國家安全會議
NATIONAL SECURITY COUNCIL

台灣資安的未來10年-以國安面向思考

李漢銘諮詢委員

2021.11.26

國家安全會議
NATIONAL SECURITY COUNCIL

報告大綱

第一部分	1.0執行成效、複合威脅與趨勢
第二部分	2.0戰略架構
第三部分	推動策略與發展方案

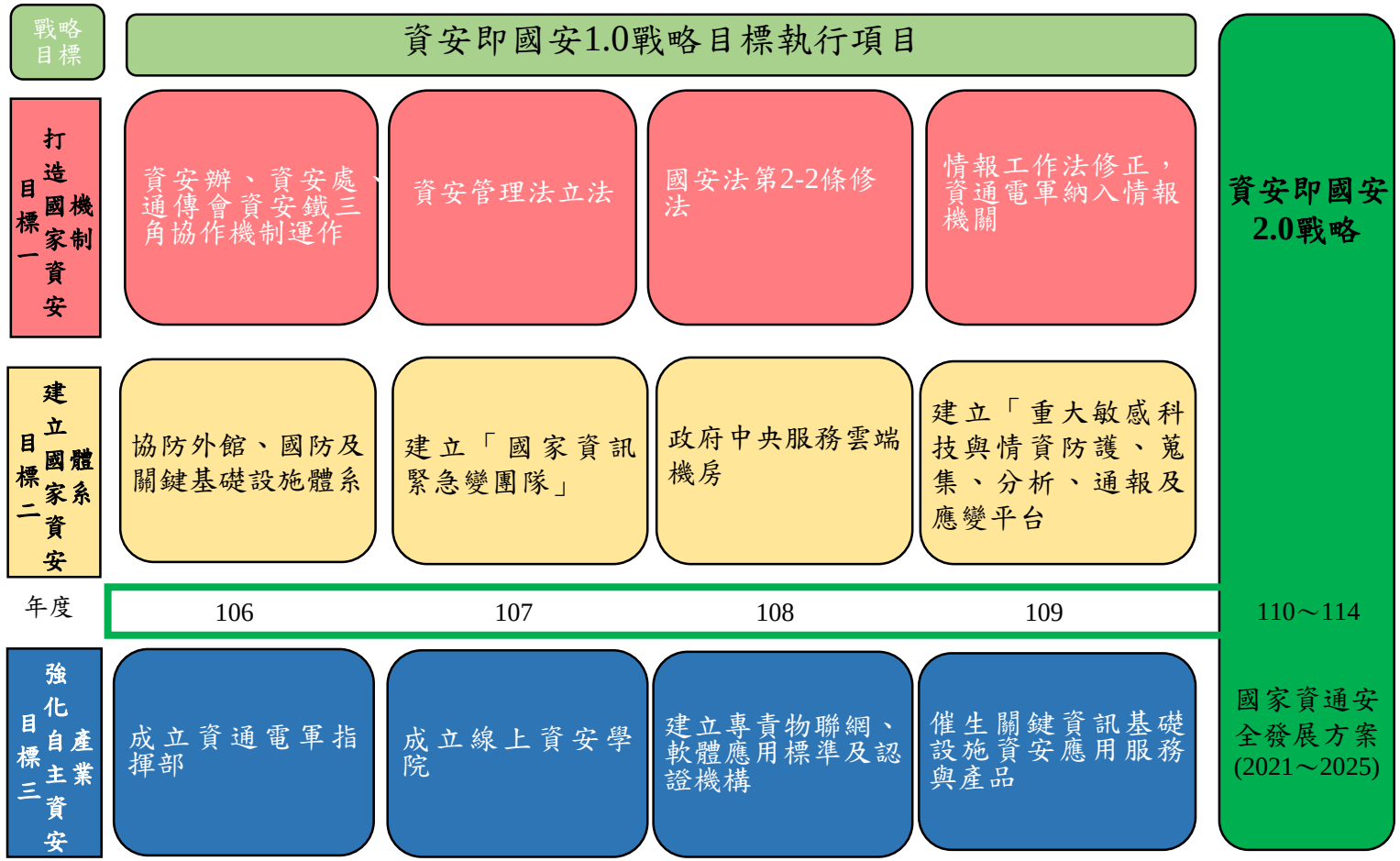
第一部分

1.0執行成效

政策依據

複合威脅與趨勢

資安即國安戰略 1.0 成效



	資安即國安1.0
組織	成立行政院資通安全處
法制	實施資安管理法、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

國家安全會議
NATIONAL SECURITY COUNCIL

政策依據

總統政見與指裁

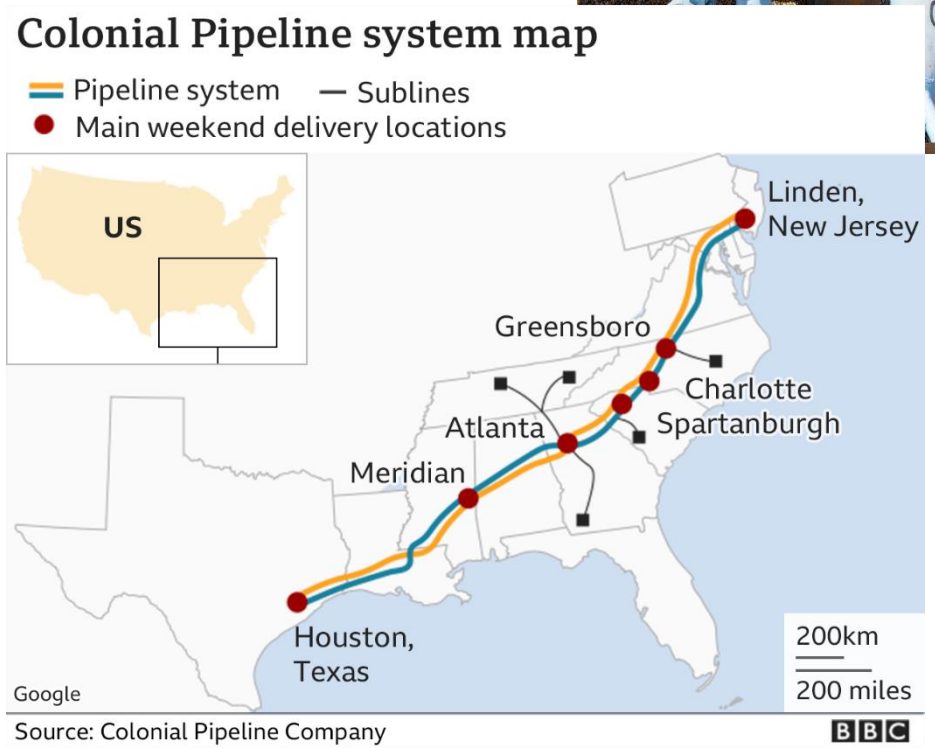
- 守護台灣安全的三道防護網第二道防護網：**資訊安全防護網**。
- 在5+2產業創新的既有基礎上，以**資安產業**貫穿「六大核心戰略產業」，讓台灣成為未來全球經濟的關鍵力量。
- 面對嚴峻的國際情勢，必須提高戰略思維層級及**更完善的資安對應策略**，發展台灣的數位科技實力及維持國家產業的核心競爭力。
- 限期完善資安的**組織結構**、**人力**與**資源配置**及強化國家資訊安全團隊（**質與量**的提升）。
- 調整國安會與行政院的資安推動組織架構。

資安專案會議指裁

- 資通安全規範之落實:強化CI防護、維護計畫、資安稽核、聯防機制(ISAC、CERT、SOC)。
- 資安法排除之軍事及情報機關的資安稽核強化。
- 完備政府單位、公營事業與關鍵基礎設施之資安需求，驅動資安產業。
- 研擬資訊資安委外廠商管控(含廠商評鑑、違約究責、監理稽查)精進作為。

美國最大燃油管道系統Colonial Pipeline遭勒索軟體攻擊，美國宣布進入緊急狀態

- **背景說明:**美國最大燃油管道系統Colonial Pipeline今年5月7日遭到勒索軟體攻擊，Colonial Pipeline負責美國東岸多達45%的燃料供應，每天運送多達1億加侖的汽油、柴油、航空媒油與家用燃料油，也負責美國7個機場的燃油供應。並因攻擊事件而暫停所有的管道作業，此事讓美國政府於宣布進入緊急狀態（State of Emergency）。



國家安全會議 NATIONAL SECURITY COUNCIL

產業面臨資安事件挑戰日益加劇

企業在2023年因資安攻擊財損將超過500億美元

	聯網帶來資安事件暴增	國際供應鏈安全要求	工控IT化非傳統資安方案可解
產業問題			
實際案例	 01 2021年5月美國最大燃油供應業者Colonial Pipeline遭勒索軟體攻擊，暫停所有輸油管線運作，對此美國共18州進入緊急狀態	 02 2018年8月台積電產線中毒事件、2021年4月廣達遭駭勒索14億事件，引起國際大廠將供應鏈安全納入RFP	 03 2017年底中東一家石油工廠發生設備故障，導致產線中斷，為首個專門針對工控安全系統惡意程式攻擊的案例
產業需求	疫情下，遠端作業帶來更高的**資安風險**	資安已成為國際供應鏈**採購「門票」**	傳統資安解決方案難以因應**新興挑戰**

資料來源：經濟部工業局

國家安全會議 NATIONAL SECURITY COUNCIL

微軟exchange漏洞、solarwindn及最大燃油管系統Colonial Pipeline遭勒索軟體攻擊，美國相關行政作為

發布間	形式	發布人/單位	名稱	關注面向
2021.05.12	行政命令	總統	Executive Order on Improving the Nation's Cybersecurity(改善國家資安行政命令)	1. 軟體供應鏈攻擊之應處 2. 改善聯邦政府網路安全
2021.05.28	資安指示	國土安全部(DHS)	Security Directive-pipeline-2021-01(針對油管勒索事件之資安指示)	油管業者(關鍵基礎設施提供者)之資安與通報應變機制： 1. 規範油管運輸業者通報資安事件 2. 要求油管運輸業者檢視資安防護
2021.06.02	公開信	副國安顧問 Anne Neuberger	What We Urge You To Do To Protect Against The Threat of Ransomware	因應勒索軟體攻擊： 1. 提供企業勒索軟體防範指引 2. 籌組勒索軟體工作小組，並通知全美檢察官對勒索軟體之調查工作，應於前述工作小組及中協調
2021.06.04	內部指南	司法部(DOJ)	Memorandum for All Federal Prosecutors	

白宮邀集民間產業代表召開資安會議

科技巨擘承諾增加網路安全投資

- 因應自去年12月起網路管理公司SolarWinds、關鍵輸油管道公司Colonial Pipeline(2021年5月)、全球最大肉品加工廠JBS(2021年7月)接連爆發網路攻擊事件後，網路安全已成為拜登政府重要任務
- 2021年5月拜登簽署「改善國家網路安全」總統令
- 2021年8月白宮邀集科技業、金融業、能源產業、保險業及大學共商官民合作資安防護

科技巨擘紛紛響應，承諾未來增加網路安全投資：

	Microsoft	Google	IBM	Amazon	Apple
投資金額	200億美元	100億美元	–	–	–
技術研發	–	零信任、軟體供應鏈、開源軟體安全性	量子計算、量子加密	雲端運算、多重身分認證	雙因素認證、漏洞修復、事件紀錄及應變
供應鏈安全	提供政府1.5億美元技術服務	強化軟體供應鏈安全	–	–	要求所有蘋果供應鏈業者符合供應商安全規範
資安人才培育	擴大培訓合作	10萬人	15萬人	免費資安課程	–

資料來源：經濟部工業局

美國政府攜手民間產業推動網路防禦計畫

官民合作加強資安聯防

- 美國網路安全暨基礎架構安全管理署(CISA)與民間科技公司發展強化「資安聯合防禦協作」計畫，成立聯合防禦中心共同防制勒索攻擊等各種資安威脅

參與單位與業者

- ✓ **政府機關**：美國網路作戰指揮部、國防部、國安局、聯邦調查局、司法部、國家情報總監辦公室
- ✓ **科技業者**：AWS、Google Cloud、Microsoft
- ✓ **電信業者**：AT&T、Verizon、Lumen、
- ✓ **資安業者**：Crowdstrike、FireEye Mandiant、Palo Alto Networks

聯合防禦中心主要工作項目

- 設計實施全國網路防禦計畫
- 情資分析與共享
- 整合網路防禦能力
- 計畫與合作的機動性
- 制度化演練與評估
- 與特定風險部門密切合作

資料來源：經濟部工業局

國家安全會議 NATIONAL SECURITY COUNCIL

歐盟與美國提出網路安全認證架構

ICT產品未來必須通過網路安全認證才能銷售

- **由歐盟網路與資訊安全局(ENISA)**負責推行**「網路安全認證機制」，已研擬基於通用標準(CC認證)的歐洲網路安全驗證規範EUCC，並提交歐盟執委會及會員國進行意見徵詢、預計2023年開始在部份國家施行**
- EUCC驗證方案包括資通產品、**資訊服務及資料處理流程**，將依資安風險程度在證明書上區分低、中、高三個安全級別
- **美國拜登總統令**，也要求2022年規劃**物聯網設備**與**軟體**的「**網路安全標示計畫**」，協助使用者在採購前了解產品的資安風險

網路安全認證對市場帶來以下效益

產品或服務提供商(中小企業和新創)

廠商獲得進入歐盟單一市場的門票：借由該機制獲得歐盟證書，提升競爭力

公民和最終使用者(如：基礎設施運營商)

消費者事先瞭解聯網設備資安風險：可藉由ENISA的網路安全認證網站諮詢產品的資安資訊

個人、商業買家和政府

採購產品或服務前的抉擇：可以藉此機制讓產品或服務的資訊透明化，做出更好的抉擇

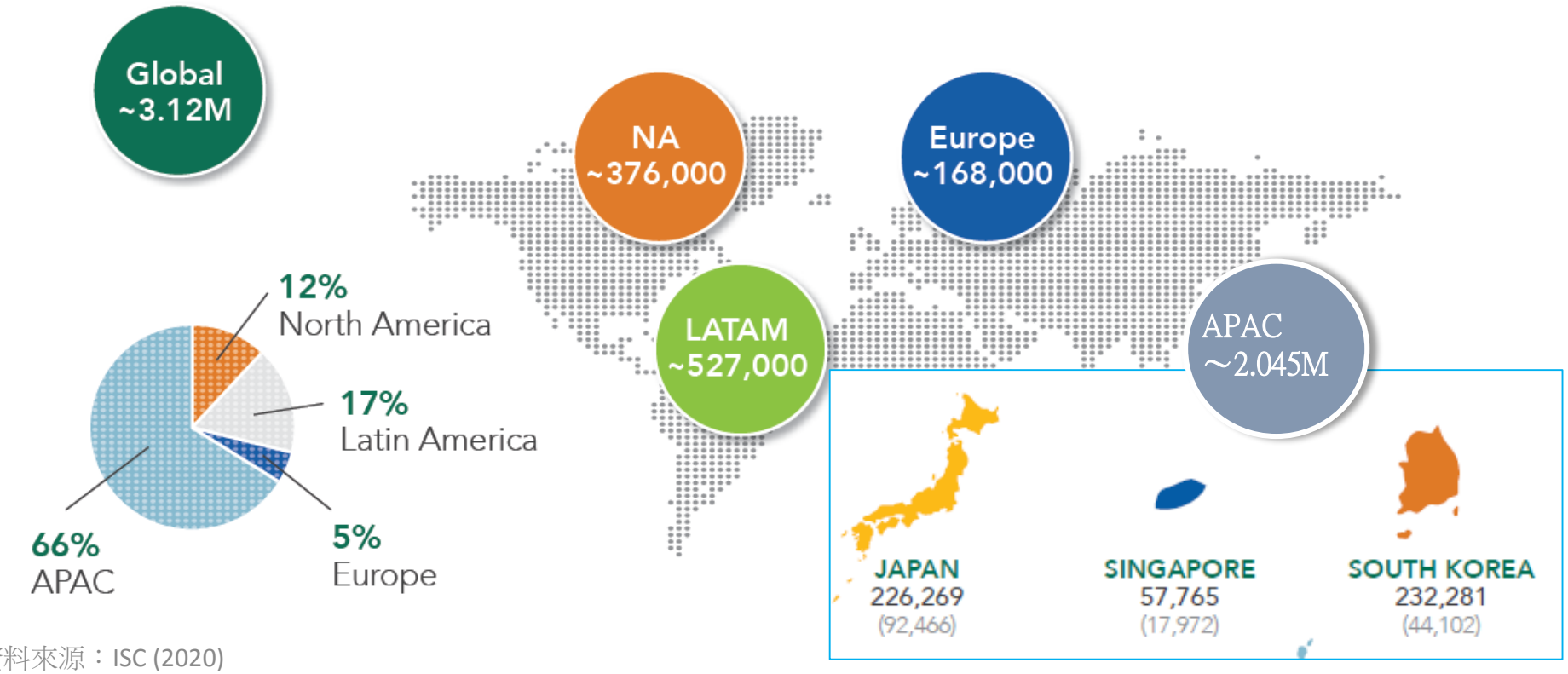
資料來源：經濟部工業局

國家安全會議
NATIONAL SECURITY COUNCIL

全球資安人才告急

亞太地區資安人才缺口達200萬人

- 根據「國際資訊系統安全認證協會」(ISC)在2020年的全球資安人力研究 (Cybersecurity Workforce Study) 指出，**全球資安人才短缺達312萬，亞太地區缺乏資安人才最為嚴峻**
- 美國大約有87.9萬名現職資安專業人員，但還缺乏35.9萬的資安人才；日本、韓國、新加坡缺口都在**數萬人**以上



資料來源：ISC (2020)

國家安全會議 NATIONAL SECURITY COUNCIL

供應鏈安全與產品資安為產業重要議題

國內市場太小

臺灣國內市場不足以支撐資安產業大幅成長

- ✓ 攻擊事件頻傳，臺灣產業整備程度落差大
- ✓ 中小型企業需要簡單的一站式方案和有效量化資安投資回報(ROI)的方法

供應鏈安全

供應鏈安全被視為國內企業必須正視的一部分

- ✓ 國際大廠將要求第三方協作廠商證明強化資安防護管理

高質化資安產品

國內資安仍以特定解決方案為主

- ✓ 國內資安業者跨業合作，發展具國際競爭力之資安解決方案，雲端解決方案

培育資安獨角獸

全球資安獨角獸募資屢創新高、但臺灣新創還沒出門

- ✓ 臺灣新創以技術開發為主，缺乏與市場、資金提供者溝通的能力

資安人才

臺灣資安人才如何找？

- ✓ 臺灣駭客社群蓬勃發展，但國內缺乏資安技術產品化能力的人才、以及產業防禦型人才

資料來源：經濟部工業局

國家安全會議
NATIONAL SECURITY COUNCIL

威脅情勢評估

對象 高價值 / 敏感資料擁有者
關鍵基礎設施, 高科技產業

弱點

手法 APT
Ransomware
DDoS…

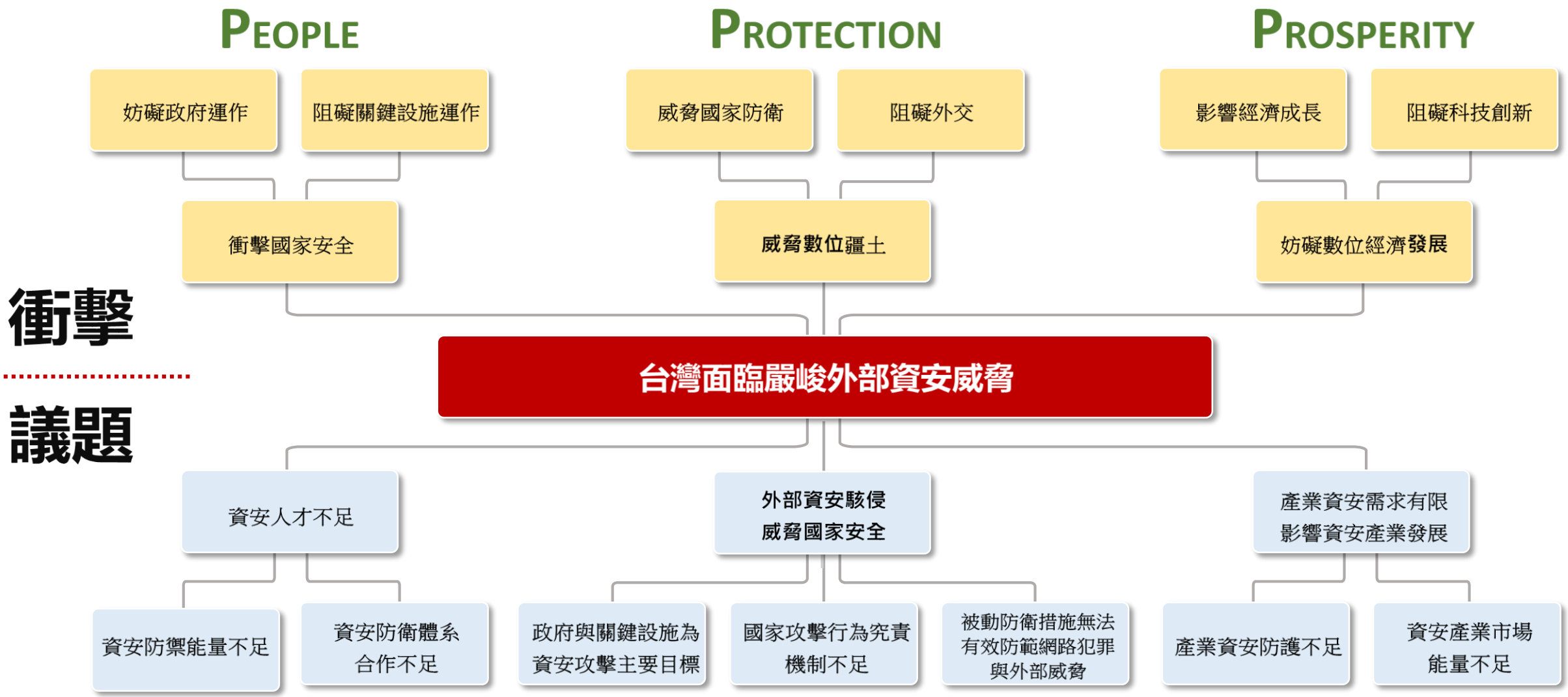
國安威脅趨勢分析：

- 以經濟貿易戰、數據戰、輿論戰等為核心的複合式操作的新型態戰爭
- 資安法需要時間落實，精益求精的威脅，尋找整體防護的弱點
- 手法特色：APT精準打擊、合法掩護非法（如遠端連線）

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、商用電郵系統、雲端服務
資金	股權結構、外包	事務所	資通訊廠商、戶政委外公司
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）
腦	爭議訊息	各國大選	飛機投共

國家安全會議
NATIONAL SECURITY COUNCIL

政策分析



國家安全會議
NATIONAL SECURITY COUNCIL

主動防禦趨勢

主動防禦機制

後盾：威脅情報、數據、資安分析

執行者	政府與關鍵基礎設施防護團隊
	根據攻擊者的駭侵行為
（強化） 主動式應變	• 鑑識潛在入侵者 • 清除後門與惡意程式 • 主動阻斷攻擊來源 • 重新配置資安防護縱深

目標

1. 早期預警
2. 緊急應變
3. 持續維運

第二部分

2.0戰略架構

國家安全會議 NATIONAL SECURITY COUNCIL

資安即國安2.0戰略架構

願景：資安即國安 2.0－打造堅韌、安全、可信賴的智慧國家

主軸	PEOPLE	PROTECTION		PROSPERITY
目標	充實資安卓越人才	強化人民家園安全防護	鞏固資安外交網路防禦	促進產業繁榮發展
策略	T 培育資安卓越人才聯合作戰機制	R 提升防護韌性	U 促進資安國際合作，建構國內外聯防體系	S 發展精實防禦機制，打擊網路犯罪	T 產業落實資安驅動資安產業
	Talent	Resilience	Unity	Security	Technology
做法	1. 強化資安特戰能力，培育卓越與實戰人才 2. 建構聯合作戰機制、推動公私協同治理 3. 完備資安組織架構	1. 強化弱點管理，提升公私數位聯防與應變能力 2. 國家層級的資安風險盤點與評估，研發關鍵技術 3. 資源向上集中，盤點關鍵系統、網路架構	1. 深化國際情資分享 2. 擴大國際參與，聯合理念相近夥伴 3. 鞏固友邦發展數位資安外交	1. 賡續落實資通安全管理相關規範 2. 提升科技主動偵查、網路溯源分析能量 3. 完善網路法規與標準程序，建立查核制度	1. 落實六大核心戰略產業資安導入 2. 提升資安產業自主能力，發展新領域資安能量 3. 接軌國際規範
行動方案	國家資通安全發展方案				

國家安全會議 NATIONAL SECURITY COUNCIL

整體資安防護整體架構行動方案

行政院第六期資通安全發展方案

願景：打造堅韌安全之智慧國家

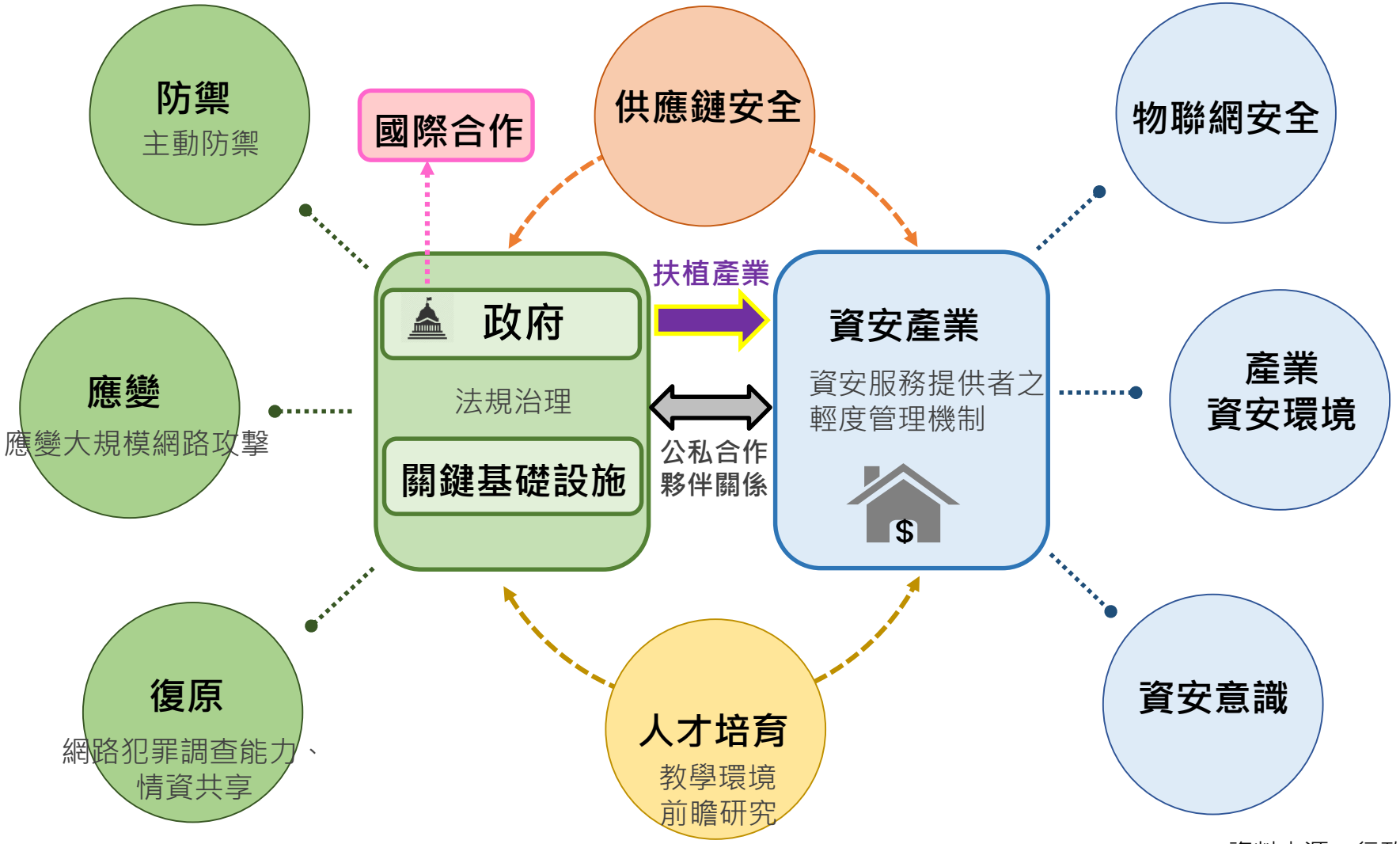
目標：
- 成為亞太資安研訓樞紐
- 建構主動防禦基礎網路
- 公私協力共創網安環境

推動策略	具體措施
吸納全球高階人才 培植自主創研能量	1. 擴增高教資安師資員額與教學資源 2. 挹注資源投入高等資安科研 3. 培育頂尖資安實戰及跨域人才
推動公私協同治理 提升關鍵設施韌性	1. 建立各領域公私協同治理運作機制 2. 增強人員資安意識與能力建構 3. 公私合作深化平時情資交流與應變演練
善用智慧前瞻科技 主動抵禦潛在威脅	1. 賡續推動政府資訊(安)集中共享 2. 擴大國際參與及深化跨國情資分享 3. 制敵機先阻絕攻擊於邊境 4. 提升科技偵查能量防制新型網路犯罪
建構安全智慧聯網 提升民間防護能量	1. 輔導企業強化數位轉型之資安防護能量 2. 強化供應鏈安全管理 3. 建構安全智慧聯網

資料來源：行政院資安處

國家安全會議
NATIONAL SECURITY COUNCIL

整體資安防護架構戰略構想



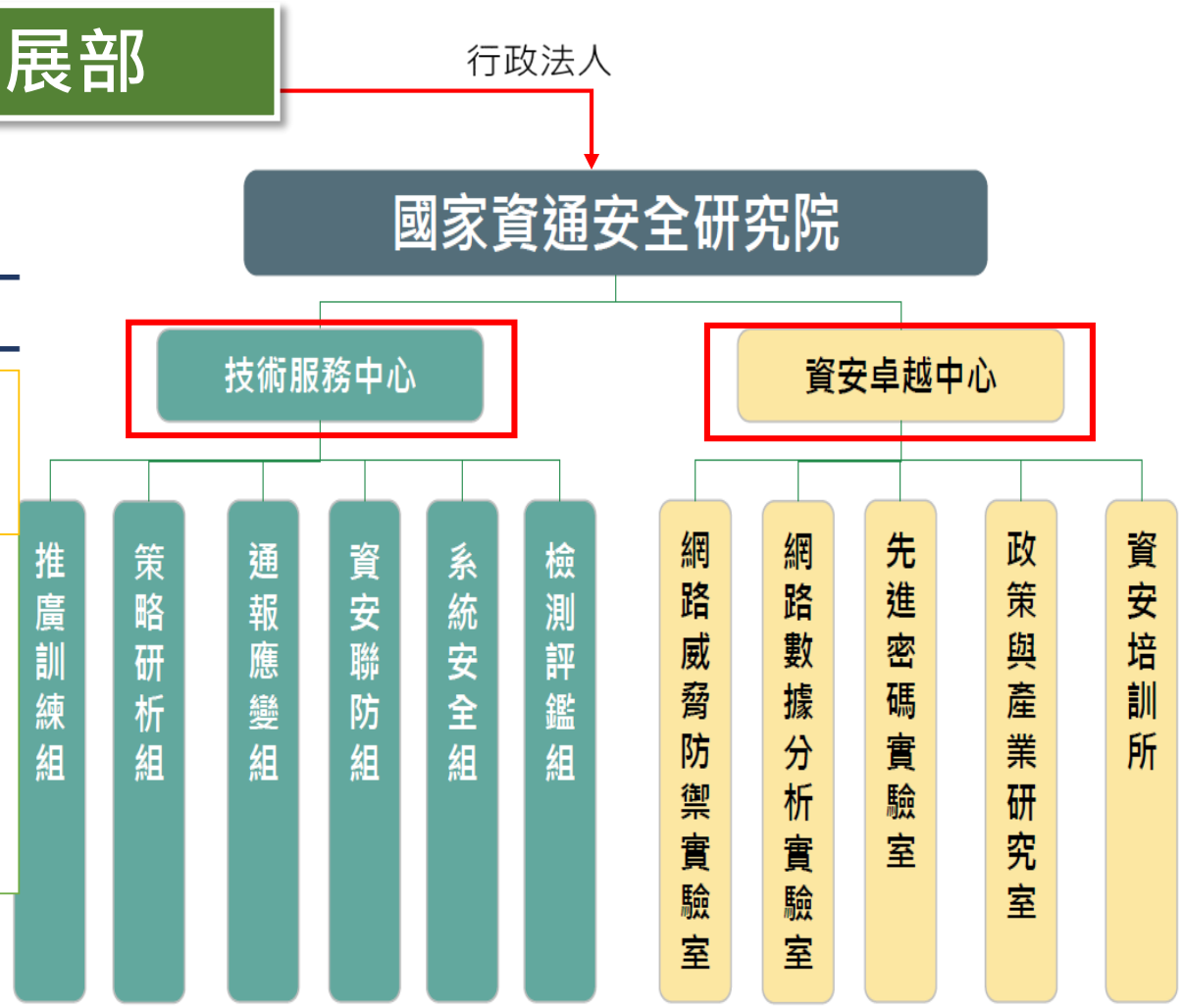
資料來源：行政院資安處

第三部分

推動策略與發展方案

People－培育資安卓越與實戰人才

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

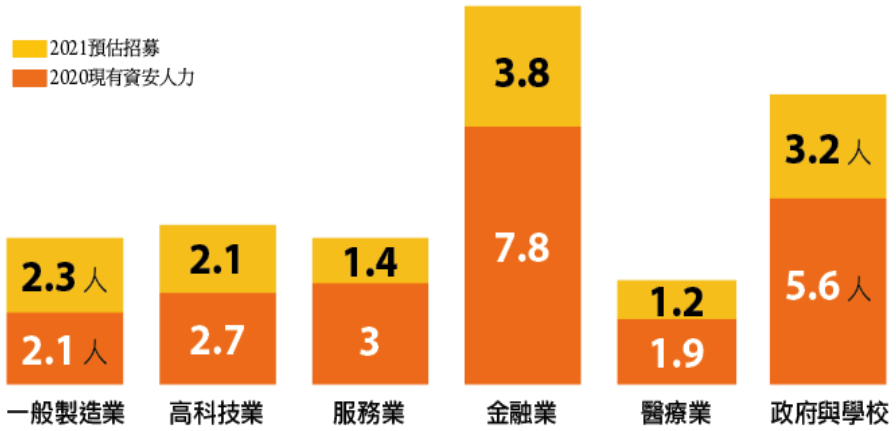


國家安全會議 NATIONAL SECURITY COUNCIL

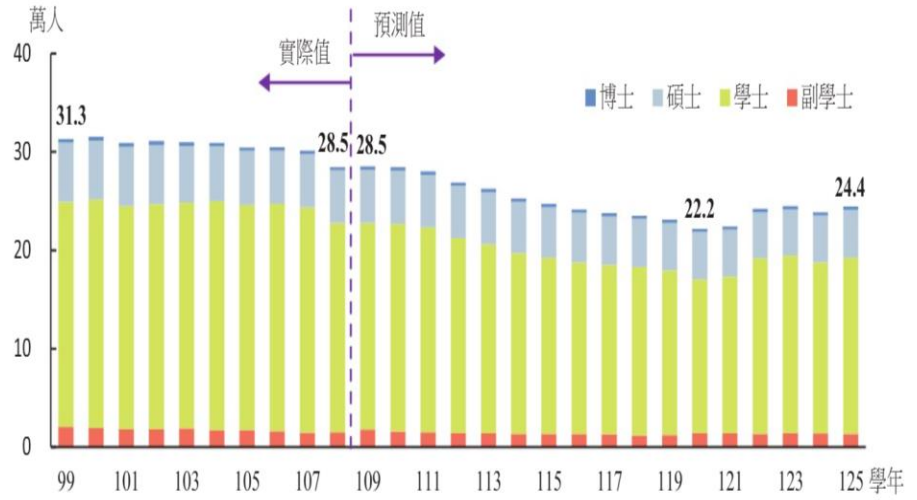
臺灣資安人力現況與需求
國內資安人才供給遠遠不足

- 臺灣資安產業就業人才，2020年達9,000人, **缺額約15%(1,350人)**
- 臺灣資通安全相關專業人才約21,000人, 缺額達**3,800人**, 每年15%成長
- 政府機關也鬧資安人力荒，據資安處統計公務機關資安人力缺額高達**1,024人**
- 在少子化的浪潮下，我國資訊、工程領域大學生10年來減少5萬人，其中學士班含四技，資訊領域學生數從7萬5千人，減少至6萬3千人**(-16.2%)**
- 教育部規劃在2030年達到培育8萬3000名資通訊人才的目標，每年增加資訊系所招生名額10%，但必須與半導體、資訊服務搶人才，**資安人才需求遠遠不足**

各產業平均資安人力現況與需求

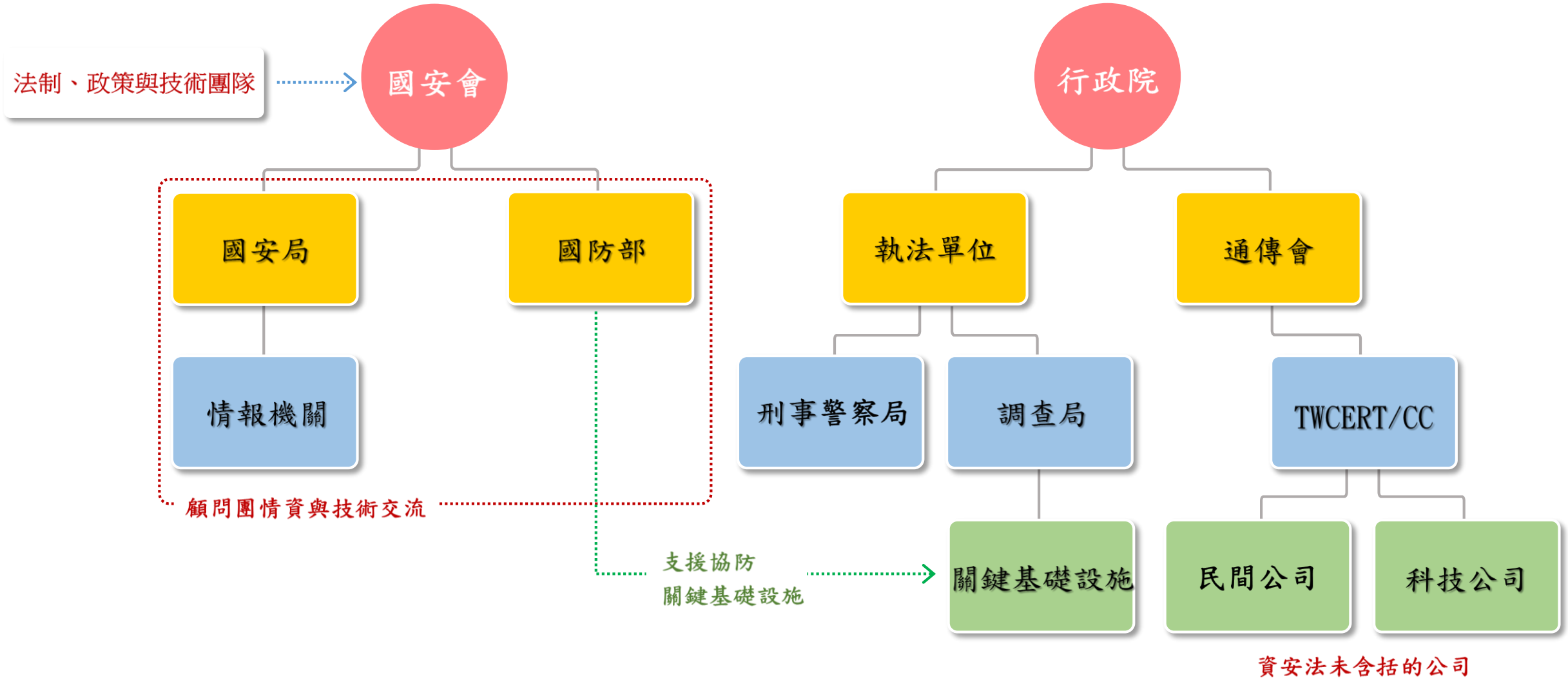


大專院校畢業生人數變化趨勢



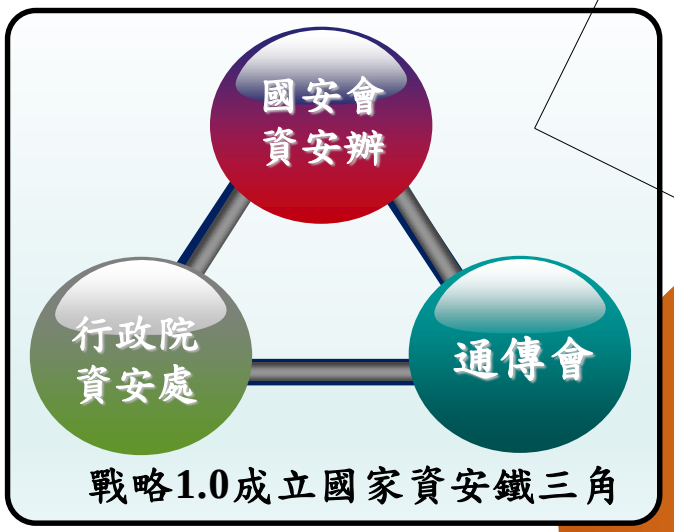
國家安全會議
NATIONAL SECURITY COUNCIL

People－聯合作戰機制：公私協力團隊



國家安全會議
NATIONAL SECURITY COUNCIL

People - 六塊基礎聯防體系



戰略1.0成立國家資安鐵三角

國安會

國安局

國防部
資通電軍

精實防禦機制

調查局

刑事警察局

行政院資安處

戰略2.0成立國家資安六塊基

通傳 金管 經濟 衛福 科技 交通

關鍵
基礎設施

Protection－Resilience：提升防護韌性

一、強化弱點管理，提升公私數位聯防與應變能力

1. 強化委外供應鏈風險管理
2. 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
3. 半導體與高科技公司資安聯防

二、國家層級的資安風險盤點與評估，研發關鍵技術

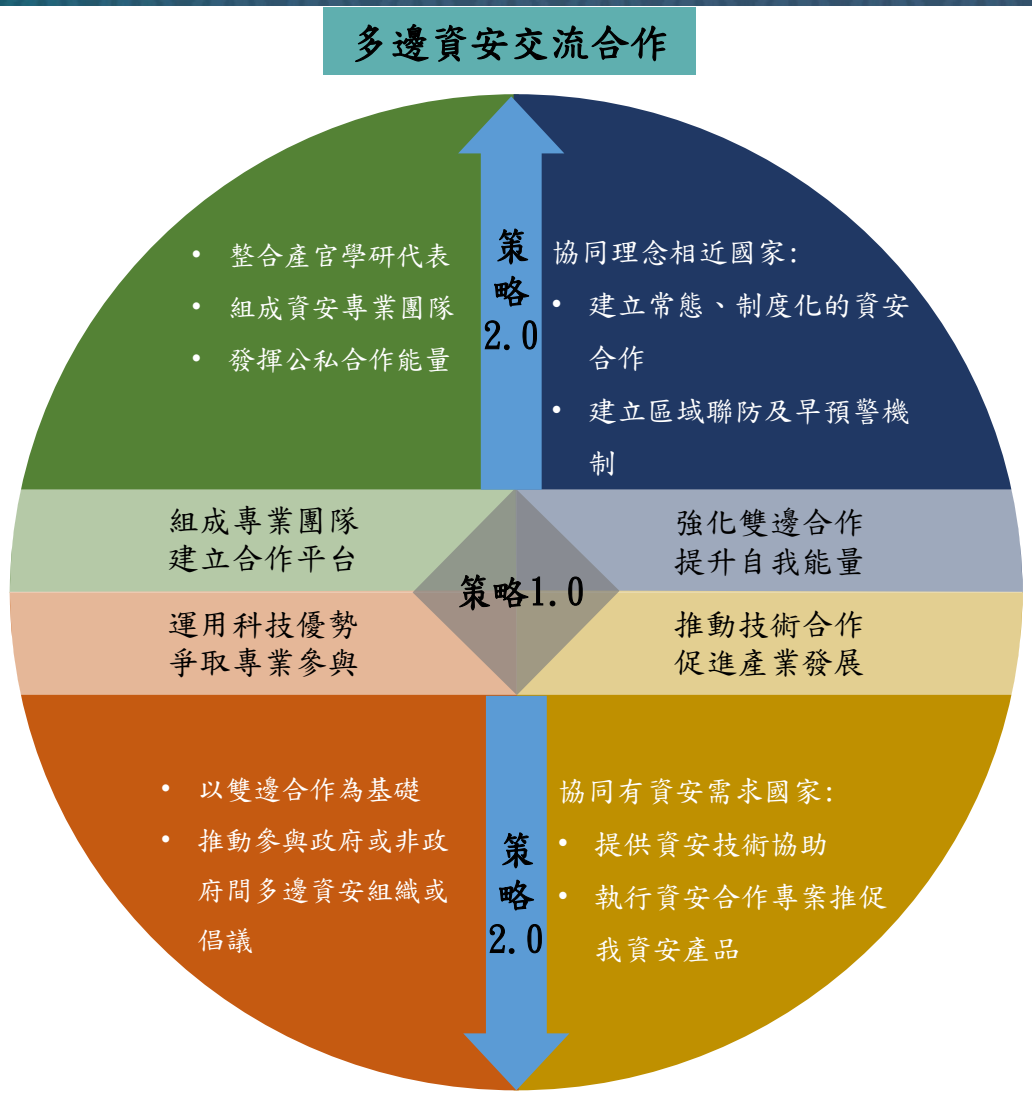
1. 推動國家層級資安風險評估
2. 推動落實關鍵基礎設施資安防護基準
3. 建構工控領域資安治理成熟度

三、資訊資源向上集中策略

1. 機房整併
2. 網路集中出口
3. 機房能源效率改善
4. 共用行政資訊系統

資料來源：行政院資通安全處、國家發展委員會

Protection－Unity：促進參與資安國際合作



做法：

1. 深化國際情資分享
2. 擴大國際參與，聯合理念相近夥伴
3. 鞏固友邦發展數位資安外交

國家安全會議
NATIONAL SECURITY COUNCIL

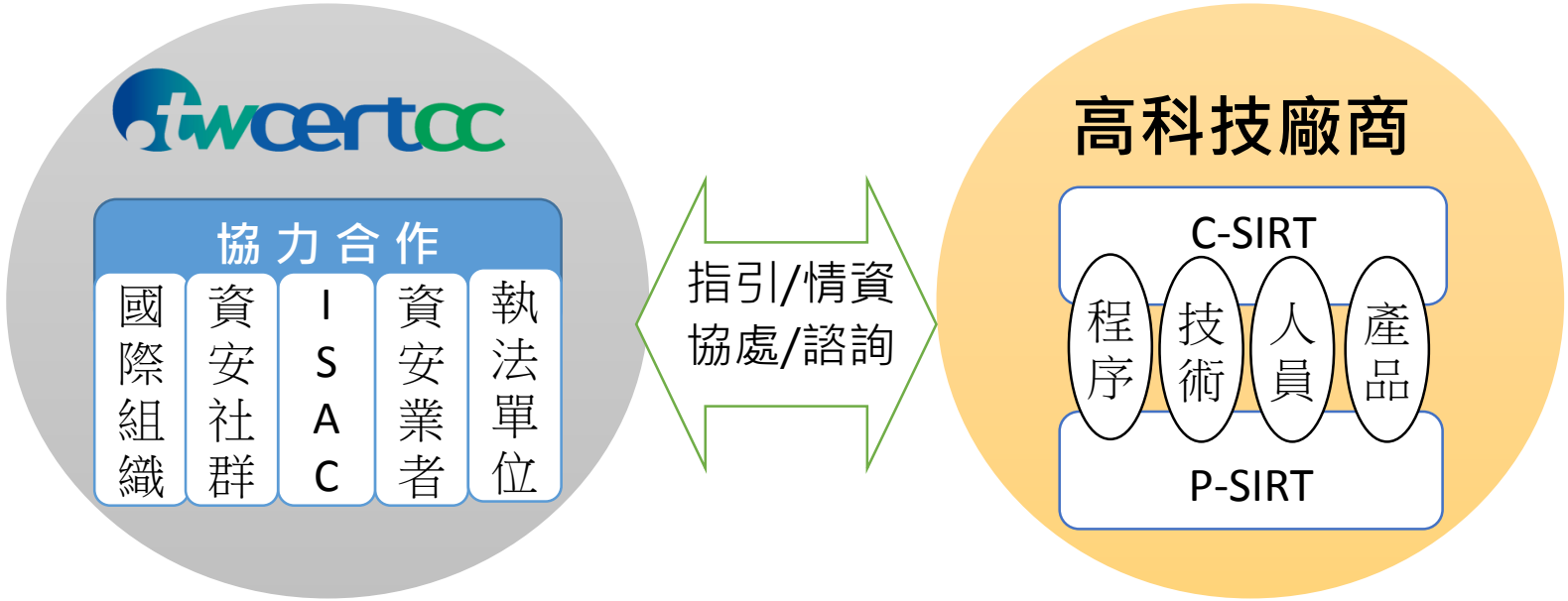
Protection－Security：精實防禦機制

國安局 國防部	【制敵機先阻絕攻擊】 依「資安向前防禦」方針， 從源頭擾亂或阻止境外敵對勢力網路作戰
國境線	
調查局 刑事警察局	【防治新型網路犯罪】 提升資安事件溯源追蹤能力 並加強跨境網路犯罪偵查機制
各部會與政府機關	應變協作
八大關鍵基礎設施	安全韌性
資安產業與資安相關協會	【公私領域協同治理網路空間】 建構與提升公私領域資安情資通報與聯防平台效率

做法：
1. 賡續落實資通安全管理相關規範
2. 提升科技主動偵查、網路溯源分析能量
3. 完善網路法規與標準程序，建立查核制度

公私協力-跨域聯防：精實防禦機制

1. 台積電成立TSMC-SCSA:確保公司的供應商符合資安的標準。
2. 成立SEMI臺灣資安委員會:構建供應鏈資安評估方法，幫助產業增加透明度與可視性。
3. TWCERT/CC協助成立高科技資安聯盟:進行威脅情資共享，促進資安經驗交流與聯防，強化整體資安防護能量。



國家安全會議
NATIONAL SECURITY COUNCIL

Prosperity - 發展具數位實力和國家安全的資安產業

➔ 109年產值：新臺幣552億元

➔ 廠商家數/從業人數：約340家 / 約9,000人

終端與行動裝置防護

2019年產值：新臺幣108.3億元
2020年產值：新臺幣120.9億元

身份驗證、存取控制、防毒/惡意程式防護...

網路安全

2019年產值：新臺幣139.5億元
2020年產值：新臺幣156.9億元

防火牆, IDS/IPS,UTM, APT防護,...

資安營運管理服務

2019年產值：新臺幣50.3億元
2020年產值：新臺幣58.0億元

SOC監控服務、ISAC服務、雲端資產管理...

資安系統整合建置

2019年產值：新臺幣83.8億元
2020年產值：新臺幣90.4億元

資安系統整合、經銷服務...

物聯網安全

2019年產值：新臺幣20.0億元
2020年產值：新臺幣22.3億元

IOT加密模組、ICS Gateway、IC PUF...

資料與雲端應用安全

2019年產值：新臺幣26.5億元
2020年產值：新臺幣30.4億元

Email安全、WAF設備、內容過濾軟體、資料庫安全...

資安檢測鑑識顧問服務

2019年產值：新臺幣61.7億元
2020年產值：新臺幣69.5億元

資安顧問、資安驗證、稽核鑑識、資安檢測...

資安支援服務

2019年產值：新臺幣3.3億元
2020年產值：新臺幣3.7億元

資安教育訓練、資安保險服務...

方案：

1. 六大核心戰略產業資安導入。
2. 提升資安產業自主能力，發展新領域資安能量。
3. 接軌國際規範。

國家安全會議
NATIONAL SECURITY COUNCIL

資安精進作為
供應鏈安全

1. 強化產業供應鏈安全

① 建立接軌國際之IoT資安檢測標準及驗證體系

② 輔導產業導入國際資安治理成熟度認證(如CMMC)

③ 提高供應商SSDLC能力及資安法遵

④ 公私協力推動各產業領域ISAC及資安防護聯盟

2. 加速資安產業成長

① 透過六大戰略產業與前瞻基礎建設，加速政府及產業數位轉型，以擴大國內資安市場

② 連結國際資金及市場，扶植born global資安新創，以加速資安產業國際化

③ 導引我國大型資通及電子企業投資資安事業，發展全球物聯網資安方案之供應基地

④ 加強國際合作網絡，運用全球資安人才

資料來源：行政院

國家安全會議
NATIONAL SECURITY COUNCIL

資安即國安1.0 與 2.0進程與規劃

	1.0	2.0
組織	成立行政院資安處	1. 加速成立**數位發展部** 2. 政府機關六塊基礎團隊堅實合作
法制	實施資安管理法、修正國家安全法及國家情報工作法	**法遵落實**：關鍵基礎設施、委外管理、供應鏈管理、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**

國家安全會議
NATIONAL SECURITY COUNCIL

結語

蔡總統：「發展結合5G時代、數位轉型、以及國家安全的資安產業。我們要全力打造可以有效保護自己，也能被世界信賴的資安系統及產業鏈」。

1. 加速設立一個數位發展部會，推動前瞻數位資安產業應用發展，建立數位國力。
2. 以六大核心產業落實資安來驅動資安產業。擴大投資於科研能量與資安人才培育
3. 強化重要產業，特別是國防、八大關鍵基礎設施和半導體資通訊產業。
4. 建立精實防禦機制，早期預警、緊急應變、持續維運。
5. 持續府院、國際及公私夥伴關係的合作模式，強化實質國際資安合作。

總統蔡英文於「臺灣資安大會2021」致詞，她強調，政府會持續強化組織、落實法制、培養人才、支持產業，她也期待政府及民間資安領域的先進攜手打拚，共同建立「堅韌、安全、可信賴的智慧國家」。
(資料來源：總統府新聞網:2021/5/4)

蔡英文總統2021/5/4接見「2021 GiCS第一屆尋找資安女婕思獲獎隊伍」時，肯定科技部舉辦活動鼓勵女性投入資安及科技領域，並強調邁入物聯網及5G時代，將持續推動「資安即國安」戰略，打造受世界信賴的資安系統及產業鏈，提升臺灣數位產業實力。
(資料來源：https://www.president.gov.tw/NEWS/26081

國家安全會議
NATIONAL SECURITY COUNCIL

資安就是數位免疫力

早期預警、緊急應變、持續維運