AI自主防禦
提升國軍資安管理能力研究

作者簡介

翁仁遠中校，指職軍官94年班、陸軍指參107年班、戰略研究班108年班、健行科技大學資管所碩士；曾任連長、通信官、資圖主任、通訓中心大隊長、防衛部通資組組長，現為國防大學戰爭學院學官。

王宇安上校，海官90年班、海軍指參104年班、戰院110年班；曾任168艦隊作訓官、基支部軍務科長、中建軍艦艦長，現任國防大學戰爭學院教官。

提　要

一、隨著現代戰爭日益數位化，網路攻擊手段日趨複雜且高頻，傳統資安管理模式無法全面應對國軍在數位戰場上的挑戰。特別是在資安人力資源短缺與技術能力有限的背景下，引入人工智慧(Artificial Intelligence, AI)自主防禦技術已成為提升國軍資安防護效能的必然趨勢。本研究聚焦於AI技術在威脅偵測、自動化事件響應與數據分析中的應用，提出以自動化與智能化處理大規模網路數據的綜合解決方案，旨在提高國軍資安管理的即時性與準確性。

二、本文採用案例分析與文獻回顧相結合的方式，針對國軍需求設計AI自主防禦的整合性應用模型，涵蓋實施策略、數據管理及隱私保護等核心面向。研究結果顯示，AI技術可顯著提升威脅偵測效率，降低人為操作誤差，並為非技術背景的管理者提供有力支持。在處理高階持續性威脅(Advanced Persistent Threat, APT)等複雜攻擊時，AI工具能有效補足人力資源不足的

問題，進一步增強國軍的防禦韌性與反應能力。

三、本研究提供了一套可行的技術整合方案，為國軍資安管理的升級與數位化轉型提供具體指引。未來，透過持續優化AI技術應用，國軍將能更有效應對不斷演變的數位威脅，構建全面且前瞻的網路防禦體系，確保國防資訊安全與作戰效能。

關鍵詞：AI自主防禦、國軍資安管理、資訊安全

前　言

隨著網路攻擊威脅日益增長，網路空間已成為現代戰爭的重要戰場，並對國防安全構成了巨大的挑戰。過去，國軍多依賴傳統資安管理方式，這些方法雖然歷經多年發展，具備一定的穩定性與實務性，但隨著攻擊手法的不斷進步與威脅頻率的增加，傳統資安管理方式逐漸無法應對新型且複雜的威脅。這些威脅不僅是針對國軍的關鍵網路基礎設施，還可能涉及國家機密與戰略資料的竊取，嚴重影響國防運作效率與安全性。尤其在面對高階持續性威脅(Advanced Persistent Threat, APT)等技術性高且複雜的網路攻擊時，傳統防護策略往往顯得不足，且難以迅速調整應對。

此外，國軍目前面臨人力資源短缺的挑戰，尤其在少子化的影響下，志願役人力充足度逐年降低，導致技術背景強的資安人員供不應求。根據國防部報告，截至2022年6月底，志願役現員編現比僅84.98%，而士官階層的充足率甚至低至83.77%。這些不足限制了國軍在資安管理中的即時反應能力，影響了國軍資安團隊在面對突發攻擊時的應對效率。此外，民國111年的徵兵及齡男子僅11萬8千餘人，[1]創下近10年新低，顯示未來的可用人力資源仍將受到嚴重限制，這進一步加劇了國軍依賴傳統人力操作的資安管理模式的侷限性。

面對這些挑戰，人工智慧(AI)技術的快速發展為國軍資安管理提供了新穎的解決途徑。AI技術不僅可以在資安防護中發揮關鍵作用，還能透過自動化數據分析和威脅檢測來提升應對效率並降低對人力的需求。AI技術中的大數據分析、機器學習與深度學習應用，能夠快速偵測異常

1　預算中心，〈112年度中央政府總預算案整體評估報告〉，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=45676&pid=221540，檢索日期：民國113年11月15日。

行為、提前預測網路威脅，並自動執行應對措施。[2]

針對上述背景，本研究的動機在於探索如何透過AI技術增強國軍的資安管理應對能力，並以符合中華民國112年國防報告書中，國軍網路與資訊安全方面的政策(強化入侵偵測、防火牆等多層次防護措施，以阻隔網路攻擊)方向。[3]藉由導入及適當應用AI自動化技術，進而補足國軍在人力及技術上資源不足方面的問題，以提升網路防禦的整體應對效率。

研究的範圍將聚焦於AI技術在國軍資安管理中的應用，尤其是威脅偵測、自動化事件響應以及決策支持三個核心方面。AI技術的引入將針對資安管理中的重點環節進行自動化處理，包括機器學習和深度學習模型的運用，並參考美軍的相關規範，以制定符合國軍需求的整合方案。透過這些技術的實踐應用，AI技術可協助國軍資安管理部門快速響應並肆應不同的攻擊類型，增強整體資安防護能力。

然而，本研究在進行時可能面臨幾項限制。首先，國軍內部的資安數據具有高度保密性，可能無法取得完整且真實的數據來進行分析，這可能限制了研究的真實性與精確度。因此為提升本研究的技術可信度，補充了AI模型運作示意與引用相關國外文獻作為支撐。其次，AI技術尚處於快速發展階段，部分技術應用尚未完全成熟，在威脅預測及自主防護方面的效果仍存在不確定性，尤其是在應對高階持續性威脅時，AI技術的成效可能受限。

即便如此，AI技術的應用仍為國軍資安管理提供了新的契機。透過異常行為檢測、威脅情報與預測分析、自動化事件回應與修復、自適應學習與強化學習等相關核心技術，能大幅減少對高技能人力的依賴，並提高國軍資安管理的整體應對效率。國軍在現代網路戰爭中所需的防禦能力將因AI技術的導入而得到提升，進而更好地保護國家安全。本研究期望能提出具體的相關建議，以幫助國軍有效應對不斷變化的數位威脅環境，確保資安管理的穩定性與效率，並增強國防的整體安全性。

AI自主防禦技術概述與應用

2 《智慧物聯網：AIoT技術創新應用與未來趨勢》〈AI技術在數據隱私保護中的應用與挑戰〉，https://aiot.qshop.net.tw/data_driven_tech/ai%E6%8A%80%E8%A1%93%E5%9C%A8%E6%95%B8%E6%93%9A%E9%9A%B1%E7%A7%81%E4%BF%9D%E8%AD%B7%E4%B8%AD%E7%9A%84%E6%87%89%E7%94%A8%E8%88%87%E6%8C%91%E6%88%B0/，檢索日期：民國113年11月15日。

3 中華民國112年國防報告書編纂委員會編，《中華民國112年國防報告書》(臺北：國防部，民國112年9月)，頁79。

一、AI自主防禦技術基本概念

AI自主防禦技術作為網路安全領域的前沿技術之一，目前正在澈底改變網路防禦，並且可能證明是抵禦未來AI攻擊的最佳防線。[4] 透過自動化和智能化手段提供高效的資安防護，正逐步改變傳統的防禦策略。傳統的資安防禦主要依賴人工監控和靜態規則設置，通常難以即時應對日益複雜且多變的網路威脅，而AI自主防禦技術是引入大數據、機器學習等人工智慧技術來提升網路安全防禦能力的一種途徑，透過利用AI的模糊訊息處理能力、協作能力、運算能力和學習推理能力，使網路安全防禦具有數據快速分析、自我學習和準確預測等能力。[5] 主要架構如圖1。另外，AI學習模型能夠應對不斷演化的攻擊手段，例如零日攻擊和高階持續性威脅(APT)，這些威脅通常以隱蔽、持久為特點，[6] 傳統防禦手段難以即時檢測和攔截。而AI自主防禦系統能夠動態學習新型威脅模式，自動更新其防禦策略，從而實現對未知威脅的即時偵測和響應 。

自主防禦技術的核心還在於它的分析和深度學習模型，AI可以提取大量網路流量和事件紀錄中的特徵，進行預測性分析。這種預測不僅能主動識別潛在威脅，還能發出預警信號，讓安全團隊提前做

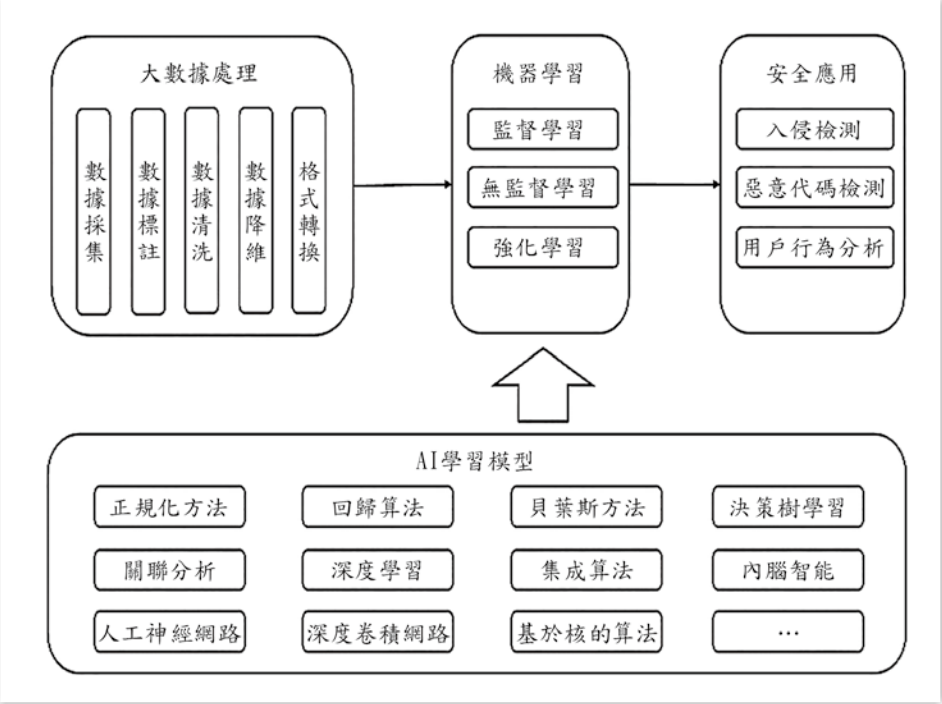

圖1　智能驅動的網路安全技術的實現框架

資料來源：陳福才、劉文彥、程國振，《網路空間主動防禦技術》(北京：科學出版社，2018年10月)，頁209。

4　Ithome，〈自主網路AI正在澈底改變網路防禦〉，https://www.ithome.com.tw/pr/134086，檢索日期：民國113年11月15日。

5　陳福才、劉文彥、程國振，《網路空間主動防禦技術》(北京：科學出版社，2018年10月)，頁209。

6　資安趨勢部落格，〈什麼是APT攻擊/進階持續性威脅(Advanced Persistent Threat, APT)？〉，https://blog.trendmicro.com.tw/?p=123，檢索日期：民國113年11月15日。

好應對準備。例如，Google的Chronicle平台的Duet AI能夠透過生成式人工智慧以及安全基礎模型，簡化用戶在威脅偵測、調查和回應的工作，實現對異常活動的實時監控與響應。[7]

由於AI自主防禦技術能夠以低人力需求和高效應對的方式，提供全天候防護，目前相關資安管理機構正將其應用於資安防護中。未來，隨著技術的不斷成熟和學習能力的增強，自主防禦技術有望在高風險領域發揮更加重要的作用，從根本上改變資安防禦的方式和範疇。

二、AI自主防禦技術的應用

AI自主防禦技術在網路中可扮演強化的角色，使得資安管理人員能夠應對日益複雜的網路威脅，確保資訊環境安全。早在2019年時Kazi Abu Taher, Billal Mohammed Yasin Jisan, Md.Mahbubur Rahman Department等3位學者提出人工神經網路(Artificial Neural Network, ANN) 在網路入侵檢測方面的優勢，特別是與包裝器特徵選擇相結合時，[8] 奠定了後人開發更先進的機器學習驅動的入侵檢測系統的進一步研究。以下將從近年來AI自主防禦技術的常見應用，如異常行為檢測、威脅情報與預測分析、自動化事件回應與修復、自適應學習和強化學習方面實施探討。

(一)異常行為檢測

使用深度學習的AI方法透過分析安全事件來檢測網路威脅。它能專注於區分真正的正面警報和虛假警報，幫助專家有效應對潛在的網路攻擊和內部威脅，[9] 並自動識別與此模式不符的異常行為。這種技術廣泛應用於識別潛在的網路攻擊和內部威脅，避免零日攻擊和高階持續性威脅(APT)造成的影響，Fang Yuqiang的研究論文中指出使用基於生成對抗網路的網路行為異常預測(APIB-GAN)模型(如圖2)。並使用均方根誤差(Root Mean Square Error, RMSE)作為評估異常預測方法的指標，其公式計算方式，如圖3所示。結果顯示在不同員工數據類別中預測互聯網行為數據中的異常情況，分別有 87.23%，85.13% 和 83.47% 的準確度，證明AI有效檢測異常在線行為的能

7 iThome，〈Google推出統一Chronicle安全營運平台〉，https://www.ithome.com.tw/news/158813，檢索日期：民國113年11月15日。

8 Kazi Abu Taher, Billal Mohammed Yasin Jisan, Md.Mahbubur Rahman Department, “ Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection ”, International Conference on Robotics, Electrical and Signal Processing Techniques,(Bangladesh),(2019),pp. 643～646.

9 P Ramya Sai, K.S Niraja, “ Cyber Threat Detection Based on Artificial Neural Networks ”,International Journal for Research in Applied Science and Engineering Technology,(India),Vol.11,Issue X(2023),pp. 1469～1472.

力。[10] 因此，就可以利用AI監測到內部網路與外部聯繫的異常頻次變化，提早發現敵人網路入侵企圖或外部數據竊取行為。

(二)威脅情報與預測分析

AI自主防禦系統透過持續監控和學習歷史數據，進行威脅情報和預測分析，研究顯示透過比較多種AI方法在網路入侵偵測中的表現，可以證實AI技術在提升網路安全性方面具有顯著價值，[11] 也間接說明AI技術能夠提前發現可能的威脅模式並發出預警，讓資安管理人員有較多的時間提前應對。藉由這樣入侵的偵測，就可以提前發現敵方網路干擾活動，並預測其可能對通訊網路造成的影響，使資安管理人員可以提前採取防護措施，以確保資料和系統的安全性。

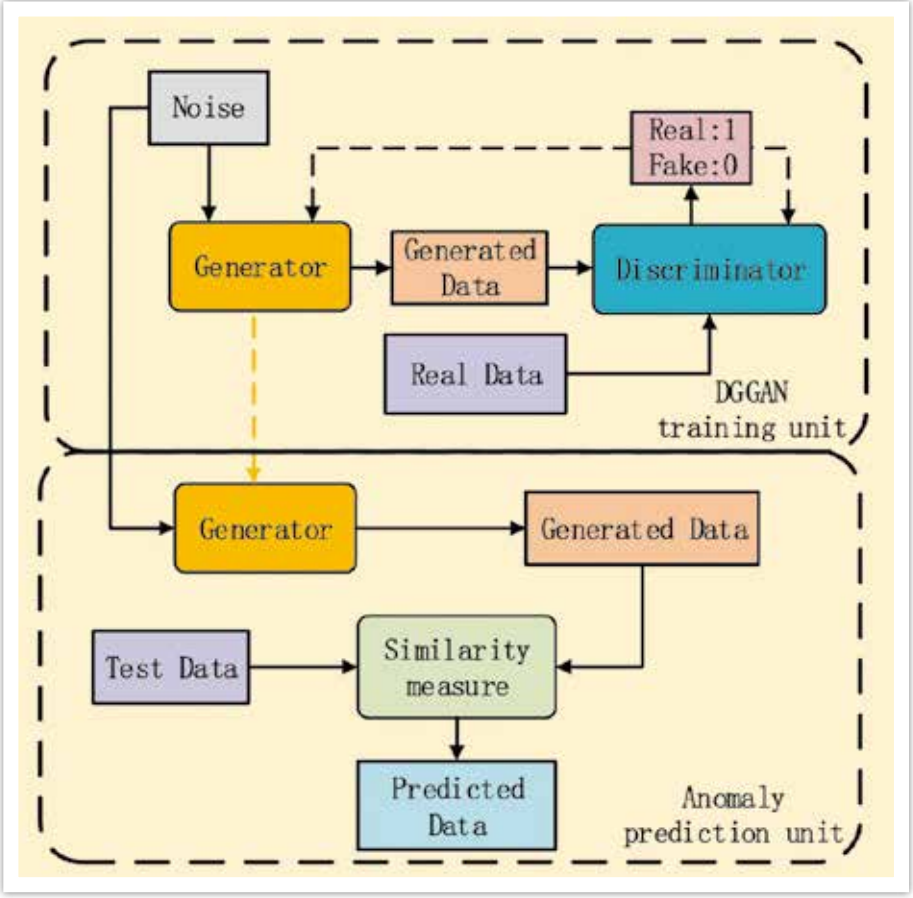

圖2　APIB-GAN模型

資料來源：Ibid 10, p6.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(X_{real} - X_{predict})^2}{n}}$$

$$Score = \frac{1}{RMSE + 1}$$

圖3　RMSE 公式

資料來源：Ibid 10, p6.

10　Fang Yuqiang, “ APIB-GAN: A Generative Adversarial Networks based approach for Anomaly Prediction of Internet Behavior ”,Physical Communication(Netherlands),Vol.64(2024),pp. 2～6。

11　郭芳瑜、林宗儀，〈人工智慧方法對於網路入侵攻擊的預測〉《智慧科技與應用統計學報》，22卷1期(民國113年7月)，頁22。

(三)自動化事件回應與修復

AI在即時事件回應和修復方面發揮至關重要作用，因為它能夠偵測威脅、透過關聯快速調查，以及使用預先設定的規則快速回應，顯著提高安全團隊的早期威脅控制和復原效率，[12] 在動態威脅環境下，例如戰時網路環境中的持續性攻擊，此技術可以根據攻擊行為的變化進行自我調整，並即時更新防禦策略以增強戰場中的網路安全。

(四)自適應學習與強化學習

1.自適應學習(Adaptive, AI)

是一種能夠自我調整和學習的AI系統，其目的是透過根據不同情況和數據源自動調整其行為和結果，從而更好地達到其目標。具體來說，自適應學習可以根據所處環境的變化、數據的變化、使用者的反饋等多種因素，自動調整其模型和算法，以提高其效率和準確性，[13] 藉由圖4的比較可以看出其不同於靜態學習以往的訓練模式，自適應學習更加強在互動的過程持續優化模型。

2.強化學習(Reinforcement Learning, RL)

強化學習是一種機器學習方法，其核心理念是透過智能體(Agent)與環境

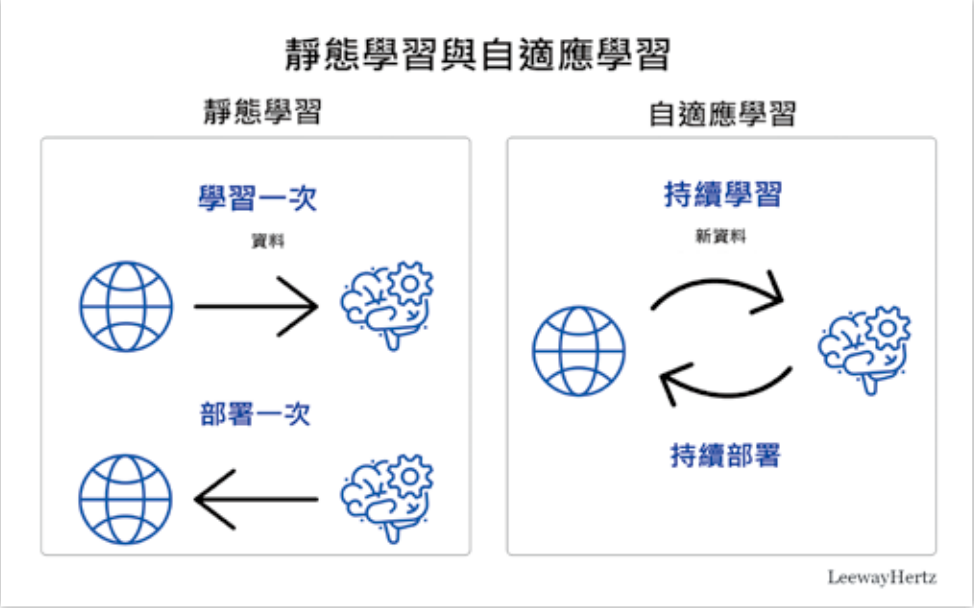

圖4　靜態機器學習與自適應學習

資料來源：LeewayHertz,<How to implement adaptive AI in your,business?>,https://www.leewayhertz.com/how-to-implement-adaptive-ai/,檢索日期：民國113年12月1日。

12　Mahida, Ankur,“ Real-Time Incident Response and Remediation-A Review Paper ”.Journal of Artificial Intelligence & Cloud Computing,(U.K), Vol2, (2023),pp. 1～3.

13　WeiYuan，〈五個必須掌握的AI發展趨勢〉，https://blog.v123582.tw/2023/03/10/%E9%99%A4%E4%BA%86-ChatGPT-%E4%B9%8B%E5%A4%96%EF%BC%8C%E5%BF%85%E9%A0%88%E6%8E%8C%E6%8F%A1%E7%9A%84-AI-%E7%99%BC%E5%B1%95%E8%B6%A8%E5%8B%A2/，檢索日期：民國113年11月15日。

(Environment)的互動，學習如何在特定任務中最大化累積獎勵。這種學習方式強調「試錯學習」，即智能體在探索過程中根據行動的結果獲得反饋，進而調整其行為策略，目的是獲得最大化的累積回饋，其運作架構如圖5所示。

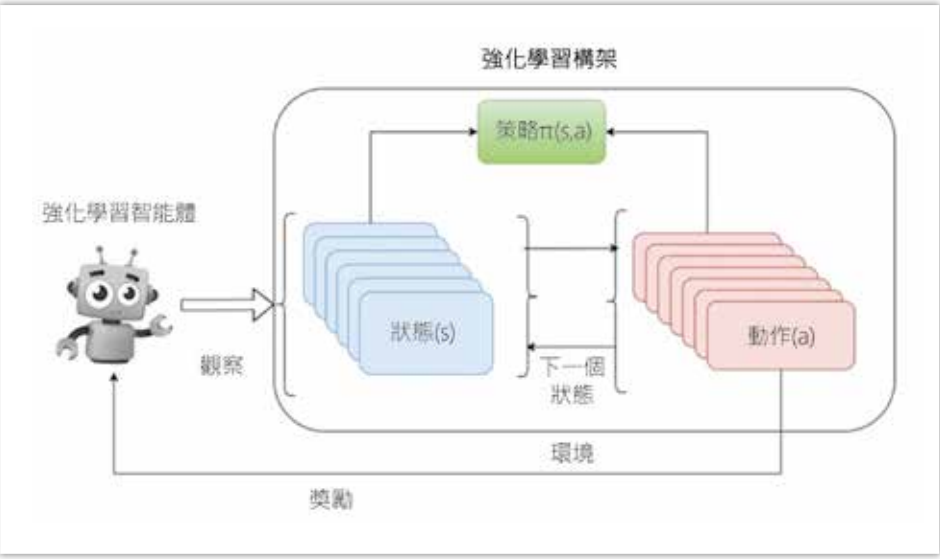

圖5　強化學習架構圖

資料來源：Sivamayil, Keerthana, Elakkiya Rajasekar, Belqasem Aljafari, Srete Nikolovski, Subramaniyaswamy Vairavasundaram, and Indragandhi Vairavasundaram, "A Systematic Study on Reinforcement Learning Based Applications" MDPI,(Switzerland), Vol.16, No.3(2023),p2.

由此可知自適應學習和強化學習各有其獨特的優勢和應用場景，自適應學習更專注於教育領域，旨在提升學生的個性化學習體驗；而強化學習則在需要自主決策和即時反應的環境中發揮關鍵作用。兩者都展示了人工智慧在不同領域中的潛力，並且隨著技術進步，它們的應用範圍將持續擴大，因此若綜合自適應學習和強化學習能力，使AI自主防禦系統可以根據新的攻擊模式不斷自我調整，進而確保防禦系統能夠應對不斷變化的網路威脅，保持防禦措施的最新有效性。

三、小結

綜合上述，我們可以了解AI自主防禦技術在資安領域中的多元應用，藉由異常行為檢測、威脅與情報分析、自動化事件回應與修復、自適應學習與強化學習的循環模式，在學理及實際應用上確實有顯著的防禦效果，因此這樣的技術若能應用在國軍資安管理上，就能使國軍在面對多變的網路攻擊時建立更具韌性的防護能力。

AI自主防禦技術在國軍資安管理的應用

一、美軍目前的防護機制

依據美國國防部於2023年1月頒布的網路安全架構5.0版(DoD Cybersecurity Reference Architecture Version 5.0)，內容區分識別、管理、控制、保護、偵測、分析、自動化、協調等8個階段，整體的運作流程如圖6所示，並朝向由內而外降低風險、透過彈性提高任務保障、實現現代

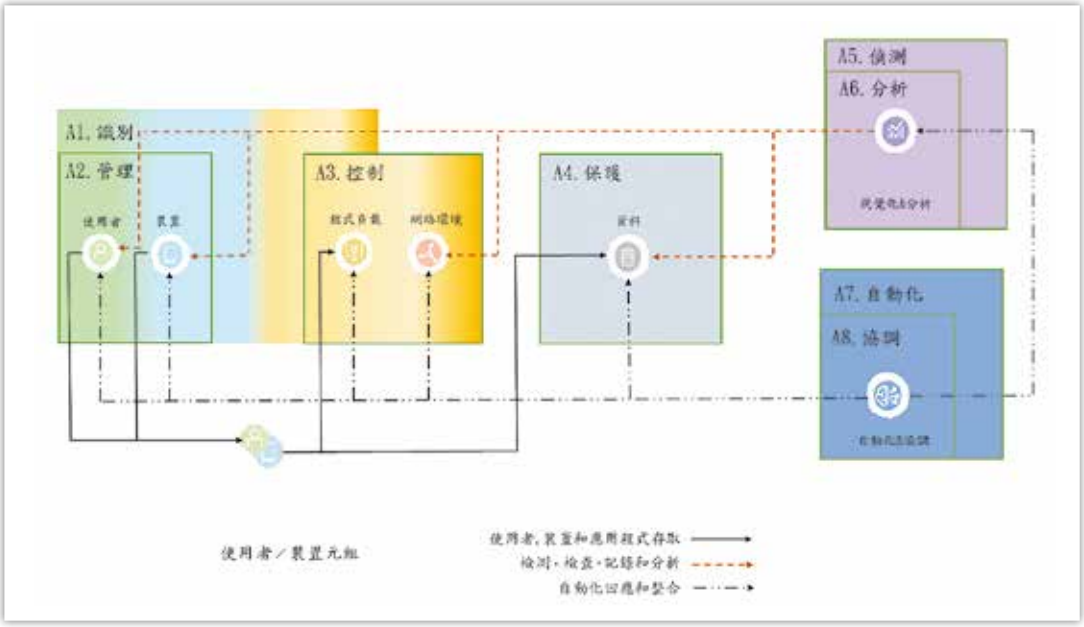

圖6　美國國防部網路安全架構運作概念圖

資料來源：Ibid 14, p12.

化等三個原則，[14] 以下針對各個層面實施探討。

(一)識別

識別階段是整個網路安全架構的基礎。這個階段主要在建立一個完整的資產清單，包括所有使用者、裝置和服務。透過持續更新這個清單，並結合身分識別管理系統(Identity and Access Management, ICAM)，[15] 使我們可以更精確地掌握系統的現況，為後續的保護、偵測等安全措施打下堅實的基礎。

(二)管理

管理階段，旨在透過嚴謹的管控機制，保護系統中的各種資產，確保系統的安全穩定運作。這個階段主要聚焦於使用者、裝置和系統配置的管理。

首先，使用者管理方面，無論是內部員工或是外部合作夥伴，都必須遵循統一的管理規範，確保每位使用者都擁有適當的權限。其次，裝置管理則涵蓋了國防部所擁有的裝置以及員工自帶的裝置，所有裝置都必須符合嚴格的安全要求，並能夠主動報告自身的安全狀態。最後，配置管理則確保系統的設定符合安全標準，防止未經授權的存取。透過這些管理措施

14　DoD CIO Cybersecurity Architecture Division,Department of Defense (DoD) Cybersecurity Reference Architecture(US:US.Department of Defense,2023), pp. 4～25.

15　身分識別管理系統(ICAM)：這個系統主要用於管理組織中用戶的身分和存取權限，確保只有經授權的用戶能夠訪問特定的資源和資訊。

，可以有效降低系統遭受攻擊的風險，並確保系統的穩定運作。簡而言之，管理階段就是透過對使用者、裝置和配置的全面控管，來建立一個安全可靠的系統環境。

(三)控制

控制階段中，網路與環境分割是一項關鍵的安全策略。透過將整個網路劃分為較小的、相互隔離的區域，我們可以有效限制攻擊的影響範圍。這種分割方式有兩種主要類型：巨型分割和微型分割。

巨型分割是將網路劃分成較大的區塊，例如將測試環境與生產環境分開。這種較高層級的分割通常基於組織單位、功能或其他策略性考量。微型分割則更細緻，它將網路切分成更小的單位，例如個別的系統、服務或應用程式。

無論是巨型分割還是微型分割，其核心目標都是提升網路的安全性。透過分割，我們可以減少攻擊者在網路中橫向移動的機會，降低各種攻擊手法(例如偵察、執行、防禦規避等)的成功率。此外，分割也能夠提高系統的韌性，即使某個部分受到攻擊，也不會立即影響整個系統。

例如，DoD365(Department of Defense, DoD)[16] 就採用了這樣的策略。它透過建立不同的用戶組織來實現巨型分割，而在每個用戶內部，又進一步將應用程式分隔成不同的微區段，以達到更細緻的保護。

總結來說，網路與環境分割是一種行之有效的安全防禦手段。透過將網路劃分為更小的、相互隔離的區域，我們可以顯著提升系統的安全性，減少潛在的風險。

(四)保護

美國國防部(DoD)對於「國防武器獲得系統」(Defense Acquisition System, DAAS)[17] 的安全防護極為重視，特別是考量到敏感國防資訊的處理、儲存與傳輸。為此，DoD制定了一套嚴謹的安全措施，包括：最小權限原則，確保每位使用者僅能存取執行任務所需的必要資訊；數據標籤與標記，以便系統能有效地管理與保護各種類型的數據；加密技術，以強大的加密演算法保護數據的機密性，防止未經授權的存取；以及動態安全政策執行，根據即時威脅與使用者行為，調整安全設定，提供更全面的保護。透過這些多層次

16 DoD365:是美國國防部(Department of Defense, DoD)所提供的一個基於雲端的服務平台，旨在支持國防部的業務需求。這個平台整合了多種工具和應用程式，以促進內部協作和數據管理，並增強安全性。

17 DAAS:在美國國防部的背景指的是「Defense Acquisition System」，即國防武器獲得系統。這個系統的主要目的是確保美國軍隊能夠即時獲得有效、合適且可持續的武器和相關資源，以滿足其作戰需求。

的防護機制，DoD旨在確保DAAS平台上所有敏感資訊的安全，並符合相關的安全規範。

簡而言之，DoD對DAAS的安全防護相當重視，透過嚴格的措施確保敏感資訊在整個生命週期中都能得到妥善的保護。

(五)偵測

偵測活動，旨在透過持續監控網路環境，主動識別並防範潛在的網路攻擊。為了達成此目標，DoD採用了多種先進技術。首先，透過建立用戶、設備及應用程式的行為基準，系統能快速辨識出偏離正常模式的異常行為。接著，運用機器學習與人工智慧等技術，系統能更精準地分析大量數據，找出隱藏在海量資訊中的潛在威脅。此外，深度封包檢測技術則能深入剖析網路流量，即使是加密過的通訊內容也能被仔細檢查。簡言之，DoD的「偵測」活動就像是一個全天候運作的警衛，時刻警惕著網路中的任何異常，並即時發出警報。

與傳統的被動防禦相比，DoD的「偵測」活動更具主動性。DoD不再只是等待攻擊發生，而是主動出擊，透過持續的監控與分析，預測並防範潛在的威脅。這種主動防禦的策略，使得DoD能夠更有效地應對日益複雜的網路安全威脅。

總結來說，「偵測」活動是DoD網路安全防禦體系的核心。透過這項活動，DoD不僅能即時發現並回應網路攻擊，更能不斷提升自身的網路安全防禦能力，以應對不斷變化的威脅環境。

(六)分析

當系統偵測到異常活動時，立即啟動「分析」程序，深入剖析這些事件，以評估其對系統的潛在威脅。分析人員會仔細檢視流量內容、測量數據等相關資訊，並結合威脅情報，深入了解攻擊者的手法與目的。所有被檢測過的流量都會被妥善記錄，這些記錄不僅有助於追溯事件，更能作為日後優化防禦策略的寶貴資料。透過運用人工智慧和機器學習等先進技術，系統能夠快速、準確地從海量數據中找出異常模式，並預測潛在的攻擊。為了因應不斷變化的威脅情勢，分析流程必須持續優化，以確保系統能即時偵測並回應新的攻擊手法。簡而言之，「分析」活動是網路安全防禦體系中不可或缺的一環，透過深入分析，我們能更有效地保護系統安全，並降低遭受攻擊的風險。

(七)自動化

為了更有效地防禦網路攻擊，並實現零信任架構，自動化在網路安全中扮演著越來越重要的角色。透過自動化，系統可以根據預設的安全政策，對異常事件做出即時回應，例如封鎖入侵來源、隔離感染設備等。人工智慧和機器學習的導入，更讓自動化系統能夠從大量的數據中

學習，不斷優化應對策略，提升系統的安全性。簡而言之，自動化不僅能加速事件處理速度，還能提高應對準確性，是現代網路安全防禦體系不可或缺的一環。

(八)協調

為了建立更完善的網路安全防禦體系，協調各項安全功能顯得至關重要。就像一個交響樂團，不同的樂器需要指揮家來協調，才能演奏出完美的樂章。透過整合威脅情報、自動化工作流程，並運用人工智慧等技術，我們可以將分散的安全系統串聯起來，形成一個協同作戰的整體。這種協調不僅能提升系統的反應速度，還能提高對複雜威脅的應對能力，是實現零信任架構的關鍵一步。

綜合上述我們可以了解到，美國國防部網路安全架構5.0透過八大階段(識別、管理、控制、保護、偵測、分析、自動化、協調)，建立了一套多層次的防禦體系。從資產清單的建立、使用者權限的嚴格控管，到網路分割、數據加密，以及利用AI進行威脅偵測與分析，美軍逐步建構起一個主動且智能的網路防禦體系，運作概念如圖6所示。特別是AI的導入，讓美軍在海量數據中快速識別異常，並自動化應對威脅，大幅提升了網路安全防禦能力。這套架構不僅強調技術層面的防護，更重視人與流程的協同，為其他國家，尤其是面臨相似挑戰的國軍，提供了寶貴的參考。接下來，我們將在美軍的防禦基礎上，探討AI技術能提供國軍在資安管理的參考，以提升國軍的網路安全防護能力。

二、國軍資安管理的現況與挑戰

(一)國軍目前資安防護機制

區分防護端及中心端兩大區塊，中心端由資安事件管理平台(Security Information and Event Management, SIEM)巨量資料安全分析系統、風險事件調查平台、規則建議(Recommended Standard, RS)、資安共同圖像顯示裝置(Dashboard)、資產管理主機(Asset Management Host, AMH)及資料外洩防護(DLP)所組成；另防護端的部分則由入侵偵測防護系統中控端(IPS)、網頁式防火牆中控端(WAF)及流量側錄中控(Flow)等構成。

(二)國軍目前管理現況

目前國軍資安防護單位為國軍資安防護管理中心(Military Security Operation Center, MSOC)，負責國防部及所屬各軍司令部、聯合作戰中心、各作戰區資安監防，提供入侵偵測、事件分析、早期預警、網路動態監測及緊急應變處理作為，確保國防資訊作業安全。分由北、中、東、南等4區資安防護管理中心負責監控軍、民網，各區資安管理中心平時運用資安事件管理平台監看資安事件及系統維運狀態，採人員輪班方式實施監控與處理資安事件。

(三)國軍目前的挑戰

隨著網路攻擊手法日益多樣且複雜，國軍在資安防護上雖已建立涵蓋防護端與中心端的完整體系，但在實際運作中仍面臨多重挑戰，主要體現三個面向如下：

1.人力資源短缺與專業技術瓶頸

少子化與軍隊現代化轉型使國軍在資安管理領域面臨嚴重人才短缺。現有人力不僅數量不足，且培訓機制仍偏重傳統防護技術，難以應對新型網路攻擊與複雜威脅。為此，亟須推動跨部門、分層次的人才培育與技術更新，提升資安管理專業能力，確保國軍在快速變化的網路戰場上維持高效防護。

2.多元系統整合與跨部門協同困境

國軍現行防護架構中，中心端涵蓋資安事件管理平台、巨量資料安全分析系統、風險事件調查平台、規則建議、資安共同圖像顯示裝置資產管理主機及資料外洩防護，而防護端則由入侵偵測防護系統、網頁式防火牆及流量側錄中控等組成。雖透過Connector將各單位警訊與日誌數據傳輸至中心端，但由於資料來源異質、更新延遲及格式不一，導致即時關聯分析與風險評估難以精準。此外，不同單位在管理標準與協同應變上的落差，也進一步影響了整體防禦效能。

3.新型網路攻擊與複合威脅應對侷限

傳統依賴靜態規則與簽章比對的防禦機制，對於高度隱蔽且動態演變的攻擊手法(如APT、零日攻擊及多階段滲透)顯得力不從心。然為確保國軍內部機密資訊安全，目前採用軍網與民網實體隔離的封閉式架構，雖有效降低外部攻擊風險，但也限制了對全球最新威脅情報的即時吸收與資料庫更新。這使得在面對快速演變的網路攻擊時，預警系統可能因情報滯後而無法迅速調整防禦策略，進而影響整體應變效率。

綜合而言，國軍儘管已構建功能完備且分工明確的資安防護系統，但在人才儲備、系統整合、技術更新及情報動態更新等方面仍面臨嚴峻挑戰。未來，應透過導入AI自主防禦技術，強化資安管理的自動化與智能化能力，並在人才培育、跨部門協同、標準化接口及離線資料導入等領域推動系統性改革，使AI技術能夠更有效地融入國軍資安體系，提升動態威脅應變、即時預警與精準防護能力，以因應數位戰場上日益嚴峻的網路安全挑戰。

三、AI如何提升國軍資安實施管理

隨著國軍在網路戰場上面臨日益複雜的攻擊型態與內部資安整合上的諸多挑戰，AI自主防禦技術提供了一條切實可行的升級路徑。以下將依據國軍目前所面臨的三大挑戰，並參照美軍頒布之網路安全架構5.0版，探討AI在資安實施管理上

的應用與優化策略。

(一)藉由AI彌補人力資源短缺與專業技術瓶頸

由於國軍在資安專業人力與技術培訓上的不足，傳統依賴人工監控與反應的模式難以滿足快速變化的威脅需求。AI自主防禦技術可透過以下方式改善此現狀。

1.自動化監控與異常檢測

利用深度學習與機器學習演算法，AI能夠自動分析海量網路流量與事件資料，快速識別出偏離正常模式的異常行為，進而自動觸發預警或對應措施。這不僅能夠大幅降低對高技能人力的依賴，也能在第一時間內捕捉潛在攻擊訊號。

2.智能決策與自動事件回應

藉由引入強化學習機制，AI系統可以在不斷的互動中學習最佳的回應策略，達到即時反應與自動修復的目的，彌補人才專業技術不足與即時判斷的劣勢。

(二)使用AI進行多元系統整合與跨部門協同

目前國軍資安防護架構中，各項監控、告警與數據管理系統資料來源異質且更新延遲，導致整體情資關聯分析難度高。AI技術可從以下面向加以改善。

1.資料融合與多元資料關聯

利用AI驅動的資料融合技術，可自動整合來自SIEM、IPS、WAF等不同系統的數據，並進行即時關聯分析，將分散的警訊彙整為統一的情資報告，有效支援跨部門協同作業。

2.智能化介面與決策支援

借助自然語言處理和智能儀表板技術，AI系統能將複雜的數據轉換成直觀的視覺化信息，協助不同技術背景的管理者迅速掌握現況並制定因應策略，從而縮小各部門間標準不一與反應滯後的問題。

(三)使用AI應對新型網路攻擊與複合威脅

面對高階持續性威脅(APT)、零日攻擊及多階段滲透等複雜攻擊，傳統防禦機制常顯不足。AI自主防禦可透過下列技術發揮關鍵作用。

1.威脅預測與動態學習

透過持續的歷史數據學習與即時監控，AI可主動預測攻擊趨勢並調整防禦策略。自適應學習機制讓系統能夠根據新型攻擊模式自我更新，從而保持防禦措施的前瞻性與有效性。

2.跨域資料分析與行為模式識別

AI利用生成對抗網路等先進技術，可精確區分正向警報與虛假警報，並針對異常行為進行深層次解析。這種技術已在部分實證研究中顯示出超過92%的準確率，[18] 證明其在面對隱蔽性攻擊時的

18 於下頁。

優越性。

(四)改善封閉網路下情報獲取與數據更新的時效性問題

由於國軍採用封閉式網路架構以保障敏感資訊，這在一定程度上限制了即時情報的引入與數據更新。針對此挑戰，AI可採取以下策略。

1.離線學習與週期性更新

在無法直接連接外部情報資源的情況下，AI系統可運用離線學習技術，透過歷史資料建立威脅模型，並定期利用安全渠道進行資料庫更新，以維持預警系統的敏感度。

2.封閉環境內部情報流轉機制

借鑑美軍在網路安全架構中的閉環反饋機制，國軍可透過AI建立內部信息共享平台，即使在封閉環境中，也能實現各系統間的情報互通與協同反應，從而縮短應變時間。

四、小結

綜合以上分析，AI自主防禦技術在解決國軍資安管理的三大挑戰上展現出顯著優勢。無論是在自動化監控、跨系統資料整合、應對複合性攻擊，還是提升封閉網路內部情報流動方面，均能依據美軍頒布之網路安全架構5.0版的先進理念，提供一套動態、智能且高效的資安防護解決方案。未來，隨著AI技術的不斷進化，其在國軍資安體系中的應用將成為提升國防整體作戰效能與資訊安全防護的重要支柱。

AI導入國軍自主防禦中的挑戰與對策

一、符合需求的語言模型開發與適配

AI語言模型作為現代自主防禦系統的核心，在國軍的應用中需要針對特殊的軍事需求進行專業化開發。然而，現有的通用模型大多設計為商業或民用用途，難以滿足軍事應用的高精準度與高安全性要求。

(一)挑戰

1.軍事特定語言模型的缺乏

現有模型缺乏針對軍事語言模型和情境的數據訓練，可能在威脅識別和應對建議方面準確性不足。

2.語言模型學習能力限制

模型需要持續學習新型威脅，但在封閉的國軍網路中，數據來源相對有限。

(二)對策

1.建立專屬軍事需求語言模型資料庫

18 Ravindra Changala,S.Kayalvili, Mansoor Farooq, L Malleswara Rao, Vuda Sreenivasa Rao, S Muthuperumal, “Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity”, IEEE(USA),July 26, (2024),pp. 1～6.

國軍應投入資源，整合國內外重大資安事件歷史案例、歷年來模擬資安攻防演練數據及軍事報告，建構符合軍事需求語言模型資料庫以支援語言模型的開發。

2.動態學習與定製化調整

採用強化學習和自適應學習技術，讓模型能動態肆應新威脅，並針對國軍特定需求進行優化。

3.與國外合作共享經驗

與具可信度的國外盟友(如美軍)合作，學習其軍事語言模型應用的成功經驗，借鑑並改良現有技術。

二、AI生成式資料庫的安全性問題

AI生成式資料庫在資安防禦中扮演關鍵角色，其能力包含快速生成應對方案與預測潛在威脅。然而，由於國軍網路的封閉特性，造就了封閉環境有效阻止惡意數據注入資料庫，確保生成結果的可靠性，且敏感數據僅在內部循環，避免與外部網路接觸，也間接降低洩密風險。因此資料庫的安全性與學習效能呈現出獨特的挑戰與際遇。

(一)挑戰

1.外部數據學習受限

封閉網路雖然降低了外洩風險，但也導致資料庫難以即時獲取最新的威脅情報，可能影響生成式AI的反應能力。

2.內部數據資源不足

國軍內部數據資源有限，難以支援資料庫持續擴充與優化。

(二)對策與建議

1.內部數據最大化利用

國軍應整合歷年資安攻防演練模擬數據與外界重大歷史資安案例，並建置結構化的數據標準，提升資料庫內容的深度與廣度。

2.採用離線更新機制

定期由國家數位發展部及國軍資安部門蒐整外界可信來源匯入最新資安威脅情報，並經過國軍資安及保防部分嚴格審查後導入資料庫，確保資料庫更新與安全兼顧。

3.建立高效模擬環境

在國軍內部資安實驗室的封閉網路中建構模擬測試平台，持續進行攻防演練，以優化資料庫的學習模型並驗證其效能。

4.強化生成審核流程

引入雙重驗證機制，包括資安專家審查與檢測軟體自動化檢測，確保資料庫的生成內容準確無誤。

三、單位自主防禦的一致性問題

國軍內部各單位在自主防禦系統的應用中，由於缺乏統一的技術標準和實施規範，可能導致防禦效能的參差不齊，進而影響整體網路安全。

(一)挑戰

1.技術能力不平衡

各單位的資安部門人員所擁有技術

資源與專業能力，會因為所在的單位層級或是個人處理資安事件經驗多寡，存在明顯差異，影響防禦系統的協同運作。

2.資安政策實施不一致

缺乏統一的實施規範與管理機制，容易產生防禦盲點與漏洞。

(二)對策與建議

1.制定全軍統一標準

國軍應建立涵蓋系統配置、數據共享與威脅應對的統一技術標準，作為所有單位的操作依據。

2.強化跨單位協作

定期組織全軍性的資安演練，模擬多單位協同應對網路攻擊情境，提升整體協作能力。

3.專責單位負責

建立國軍專屬人工智慧運算中心，負責國軍人工智慧運算人才培育及未來相關政策制定。

4.建立集中管理平台

由國軍人工智慧運算中心設置一個中央指揮與監控系統，統一管理各單位的防禦策略和數據資源，避免重複硬體建設與相關資源浪費。

四、管理人員的肆應性挑戰

AI自主防禦系統的引入對資安管理人員的專業能力提出更高要求，然而，部分管理人員的技術背景有限，可能影響新技術的有效應用。

(一)挑戰

1.知識斷層

資安管理人員對AI技術的理解不足，導致新技術導入初期的效能降低。

2.快速迭代帶來的學習壓力

AI技術的更新速度快，管理人員可能無法即時掌握最新知識。

(二)對策與建議

1.針對性教育訓練

國軍應設置專門課程，涵蓋AI基礎知識、實操技能以及案例分析，提升管理人員對新技術的掌握能力。

2.建立技術支援小組

成立跨單位的AI專家小組，為資安管理人員提供技術支持，解決實務操作中的疑難問題。

3.分層次實施技術導入

針對不同技術背景的管理人員，分層設計技術應用方案，確保技術導入的穩定性與高效性。

五、小結

本段落針對AI導入國軍自主防禦的主要挑戰進行了深入分析，並提出具體可行的解決方案。隨著AI技術的持續進步，國軍需要逐步完善技術標準、強化管理能力，並透過整體協調提升資安防禦能力，以應對不斷變化的網路威脅環境。

結論與未來發展

國軍目前採用封閉式網路，即軍網與民網實體隔離的方式，以確保國防資訊

的高度安全性。然而，隨著全球網路威脅的多樣化和即時性增強，封閉式網路在應對動態威脅與快速資料更新方面的限制日益顯現。特別是在烏俄戰爭的啟示下，軍事行動中與外界網路銜接的必要性越來越明顯，如何在此基礎上構建高效防禦體系，成為國軍資安管理的重要課題。以下將參考美軍及企業界成功經驗，提出三點具體建議。

一、建立內外部網路交互機制

在保持封閉式網路優勢的同時，透過制定嚴格的交互規範，建立與外部可信網路的安全數據交換機制。例如，設置離線資料導入流程，定期更新全球威脅情報，並由專門小組及檢核軟體進行審查與過濾。此機制可確保國軍能即時掌握最新的全球網路安全動態，同時有效降低數據洩露的風險。此外，國軍應與盟國及國際安全組織加強合作，共享經驗與情報，以提高對新型威脅的預判能力。

二、引入AI驅動的動態防禦技術

參考美軍與微軟的經驗，國軍應加強AI技術在資安管理中的應用，特別是肆應性防護和威脅預測技術。這些技術可以實現對潛在威脅的即時感知與應對，提升整體防禦能力。例如，國軍可引入基於深度學習的威脅分析系統，對網路流量和行為模式進行全面分析，預測可能的攻擊行為。同時，透過AI技術的自動化功能，實現快速事件響應和修復，減少人工介入所需時間，確保網路安全的即時性。

三、強化資安人員的專業培訓與技術支援

針對AI應用與封閉網路的特殊需求，建議成立專責單位如國軍人工智慧運算中心，由該中心負責設置分層次培訓計畫，確保資安人員具備即時更新與威脅分析的能力。例如，可設立AI基礎訓練班，教授資安人員如何使用和管理AI防禦系統，並進一步開設進階課程，深入研究AI威脅偵測模型的設計與應用。此外，成立專業技術支援小組，提供跨單位協調與技術支援，確保防禦策略的一致性與有效性。這些小組可在資安演練中發揮關鍵作用，協助單位快速識別薄弱環節並提供針對性解決方案。

國軍若能有效結合上述策略，將在面對日益增長的網路威脅時構建更具韌性與前瞻性的資安防禦體系。

(114年2月5日收件，114年5月19日接受)