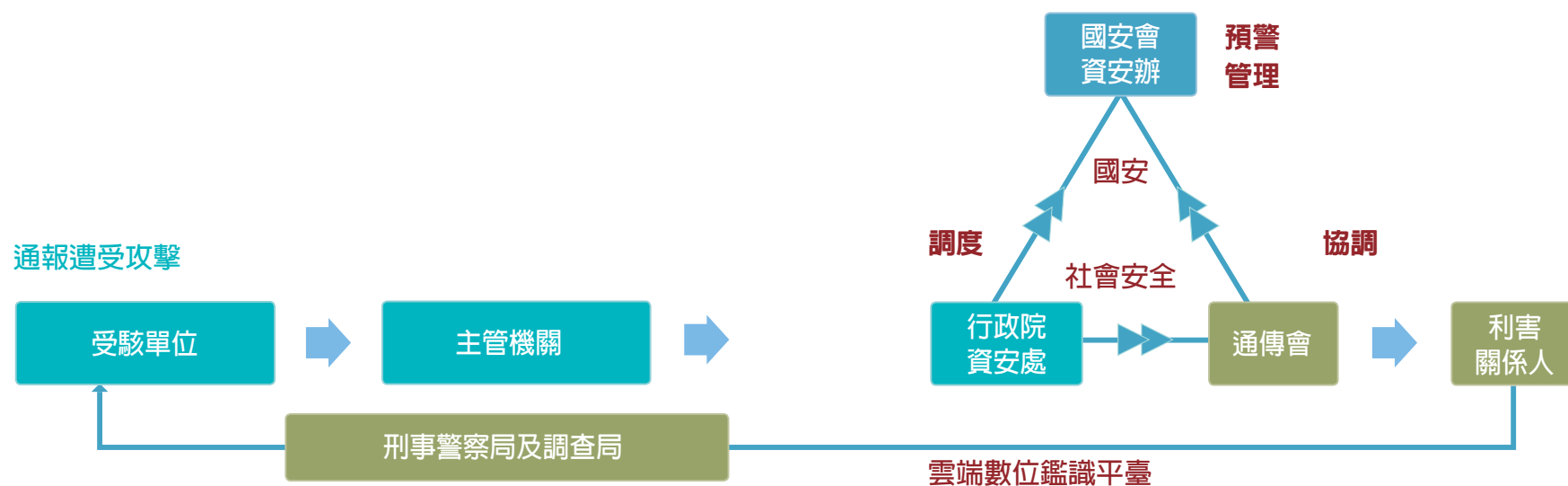


圖 5 資安防護鐵三角運作流程說明

第二節 建立國家資安體系，加速數位經濟發展

一、國家資安聯防體系

國家資安聯防體系包含政府、關鍵資訊基礎設施領

域本身以及其提供者三大層級（如圖 6 所示），以資安情報驅動形成資安聯防與合作體系，組成國家資安聯防團隊，並透過國際組織，與友邦進行國際聯防及情資分享。

建立國家級的資安聯防團隊

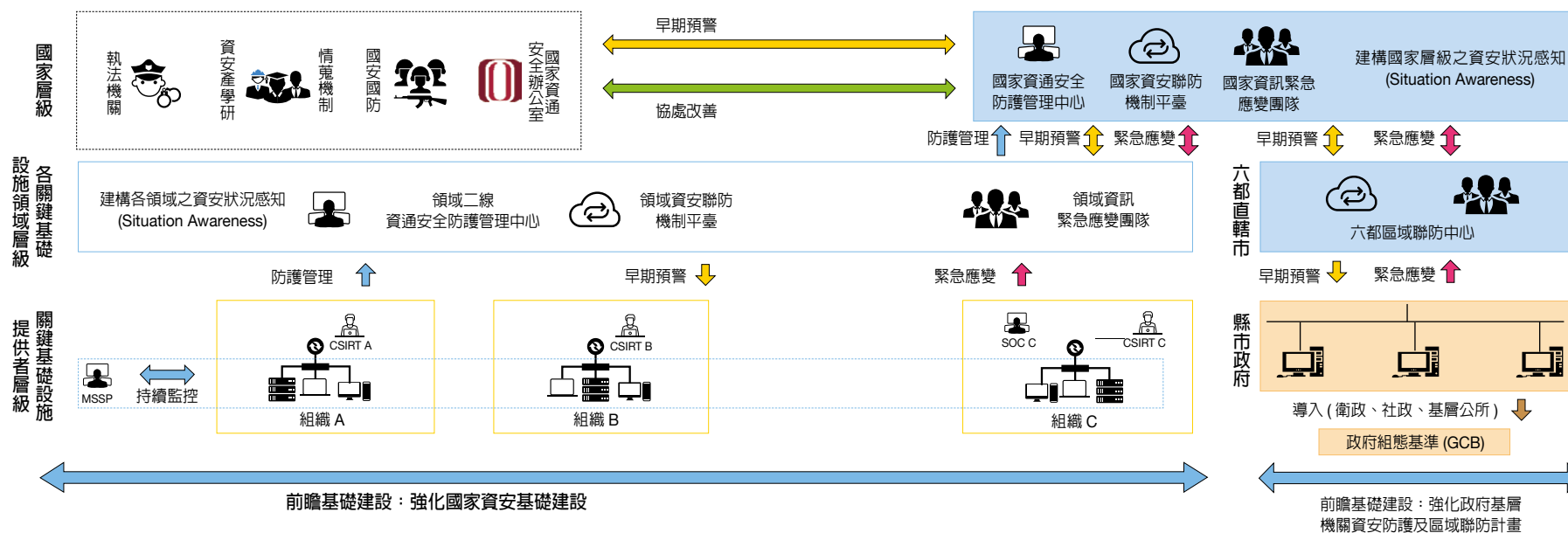


圖 6 國家資安聯防體系

資料來源：行政院資安處

（一）建立以情報驅動之國家資安聯防架構

國家資安聯防體系的建立，包含由國安單位及行政院各部會，分工籌組並整合資安緊急應變小組、資安事件通報及處理小組、資安維運及預警中心、以及情資分享與分析中心等單位，建立以「情報驅動」（資訊分享並協同應變）的資安聯防架構（如圖 7 所示），提升早期預警、緊急應變及持續維運的能量及效率。

資安情報驅動架構

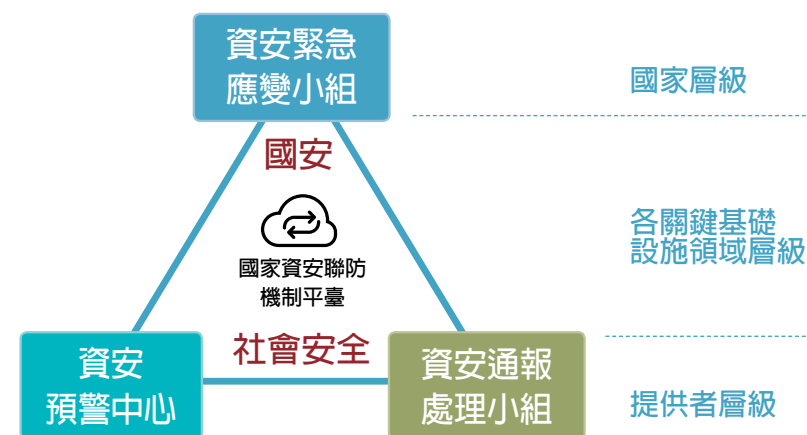


圖 7 以情報驅動之國家資安聯防架構

資安即國安

（二）建構關鍵資訊基礎設施資安聯防及情資分享體系

政府將持續推動整合和建構關鍵資訊基礎設施的資安聯防及情資分享體系，由行政院資通安全處擔任召集單位，協調各關鍵資訊基礎設施領域的主管機關，依分年目標，建構關鍵資訊基礎設施資安聯防及情資分享體系：

1. 建立各領域資安維運及預警中心、情資分享中心、緊急應變團隊，促進聯防及情資分享體系，
2. 納入行政院國家資通安全發展各期方案，以完備關鍵資訊基礎設施的安全，並建立資安聯防體系。



（三）強化政府與民間資安聯防及情資分享

完備政府與民間的資安聯防及情資分享與協作體系，提升民間企業資安通報效率，以及強化民眾資安認知。包含：

1. 藉由民間整合平臺，協調國內各類資訊緊急應變團隊與資安產業，共同強化民間聯防體系，以規劃我國資安產業發展需求導向的解決方案，提升資安聯防量能。
2. 建構線上惡意程式檢測平臺及服務。

（四）建構關鍵資訊基礎設施防護風險評估機制

建構關鍵資訊基礎設施資安防護風險評估機制，以建立風險地圖，強化資安聯防體系風險評估能力及應變效率。



（五）精進網路不法行爲偵防能量

因應數位經濟快速發展所衍生的網路的不法行爲，政府將挹注資源強化新型態網路不法行爲偵防能量，如提升網路不法行爲蒐證與鑑識能力，並建構網路跨境合作平臺。

（六）強化國際資安聯防體系

提升我國資安國際連結及合作能量，健全資安聯防及情資分享能力，完備國家資安聯防體系。

1. 我國與邦交國及理念相近國家合作組成資安虛擬聯防體系，提升資安事件跨國通報及應變效率，以達成保護網路資訊自由流通與平等接取使用的普世價值的目標。

2. 擴大我國與邦交國及理念相近國家的資安合作項目，包含政策、法規、技術研發、共同打擊犯罪、資安事件通報分析與防護能量等外交面向合作，包含：

- (1) 透過國際組織或多邊協議，強化網路犯罪聯防與資安事件情資分享。
- (2) 透過國際合作，強化資安科技尖端技術研發能量。

3. 提升我國學研、產業及民間社群的國際交流能量，促進資安防護的國際能見度。

二、資安人才培育及留才策略

提升我國資安人才的質與量是政府當前重要工作，將建立在學與在職人員的資安培訓機制，並鼓勵優秀人才投入資安產業，協助數位經濟發展。

推動資安人才培育策略，係以「**跨域試煉**」為主軸，由教育部提供資安扎根正規教育，科技部和經濟部提供實作場域試煉，培育出國家、國防、關鍵資訊基礎設施、打擊犯罪及產業所需的資安人才，以強化我數位國家發展的根基（如圖 8 所示）。



圖 8 以「跨域試煉」為主軸之資安人才培育策略

（一）扎根正規教育，培育實作人才

1. 強化資安扎根教育，以資安體驗及實作模式，激發學生對於資安知識的興趣。
2. 引導學研體系投入資安跨域實作教學，結合新興科技與跨域知識，促使學生融入實作場域，並擴散師資量能。

（二）養成職場菁英人才

1. 樹立資安菁英培訓機制，邀請國內外資安頂尖專家與學者授課與演練，並建立包含競賽在內的相關人才獎勵制度。
2. 提供實務導師培訓制度，結合業界與學界師資，達成職涯適性資安培育之目標，滿足各產業資安人才需求。
3. 培養跨域研發人才，滿足資安產業與國防需

求，在國內串聯產學研人才培育體系，並與國外著名的產、學研究與教學中心進行合作，全面性培育頂尖資安技術研發人才。

4. 關鍵資訊基礎設施領域相關主管部會提供資安試煉場域，以實戰訓練培育資安菁英及頂尖人才。

（三）建立機動性及彈性延攬資安人才機制

為提升國內外頂尖人才投入我國資安產業，將持續整合各部會資源，建立機動性及彈性延攬資安人才機制與配套措施，提升我國資安產業研發量能。

（四）建立並落實資安人才培育藍圖

為強化我國資安人才培育，跨部會建立資安人才職能地圖及培育藍圖，以提升資源運用的成效。

第三節 推動國防資安自主研發，提升產業成長

一、我國資安產業面臨的困境

我國資安自主產業受限於國內市場規模，面臨三大困境，包含自主研發產品難以形成資安整合解決方案、研發人力不足及外銷市場拓銷不易。

（一）自主研發產品難以形成資安整合解決方案

我國資安自主研發廠商屬中小型企業，沒有足夠資源開發出符合市場需求的資安整合解決方案，缺乏與大型資通訊業者合作開發出符合市場需求的資安產品或服務等機會；此外，部分代理商也自行開發資安工具，致欠缺與自主研發廠商合作開發與行銷產品的誘因。

（二）資安研發人力不足

本土資安業者相較於國外公司規模較小，進而產生資安人才留才困難。此外，資安跨域整合人才培養不易，致使多數本土資安業者面臨研發人力短缺現象，與國際知名資安廠商競爭日益嚴峻。

（三）外銷市場拓銷不易

由於多數本土資安業者規模相對較小，難以承擔昂貴的國際品牌行銷費用與龐大的在地化服務成本，成為本土資安業者拓展海外市場的瓶頸。

二、滿足國家安全防護之資安產業自主研發策略

世界各國面對涉及國家安全的產業，多數以推動自主研發為目標，藉此維護國家安全。因此，我國也擬訂

策略，以滿足國家安全防護所需的資安自主研發，並推動以資安融合資通訊產業之發展（如圖 9 所示）；結合民間社群發展資安創新創業，帶動資安產業升級，並提升資通訊產品附加價值，形成資安產業聚落與生態體系，進軍國際市場。

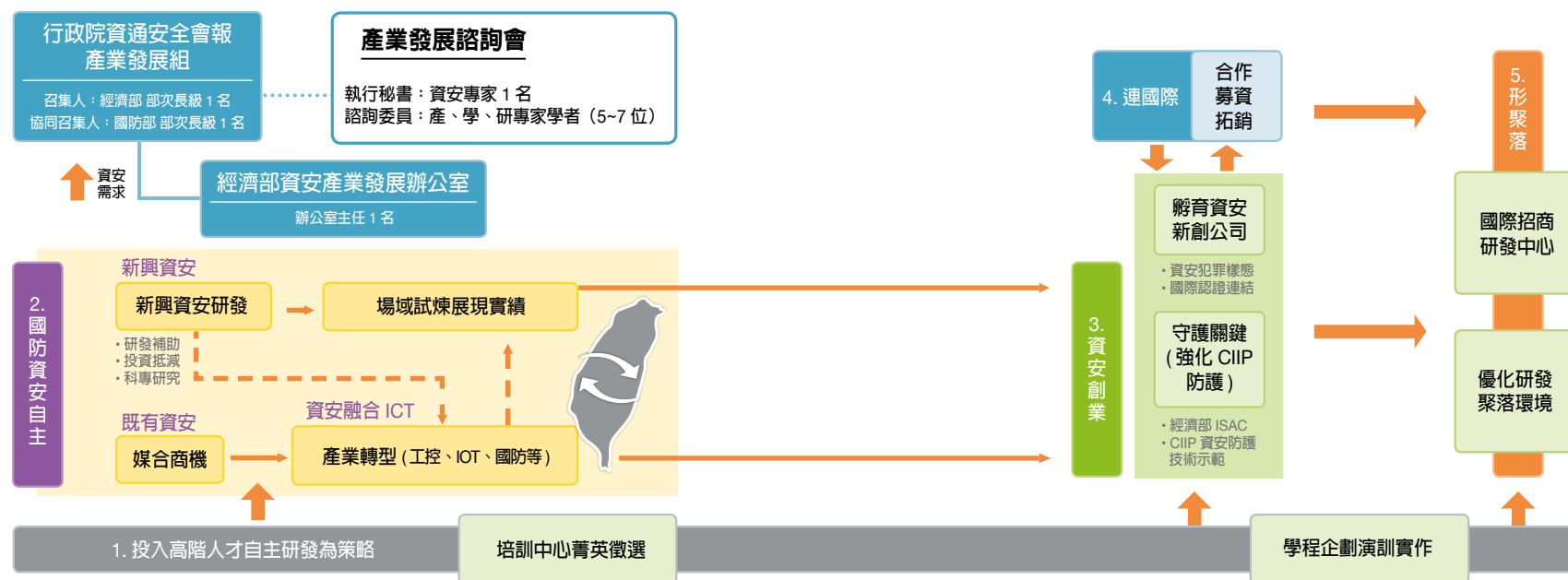


圖 9 滿足國家安全防護之資安產業自主研發策略

（一）推動資安自主研發，帶動資安產業升級

我國自主研發資安廠商長期布局於利基型資安工具、產品或服務，具有相當競爭力，可透過政策引導國內自主研發資安廠商，發展軍民兩用資安產品或服務，不僅可強化我國關鍵資訊基礎設施的資安防護能量，更可達成資安產品及服務輸出目標，以完善我國資安產業生態體系。

1. 政府相關單位引導我國資安傑出廠商或團隊，結合研究法人及學研能量，研發「國家安全防衛所需資安整合性」的產品或系統，帶領資安產業升級轉型。

2. 政府相關單位應鼓勵國內自主資安研發廠商投入八大關鍵資訊基礎設施的防護設備研究開發、攻防演練或資安健診等領域，落實「資通安全管理法」等各項規定，包含研議資安產品採購及創新相關法規優化措施，擬定我國八大關鍵資訊基礎設施資安測試場域的開放策略，以跨領域合作為核心，建構新興資安系統解決方案，布局前瞻資安技術，開創新型態資安產品與服務產業。
3. 邀集國內資安自主研發廠商共同規劃，以建立工業控制系統人才、設備和產品等相關認證機制，讓我國資安自主研發技術升級至工業控制系統及物聯網領域。

（二）推動資安融合，提升資通訊產品附加價值

隨著歐盟及美國對於資通訊產品的資安要求日益增加，使國內資通訊大廠所生產的產品資安防護能力難以符合歐、美相關法規要求的風險。

政府相關單位將邀集資通訊產業公協會與資安產業及工業控制等跨域產業籌組國家旗艦團隊，搭配資安實測場域訂定相關產業資安設計檢認證機制，並連結「智慧機械」、「亞洲・矽谷」、「綠能科技」、「生醫產業」、「國防產業」、「新農業」及「循環經濟」等 5+2 產業創新計畫及相關科專計畫，研發資安技術及開發資安產品與服務，淬鍊整體資安解決方案。除可強化資通訊設備的資安防護強度，提升資通訊產品附加價值外，更能淬鍊我國資安產品深度與成熟度，加速擴展國際市場。



（三）鼓勵新興資通安全應用領域，發展創新創業

隨全球資安威脅趨勢由資通訊領域擴散至物聯網及關鍵資訊基礎設施等領域，資安產業更需具備跨域整合之廠商或人才投入。

因此，政府相關單位將要求關鍵資訊基礎設施投入足夠資安防護資源，並透過開放關鍵資訊基礎設施資安測試場域，強化學研與新興資通安全應用領域連結，以業界出題學研解題的模式，建構新創資源整合平臺。

同時，將有意願創業的民間社群能量導入資安創新創業體系，包含創業社群建立、競賽、獎勵、企業經營輔導及合作輸出等機制。成立創業加速器與具潛力的資安新創團隊共同合作，讓資安新創團隊快速連結市場，以充實我國國家資安自主防衛能量。



（四）培育高階自主研發人才

為健全我國資安產業環境，培育資安人才是產業永續發展的重要關鍵因素，對內積極投入資安產學合作計畫，對外引進國際資安培訓資源合作，透過菁英徵選與實作演練，以培育國內高階資安種子師資，同時扶植企業界與學界建立或提升專責培訓單位能量，匯集產、學、研能量共同投入高階自主研發人才培育，建置我國資安自主培育體系。以接軌資安產業用人需求，強化我國關鍵資訊基礎設施人才防衛能力。



（五）活絡資安投資並鼓勵國際輸出

- 1.強化國際輸出量能，行政院資通安全會報除於國內建構資安產品淬鍊場域、完備資安設計檢認證機制外，更將積極參與國際資安或產業標準制定，以掌握資安產業發展趨勢，並提升國際資安標準介接程度。
- 2.引導及獎勵國內外各項基金或資金投資我國優質、具潛力資安公司，擴大資金量能，以挹注新興資安技術研發，開拓國際品牌。
- 3.邀請國內資安廠商及相關公協會，了解國際輸出所遭遇困難，並連結公協會籌組資安產業推動服務團，擬定資安國際輸出策略及規劃執行藍圖。

第四章、結語

政府將以「國家資通安全戰略報告」為上位指導方針，提出各期「國家資通安全發展方案」，並由各部門依資安治理層級推動執行，落實前述「資安即國安」戰略的三大目標；未來應持續完備資安量能，努力方向包括：

第一節 持續優化國家資安機制

- 一、因應我國家數位化與科技化發展，以及國際資安法規發展趨勢，完備我國資安相關法規修法及立法，並與國際公約連結。

- 二、持續優化我國資安整體運作機制，並逐年依我國家數位化與科技化發展，以及相對應的資安風險，調整行政院國家資通安全會報內各組的角色及任務目標。

第二節 強化國家資安體系運作效率

- 一、整合資訊安全至各式預警與應變計畫中，並建立全民與跨公私部門的全國資安預警機制，加強與企業合作，並連結國際組織及其他國家，強化我國資訊安全。
- 二、強化資安執法單位與民間社群合作調查與預防機制，如鼓勵通報資安犯罪、既有軟體與系統之弱點與修復機制。

- 三、促進與發展公私領域之網路空間安全夥伴關係，透過協作增強互信，以強化共同防衛與鼓勵資訊分享與分析的機制。
- 四、發展保護關鍵資訊基礎設施的全面性計畫，建立關鍵資訊基礎設施風險及危機管理機制，並建構中央與地方政府合作夥伴關係，以領導公私領域制定資安威脅與風險評估機制及綱要。
- 五、持續推動資安科技跨國或跨組織的國際合作。

第三節 完備資安自主產業生態體系

- 一、持續運作產、政、學、研共同合作與協調平臺，以適時反映資訊安全產業發展困難，分別就資安組織機制、法規標準、人才培養、活化投資及新興跨域技術深耕等，提出對應的資安產業發展策略。

- 二、持續針對資安產業輔導或獎勵等科研資源進行投入及產出效益分析，匯集產、學、研能量共同研擬我國資安技術與發展地圖，投入前瞻資安及新興應用研究，以滿足國際資安風險管控架構、資安產業及資通訊發展所需，減緩新興資安威脅。
- 三、持續修調資安留才及跨域人才培育策略，匯集產、學、研能量建立資安職能地圖與自主培訓體系，強化接軌國際資安相關教育訓練與認證機制，以滿足國家資安聯防體系與資安產業自主研發需求。
- 四、於國內成立單一服務窗口，號召資安產業與資通訊產業合作打造臺灣製造的共同品牌；對外持續整合及運用外交資源，引導國外各項基金、資金或創投資源投資我國優質、具潛力之資安公司，並協助資安產業參與國際展覽，達成連結國際行銷人脈、吸取國際行銷經營經驗，以開拓國際品牌。

附錄、專有名詞英文對照表

- | | |
|-------------|---|
| 1. 釣魚郵件 | Phishing Email |
| 2. 勒索軟體 | Ransomware |
| 3. 虛假訊息 | Disinformation |
| 4. 虛擬貨幣 | Virtual/Crypto Currency |
| 5. 關鍵基礎設施 | Critical Infrastructure (CI) |
| 6. 關鍵資訊基礎設施 | Critical Information Infrastructure (CII) |
| 7. 物聯網 | Internet of Things (IoT) |
-

- | | |
|-------------------|--|
| 8. 資安維運及預警中心 | Security Operation Center (SOC) |
| 9. (資訊) 情資分享及分析中心 | Information Sharing and Analysis Center (ISAC) |
| 10. 緊急應變團隊 | (Computer) Emergency Response Team (CERT) |
| 11. 國際公約 | International Convention |
-

國家圖書館出版品預行編目(CIP)資料

國家資通安全戰略報告-資安即國安 /
國家安全會議國家資通安全辦公室作.
-- 臺北市: 國安辦, 民107.09
面; 公分
ISBN 978-986-05-5818-0(平裝)

1.國家安全 2.國家戰略 3.資訊安全

599.8

107006656

書 名：國家資通安全戰略報告 - 資安即國安

著作權人 / 國家安全會議

發行人 / 國家安全會議 李大維秘書長

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 李德財諮詢委員

出版者 / 國家安全會議 國家資通安全辦公室

出版年月 / 2018 年 9 月

1010100

011101010100

00101011101010100

我國首部資安戰略報告，
強化全民資安意識、凝聚各界共識，
為數位國家、創新經濟奠定堅實基礎

1101010100

101011101010100

1110100101011101010100



GPN: 101-070-1465

定價：新台幣150元