# 數位發展部主管115年度單位預算評估報告

數位發展部(以下簡稱數發部)主管含所屬資通安全署(以下簡稱資安署)及數位產業署(以下簡稱數產署)，115年度主管預算案歲入編列24億5,251萬元，較114年度預算24億6,079萬1千元減少828萬1千元(減幅0.34%)，主要係減列「使用規費收入」所致；歲出104億451萬8千元，較114年度預算58億2,214萬1千元(含追加預算7億4,479萬7千元)增加45億8,237萬7千元(增幅78.71%)，主要係數發部新增「智慧政府數位化精進發展計畫」5億680萬8千元、資安署增列辦理「數位政府資安生態防護推動計畫」、「政府數位韌性強化計畫」、「資安治理AI化計畫」、「AI網路主動式防禦關鍵技術研究計畫」及「關鍵基礎設施資安防護計畫」等6億5,600萬7千元，及數產署增列及新增「數位產業跨域軟體基盤暨數位服務躍升計畫」5億3,230萬元、「城鄉建模與數位雙生基礎建設應用計畫」4億3,000萬元及「智慧雨林產業創生計畫-健康照護及資通訊產業推動計畫」等14項計畫18億3,884萬1千元所致。謹就115年度數發部主管預算案評估如下：

**一二、新增「數位訊息分析技術研發計畫」及賡續辦理「AI網路主動式防禦關鍵技術研究計畫」，允宜持續精進AI防禦技術並加速主動式防禦落地應用，以建構前瞻網路防禦體系**

資安署115年度預算案於「資通安全業務」工作計畫下列有「通報應變業務」及「稽核檢查業務」分支計畫，其中分別編列「AI網路主動式防禦關鍵技術研究計畫」9,378萬6千元及「數位訊息分析技術研發計畫」9,016萬元。經查：

**(一)「AI網路主動式防禦關鍵技術研究計畫」及「數位訊息分析技術研發計畫」概述**

為提升對於數位訊息威脅之多方協作應變速度及偵測速度，並籌獲人工智慧威脅內容偵測與應對能力等，資安署提出

「AI 網路主動式防禦關鍵技術研究計畫」及「數位訊息分析技術研發計畫」,計畫總經費及期程分別為3億1,917萬1千元(114至117年)及3億6,616萬元(115至118年)(詳表1)，依資安署提供資料，該兩項計畫內容摘述如下：

1.**「AI 網路主動式防禦關鍵技術研究計畫」:**數發部於114年度辦理程式碼整體結構特徵及撰寫風格特徵及行為特徵分析開發工作等，資安署接續運用AI建立威脅情資自主智慧分析技術，研發戰情匯流智慧追跡技術，透過AI分析能力，以自主方式協同處理威脅情資，提高應對網路威脅整體效能，強化政府機關緊急應變能力。

2.**「數位訊息分析技術研發計畫」:**包含數位訊息威脅情資研究，係開發數位訊息威脅情資共享平臺、威脅情資識別模型、跨國情資識別模型與可疑訊息交易模組，研擬公共情資共享機制，強化威脅情資識別機構專用模組等；多來源訊息傳播研究，係建置多來源訊息分析平臺，強化開源情資分析模組，進行多來源訊息分析場域驗證等；人工智慧威脅研究，係開發人工智慧威脅內容鑑識平臺、輕量化人工智慧偵測模型，進行人工智慧威脅內容鑑識平臺場域驗證等。

**表1　資安署「AI 網路主動式防禦關鍵技術研究計畫」及「數位訊息分析技術研發計畫」概況表**　　單位：新臺幣千元

| 計畫名稱 | 期程 | 總經費 | 計畫內容 | 計畫效益 |
|---|---|---|---|---|
| AI網路主動式防禦關鍵技術研究計畫 | 114至117年 | 319,171 | 運用AI建立威脅情資之自主智慧分析技術,進而研發戰情匯流智慧追跡技術，期能透過AI強大分析能力,以更智慧且自主方式處理威脅情資,提高應對未來網路威脅之整體效率及效能;並藉 | 1.提高資安防禦效能：透過研發AI網路主動式防禦關鍵技術，不僅在預防層面取得優勢，更能在應對新型態和複雜攻擊方面取得卓越表現。<br>2.加強對抗新興資安威脅：資安環境不斷演變，新興資安威脅層出不窮。本計畫能夠深入挖掘並應對新型態資安攻擊，建構應對未來威脅強大能力。 |

| 計畫名稱 | 期程 | 總經費 | 計畫內容 | 計畫效益 |
|---|---|---|---|---|
| | | | 由戰情匯流智慧追跡技術開發，進一步強化政府機關在資安防護、監控、預警管理及通報等緊急應變能力。 | 3.建立自主智慧分析技術：透過AI技術，建立自主智慧分析技術，有助於更智慧且自主地處理威脅情報，藉此提高對未來網路威脅整體效率和效能。 |
| 數位訊息分析技術研發計畫 | 115至118年 | 366,160 | 研發數位訊息分析技術，從數位訊息威脅情資、多來源訊息傳播及人工智慧威脅三大研究方向，及相關研究技術落地應用。 | 本計畫預計提升對於數位訊息威脅多方協作應變速度及偵測速度，協助政府相關單位掌握數位訊息威脅，逐步強化我國在開源情資應用上能力，並籌獲人工智慧威脅內容偵測和應對能力，從各層面維護及國家總體韌性及安全。 |

說　　明：1.「AI 網路主動式防禦關鍵技術研究計畫」114 年度於數發部單位預算編列 3,398 萬 5 千元。

2.「數位訊息分析技術研發計畫」總經費於預算書列 3 億 6,800 萬元，差異係 115 年度預算案未編足所致。

資料來源：資安署提供。

## (二)我國面臨數位威脅日益增加之趨勢，允宜持續精進 AI 防禦技術，俾有效建構全面且前瞻之網路防禦體系

114 年第 2 季全球各組織每週遭受網路攻擊次數平均 1,984 次，較 113 年同期增加 21%，並較兩年前增長 58%；又我國平均每週遭受攻擊 4,055 次，位居亞太地區之首，攻擊頻率為全球平均值兩倍以上[1]，顯示我國面臨數位威脅日益增加。另數發部建置「網路詐騙通報查詢網」作為通報疑似詐騙訊息之平臺，自 113 年 9 月 30 日至 114 年 10 月 4 日止，已接獲通報疑似詐騙訊息 35 萬 3,445 則，其已確認詐騙訊息 18 萬 4,699 則[2](占比 52.26%)，詐騙訊息甚多。鑑於數位威脅增加及可疑訊息數量龐鉅，又 AI 產生之假訊息辨識難度高，允宜持續優化 AI 防禦技

[1]參資安人 114 年 7 月 28 日「報告：台灣受攻擊三大產業硬體供應商、政府與軍事機構和製造業」中，Check Point Software Technologies Ltd.之威脅情報部門 Check Point Research 數據。

[2]參數產署 114 年 10 月 9 日新聞「數位發展部網路詐騙通報查詢網週快訊(09/28~10/04)」。

術，俾有效建構全面且前瞻之網路防禦體系。

**(三)為防範網路攻擊並提供即時反應能力，允宜研謀加速 AI 網路主動式防禦落地應用期程，以提升資安防護效能**

美國國防高等研究計劃署(下簡稱 DARPA) 自 112 年 8 月發起為期 2 年之人工智慧網路挑戰賽(下簡稱 AIxCC)，參賽團隊設計、測試及改進新型 AI 系統，以自動防禦關鍵程式碼之安全。觀 AIxCC 於 114 年 8 月發布之決賽成果指出[3]，AI 驅動系統可發現並修補現實世界之網路漏洞，其中參賽團隊(Team Atlanta)開發之 AI 系統分析逾 5,400 萬行程式碼，並偵測到 DARPA 設置之模擬漏洞，且該系統於 70 項決賽挑戰中共發現 54 個獨特之合成漏洞，並修復 43 個，亦發現並修補 18 個現實世界之真實漏洞，顯示 AI 網路主動式防禦已具有相當之應用成果。然依資安署「AI 網路主動式防禦關鍵技術研究計畫」之說明，該計畫多處於研究開發階段，鑑於網路攻擊日益複雜，為提供即時反應能力，允宜研謀加速 AI 網路主動式防禦之落地應用期程，以提升資安防護效能。

綜上，資安署 115 年度預算案「AI 網路主動式防禦關鍵技術研究計畫」及「數位訊息分析技術研發計畫」分別編列 9,378 萬 6 千元、9,016 萬元，主要係運用 AI 強化威脅情資分析與多來源訊息偵測能力，提升我國對數位威脅之預警、應變與防禦效能。鑑於我國數位威脅持續升高，允宜持續精進 AI 防禦技術，俾有效建構全面且前瞻之網路防禦體系，並研謀加速 AI 網路主動式防禦之落地應用期程，以提升資安防護效能。

[3]參 AIxCC 網站：https://aicyberchallenge.com/Finals-winners-announcement/