時代的變遷，科技已經離不開每個人的生活，根據 2025 年 3 月份 DataReportal 發布《Digital 2025：Taiwan》報告中，臺灣民眾在網路使用總人數已達 2,210 萬人，網路普及率已佔總人口 95.3%。當國家數位化程度與民眾網路觸及率越高時，網路安全議題就不單是技術問題，科技已將食衣住行育樂牢牢綁住我們。因此智慧工廠、智慧醫療、政府服務網路、無人機、無人車等，當這些物聯網設備或產品招受到惡意軟體攻擊，不僅會使人民財務損失，嚴重時更會危害個人生命安全與國家安全。

臺灣具有重要戰略地位，也是世界少有的民主典範，近年來自由民主與國家資訊安全進入新危機，資訊科技在極權國家可被拿來監控人民，對外則進行網路勒索攻擊。Check Point Research 在 2025 年 4 月提及，臺灣每秒招受 1.5 萬次網路攻擊，亞太地區之冠。傳統戰爭已轉變為沒有硝煙的資訊戰，可以說戰爭面貌儼然全然改變。這 10 年內曾震驚國內外重大事件中，如：2016 年俄羅斯癱瘓烏克蘭電廠、2020 年全台中油駭侵事件使其相關系統停擺、2020 年美國 SolarWinds 複合式供應鏈攻擊、2021 年美國最大燃油管道系統遭勒索軟體攻擊美國宣布進入緊急狀態、2022 年俄烏戰爭關鍵基礎設施工業控制權。這些年勒索軟體、供應鏈攻擊，以竊取各國外交、經濟與軍事文件越趨嚴重，甚至極權國家支持國家級駭客進行偷竊。對此各國開始紛紛注意並制定相關資安政策，以下將對各國與我國資訊安全政策進行簡述說明。

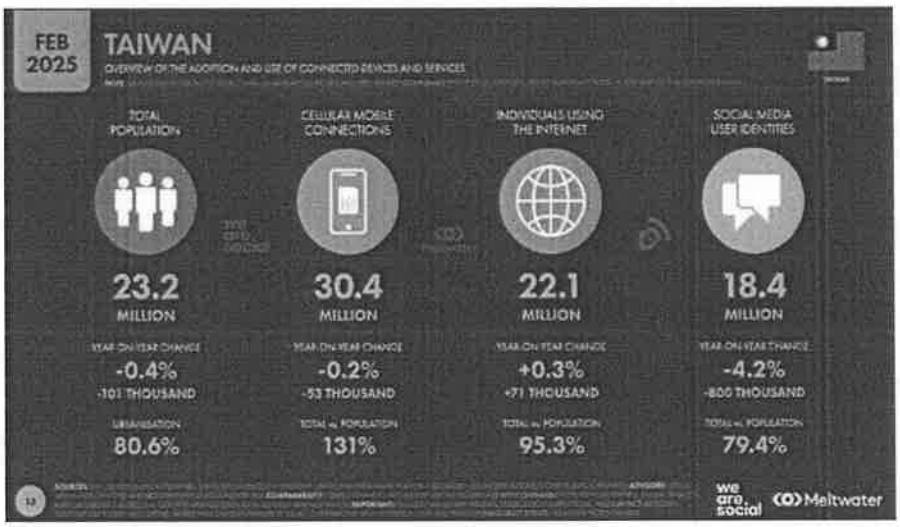


圖 1.《Digital 2025：Taiwan》資料來源：DataReportal

一、各國資安政策發展簡述

美國國家標準與技術研究所(NIST)，針對關鍵基礎設施網路安全提出了網路安全框架(Cybersecurity Framework，簡稱 NIST CSF)，這套指南於 2018 年提出，這標準目前也在全世界中運行多年。其中三大元素：框架核心、框架輪廓及框架層級，協助企業在網路安全中進行風險管理。透過框架讓企業在相同標準規範中可討論防禦措施，其中再細分五大核心「識別」、「保護」、「偵測」、「應變」、「復原」，作為評估資安成熟度與改善參考標準。2024 年 NIST 再次發布了 2.0 版本，將適用範圍延伸，不在限於關鍵基礎設施，希望讓所有的企業都可運用。新的版本將原本五大核心(識別、保護、偵測、應變、復原)新增「治理」。治理並不是新的想法，而是希望從企業組織、角色到職權需要高階管理階層的重視，讓網路安全與企業管理風險執行策略一致。回顧國內外重大資安事件，不僅使企業財物造成重大損失，還影響企業營運與商譽。

圖 2. NIST CSF2.0 變動 資料來源：iThome

歐盟於 2024 年 12 月 10 日資安韌性法(Cyber Resilience Act，簡稱 CRA) 正式生效。這是歐盟對未來要銷售到歐洲的數位產品的製造商、進口商、經銷商及開源軟體管理者，都需要嚴格遵守相關產品資安規範。若發現產品有漏洞或是資安事件，都需要進行通報義務。此法規也規定從 2026 年就需強制遵守，2027 年開始強制執行，違反者將面臨巨額罰款，罰款金額約 1500 萬歐元或前一年全球營業額 2.5%。

日本於2025年6月通過「主動式網路防禦」法案，法案在於提升日本網路安全防禦能力。法案主要內容有三項：(1)主動防禦早期預警，強化公私協力合作機制並進行跨國資訊整合分享、(2)對於跨境通訊，可進行通訊流量監控並設置檢測系統，防堵網路攻擊威脅、(3)若偵測到境外勢力有惡意攻擊狀況，授權警方或自衛隊進行該癱瘓該網路或伺服器，以主動防禦增加數位任行強化國家安全。

二、我國資安政策發展簡述

我國在2016年蔡英文總統上任推出了「資安即國安」政策理念，要求從結構整體強化資安，全面提升至國家安全層級，將資訊安全防護網列為守護臺灣第二道防線。在政策計畫中由 5+2 產業創新，以資安貫穿六大核心產略產業，並從四大不同面向提高戰略思維分別為：(1)組織面：成立行政院資通安全處、(2)法制面：實施資安管理法、修正國家安全法及國家情報法、(3)人才面：國防部成立資通電軍、(4)產業面：強化自主資安產業。透過完善結構組織、人力與資源配置，提升我國在資訊安全的質與量。

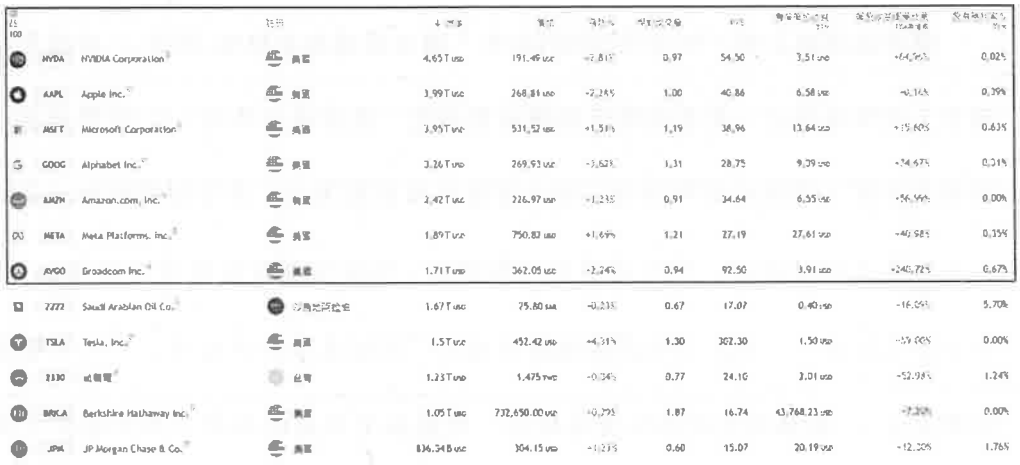
蔡英文總統第二任連任，隔年(2021)公布「資安即國安 2.0」，以「堅韌、安全、可信賴的智慧國家」為願景，提出三大目標：持續強化組織培育資安人才、加強各領域安全與防護、最後壯大臺灣資安產業發展。在三大目標下擬定 5 大策略，人為最重要寶貴資產，因此第一點為培育資安卓越人才，推動公私協力聯合作戰機制(Talent)、(2)加強各領域韌性安全防護機制，研發關鍵技術提升應變能力(Resilience)、(3)促進資安國際合作，建構國內外聯防體系(Unity)、(4)發展精實防禦機制，打擊網路犯罪(Security)、(5)落實六大核心產業驅動資安產業(Technology)，以上 5 大策略簡稱 Trust。呼應信賴臺灣訴求，透過強化組織、培育人才，落實法治、強化自主資安產業，確保社會政府信任感，讓資安防禦思維持續向上提升。

賴清德總統上任，於今年(2025)公布「國家資通安全戰略 2025」，延續先前的願景，並對複合式、灰色地帶及各種威脅滲透，提出兩大準則：(1)堅實資安治理機制及防護、(2)戰略夥伴鏈結。擴大守護我國家園決心，並分別從國防、災防、民主與民生四個面向，來打造安全可靠國家。總統就職演說提出四大支柱：「全社會防禦韌性」、「國土防衛與關鍵基設施」、「關鍵產業與供應鏈」、「人工智慧應用與安全」，建構穩定與韌性智慧國家，更視為全方面的部署。本次報告中多次提到治理與韌性，也符合目前國際資安改變趨勢。

臺灣有著民主國家多元性、包容性與自由性。有著第一防線臺灣海峽作為防護，資安即為民主韌性的第二防線。資安治理是現代組織應對數位風險的基石，堅韌則是在威脅與事件中，仍可快速恢復其營運。韌性包含：容錯能力、系統可用性、完整性，機敏性，若發生事故也可透過資料異地備源進行營運。今年 9 月 27 日韓國發生了鋰電池火災事故，此事件癱瘓國家近 650 項網路服務，其中近一半為政府服務民眾業務與服務。過了一個月截至 10 月 20 日僅復原 375 個系統(復原率 52.9%)。將近 96 個資料庫全毀，大量公務資料毀損回歸使其行政癱瘓，

三、美中貿易戰與俄烏戰爭台灣資安契機

2025 年 1 月美國川普再次上任後馬上開啟貿易戰，透過關稅來重新建構世界貿易秩序，為了就是要讓美國再次偉大。截至今年 10 月 27 日全球前 12 大市值公司(如圖 3)，前七名為美國七雄(輝達、蘋果、微軟、谷歌、亞馬遜、Meta、博通)，第八名為沙烏地阿美(石油)、特斯拉、台積電、波克夏、摩根大通。台積電排名第 10，但美國企業占了 10 席，其中美國七雄市值近 21.87 兆元，帶動的國家競爭力非同小可。七雄幾乎為資通訊產業，這七家企業帶動的產值不僅傲視群雄，更占美國 GDP 五成。這些高科技產業具有極高商業價值，因此也被駭客組織精準鎖定，以竊取資料或進行勒索。故川普再次上任後，延續他第一任「乾淨網路政策」，排除中國與其他敵對勢力威脅。



100										
	NVDA	NVIDIA Corporation		4.65 T usd	191.46 usd		0.97	54.50	3.51 usd	0.02%
	AAPL	Apple Inc.		3.99 T usd	268.84 usd	-2.24%	1.00	40.86	6.58 usd	0.39%
	MSFT	Microsoft Corporation		3.95 T usd	531.52 usd	+1.58%	1.19	38.96	13.64 usd	0.63%
	GOOG	Alphabet Inc.		3.26 T usd	269.93 usd	-3.62%	1.31	28.75	9.39 usd	0.01%
	AMZN	Amazon.com, Inc.		2.42 T usd	226.97 usd	+1.23%	0.91	34.64	6.55 usd	0.00%
	META	Meta Platforms, Inc.		1.89 T usd	750.82 usd	+1.69%	1.21	27.19	27.61 usd	0.15%
	AVGO	Broadcom Inc.		1.71 T usd	362.05 usd	-2.24%	0.94	92.50	3.91 usd	0.67%
	2222	Saudi Arabian Oil Co.		1.67 T usd	25.80 sar	-0.23%	0.67	17.07	0.40 usd	5.70%
	TSLA	Tesla, Inc.		1.5 T usd	452.42 usd	+4.31%	1.30	302.30	1.50 usd	0.00%
	2330			1.23 T usd	1,475 twd	-0.34%	0.77	24.10	3.01 usd	1.24%
	BRK.A	Berkshire Hathaway Inc.		1.05 T usd	732,650.00 usd	+0.27%	1.87	16.74	43,768.23 usd	0.00%
	JPM	JP Morgan Chase & Co.		836.34 B usd	304.15 usd	+1.23%	0.60	15.07	20.19 usd	1.76%

圖 3. 全球 12 大市值公司 資料來源：TradingView

臺灣雖為小國以硬體製造聞名世界，但我們也有著大國經濟思維。在 AI 競爭下我們也不缺席，為了站上並站穩舞台，從智慧家庭至智慧城市到智慧國家，政府持續推動科技政策，強化前瞻科技，逐年提升科技研發經費。以創新&永續為主要核心項目，推動我國重大科技政策包含：五大信賴產業、晶創臺灣方案、大南方新矽谷、智慧機器人、AI 新十大建設、次世代通訊、生醫及精準健康等。這些隨著百工百業導入 AI，資安的威脅問題也就更甚。臺灣在資安產值與資安公司雖規模都不大，但地處地緣政治且長期受到對岸敵對勢力網路威脅與攻擊，我們有著面對國家型駭客攻擊與應對戰略策略。這些新的複合式攻擊，從來都不是單一事件，如何從資安事件中掌握情勢，快速應變並恢復運作增強韌性，是我們戰略能力。

美中貿易戰對中國管制升級，去紅供應鏈也帶給了臺灣產業機會進入國際市場新契機。我國有著強大的製造業與 IC 產業實力，強化軍事實力來保護自己。因此厚植軍工產業嚇阻敵對勢力，國有化也可帶動產業發展。在俄烏戰爭中看到新型態攻擊，無人機&機器人可用來收集情資與反收集、低軌衛星可提升數位韌性保持通訊等。小至零件大到精密製造，臺灣產業不僅有機會進行升級轉型，更可以提升國際供應鏈地位。在去紅色供應鏈中，美國也擔憂駭客攻擊者轉向軍工產業，為確保自己軍事供應鏈安全，2024 年美國國防部公布網路安全成熟度模型驗

證驗證標準 2.0 (Cybersecurity Maturity Model Certification，簡稱 CMMC2.0)，2026 年正式實施。未來跟美國國防部供應鏈廠商包含採購合約，都將納入 CMMC 認證要求。此規範讓甲方更加重視相關文件、合約、系統、軟體機敏性評估。CMMC 雖先對軍工進行規範，但也對任何產業適用。因此臺灣要打入國際市場，在產品建構初期就需要將資安規範納入設計，同時政府與民間要共同合作才能雙贏。

俄烏戰爭開打前網路戰已先行，俄羅斯早好幾個月就開始攻擊各種關鍵基礎設施。正式開打後癱瘓各項民生關鍵基礎設施為第一目標，攻擊手法包含分散式阻斷(DDoS)，植入木馬刪除各項資料使其系統癱瘓，再搭配相關社群軟體進行認知戰，讓人民浮動焦慮害怕，讓人民對政府失去信心。我國在蔡總統「資安即國安」到賴總統「國家資通安全戰略 2025」，看到俄烏戰爭反思其相關作為。強化並提升數位韌性，特別在軍事指管系統及對民眾訊息傳達。故維持通訊韌性外，關鍵基礎設施防護更不可少，盤點既有資源與風險管控項目，建立風險資安地圖。另應將工控系統(OT)納入監控，掌握關鍵基礎設施(CI)與關鍵基礎設施資訊系統(CII)相依性與關鍵點。Netflix 在 2025 年上映一部新幹線倒數計數電影，裡面用新幹線做為被攻擊電影主角。交通運輸是很重要的關鍵基礎設施，平時為運輸工具，戰時視為軍事後勤補給重要節點。以臺灣高鐵為例我們應先對其功能項目分類，有核心功能(列車安全維護、乘車服務、旅客安全等)、內部重要資產(自動列車管控、電源配盤、災害警告系統等)、關鍵基礎設施(各重要車站)、外部關鍵設施(配電、網路、自來水廠等)。以上每一個都是重要節點，相互獨立但又彼此關聯。因此我們應思考會面臨到各種攻擊狀況，擴大工控系統檢核技術，並追蹤 log 以利發現異常問題。強化各部安全監控系統，不要在進行過多風險情境比例分析。另在資安問題發生時，情資也應向上整合通報，以利提升聯防效果與各部門韌性支援，這樣才能有效面對真實威脅。

最後人才培育為最重要的資產，時代變遷人人已離不開資訊系統，資安人才更是跨域的挑戰，從基礎知識到進階專業能力。今年 10 月 30 日 Fortinet《2025 年資安技能落差報告》調查中，全球資安人才缺口已超過 470 萬人。我國在 2021 年 9 月金管會宣布，具有一定規模金融機構或純網銀必須設置資安長，2022 年第一季需全數增設完畢。金融產業為高度管制對象，此法規設立保護人民財產，但也讓資安人才缺口更為嚴峻，政府部門資安人才更為悽慘，因為員額規定難以擴增，更常發生培訓完畢後，被民間高薪挖走。政府該如何有效留才、攬才，來積極面對這場全世界都在搶資安人才為重要課題。

四、結語

地緣政治下敵對勢力只會更積極入侵竊取政治、軍事、外交、經濟等資訊。前國安會李漢銘諮委在一場演講曾提到：「資安很重要，但大家忙起來常常不要」。聽起來是玩笑話，但卻是真時寫照。資安是一個很花錢卻很難看到成效工作，甚至往往聽到都不會是好消息。在 AI 時代新科技、新產品更需重視資安。同時我們的資安思維也應要有所轉變，所有的資通訊設備與軟體，皆有可能被駭侵，因此企業隨時都有可能發生攻擊事件。我們應該重視被駭侵後，讓被偷的資料是否可以讓對方看不到，或是被攻擊的服務是否可以快速恢復運作，這些皆為韌性所在。在中美貿易戰，臺灣有新契機讓產業轉型並進入國際供應鏈，為符合國際資安標準成為被信賴的國家，可學習台積電成立半導體資安標準(TSMC-SCSA)制度，這套標準從系統與設備開發就需要納入資安考量，所有跟台積電合作都需遵循，這標準不僅是企業本身自制力，更引領整條供應鏈安全可信賴發展，此典範也應擴散到其他產業如：衛星資安、無人載具等等。在資安人才嚴重不足下，除了學習運用 AI 提升戰力並強化資安防禦，公部門與私部門也須共同合力建構可信賴的全社會防禦，並以堅韌、安全、可信賴的智慧國家為最終願景。

五、參考資料

Fortinet 發布資安技能落差報告 全球逾 470 萬人才缺口(2025 年 10 月 30 日)。MoneyDJ 新聞。取自：https://www.moneydj.com/funddj/ya/yp050000.djhtm?a=%7BE16D939E-DA95-4F33-B1F3-CF0FFC03DF0B%7D。

Digital 2025：Taiwan DataReportal (2025 年 3 月 3 日) 取自：https://datareportal.com/reports/digital-2025-taiwan。

大型企業跨國市值(2025 年 10 月 27 日)。TradingView。取自：https://tw.tradingview.com/markets/world-stocks/worlds-largest-companies/。

吳碧娥(2025 年 5 月 20 日)。歐盟《資安韌性法》2027 年強制執行，違反者恐面臨巨額罰款，台廠如何應對？。經濟日報。取自：https://money.udn.com/money/story/11162/8752731。

張明德(2025 年 10 月 2 日)。【UPS 鋰電池火災引發國家級危機】韓國國家資料中心大火，暴露 UPS 電池管理與資料備援問題。iTHome 網路原生報。取自：https://www.ithome.com.tw/news/171797。

羅正漢(2024 年 7 月 25 日)。【網路安全治理當道】快速掌握 NIST CSF 2.0 的 7 大重要改變。iTHome 網路原生報。取自：https://www.ithome.com.tw/news/164080。

國家安全會議(2018 年 9 月 14 日)。國家資通安全戰略報告。取自：https://www.president.gov.tw/Page/317/969。

國家安全會議(2021 年 9 月 23 日)。國家資通安全戰略報告-資安即國安 2.0。取自：https://www.president.gov.tw/Page/317/1869。

國家安全會議(2025 年 4 月 28 日)。國家資通安全戰略 2025-資安即國安/。取自：https://www.president.gov.tw/Page/317/1870。