

AI 辨識技術導入陸軍智慧型警監系統可行性之研究

作者:吳佳紋、王昱翔

提要

- 一、因應少子化及敵情威脅的變化，國軍兵力編現比持續下滑，應著力在各種應變作為，運用各種政策及專案，減低人力負荷。
- 二、近年隨著科技進步及政策調整，國防部於108年核定各軍種智慧型警監系統建置案，以確保營區整體安全，又可減輕警勤人力負荷。
- 三、運用AI影像辨識技術，導入現行智慧型警監系統，以確保精準並實時辨識異常行為、增加防範能力，進而顯著提高整體營區安全。

關鍵詞：AI 人工智慧、影像辨識、警監系統、人力需求

前言

我國的生育率自民國 73 年以來一直低於人口替代水準 2.1，並於 2023 年降至 0.865 人為歷史低點。根據立法院資料顯示，國防部為了應對防衛作戰兵力之需求，自 113 年起，94 年次以後出生的役男恢復徵集服常備兵現役，為期一年。然而，近年來國軍志願役人數變化顯著，於 110 年底達到近年最高的 16 萬 4,884 人後，111 年和 112 年底人數分別減少了 5,492 人和 4,706 人，減幅為 3.33% 和 2.95%。截至 113 年 6 月底，志願役人數再次下降至 15 萬 2,885 人(如表 1)，這不僅是自 107 年底以來的新低，還導致多個戰鬥部隊編現比未達 80%，這可能會對新式武器操作人力培訓及長期使用造成不利影響。¹且近年雖推動多元招募管道以穩定人力招募來源，惟提前退離人數及比率均頗高，不利人力穩定增補，造成近年來國軍兵力驟然下降，可顯見的為國軍刻正面臨「人員退損補充不及」、「招募志願役困難」與「編現比偏低並逐年增加」等人力補充困境。²國軍應著力在各種應變作為，運用各種政策及專案，減低人力負荷。

1 立法院，〈114年度中央政府總預算案整體評估報告〉，頁3-4，<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=55648&pid=243255>，檢索日期：西元年2025年5月20日。

2 柯永森，〈即時評析-國軍面對人力變化的轉機〉，《國防安全研究院》，2023年10月2日，<https://indsr.org.tw/focus?typeid=26&uid=11&pid=2669>，檢索日期：2024年10月10日。



表 1 106 至 113 年度 6 月底止國軍志願役人數及比率變化情形表

項目 年份	國軍 總人數	志願役			
		人數	占國軍 總人數比率	各年度 增加人數	各年度增加 人數比率
106 年	150,906	146,785	97.27	2,094	1.45
107 年	155,421	155,412	99.99	8,627	5.88
108 年	162,044	162,039	100	6,627	4.26
109 年	164,064	164,063	100	2,024	1.25
110 年	164,884	164,884	100	820	0.50
111 年	159,392	159,392	100	(5,492)	(3.33)
112 年	154,686	154,686	100	(4,706)	(2.95)
113 年	155,390	152,885	98.39	(1,801)	(1.16)
附記	()內數據為負數				

資料來源：作者整理，參考國防部主管 114 年度單位預算評估報告(註：)

國軍面對日益複雜的環境之下，現行各營區監視器多為一般型功能之警監系統，無具備位移偵測及告警之功能，已無法滿足即時反應需求；故國防部於民國 108 年 8 月核定「重要防護營區智慧型警監系統建置」案，全軍分年逐步建置，以確保營區整體安全及減輕警勤人力負荷。各營區運用此系統後，不僅能先期預警入侵徵兆，管制合法人員車輛進出，即時控管營區重點庫房及設備之狀況，也可減少人為誤判，進而有效提升營區安全防護之能力(如圖 1)。³

然該系統雖可判別是否有人員、車輛或是物體經過營區圍牆周圍，代替人員巡邏，達到維護營區安全之效益，惟系統內未建置物件危險動作偵測、物件追蹤等行為模式，以至於居民散步於營區周邊圍牆、汽機車行駛經過等無潛在損害營區安全之行為，智慧型警監均發出告警，仍需由執勤人員實施畫面判讀，方可得知是否為異常行為。故如何有效運用智慧型警監，並導入人工智慧之技術，實施人臉、車牌辨識及行為分析，有效降低人員判讀之作業，以達到減少人力成本為本文研究動機。

3 (產品介紹-資訊科技)《中山科學研究院》，https://www.ncsist.org.tw/csistdup/products/product.aspx?product_Id=70&catalog=12，檢索日期：2024年10月10日。



圖 1 中科院建置智慧型警監系統功能示意圖
資料來源：(產品介紹-資訊科技)《中山科學研究院》

傳統警監系統，畫面監控通常需要持續掃描來自多個監視器鏡頭的即時回傳，以檢測任何安全事件，許多組織會聘僱人員來執行這項工作。然而，研究指出，當人們同時監控 4 個螢幕時，辨識重要事件的能力可能會下降多達 20%，如果是 9 個螢幕，這一比例會達到 60%；考慮到許多設施及場所配備大量攝像頭，這項工作顯然超出了人們的能力範圍。⁴通過監視鏡頭進行的人工辨識會受到低解析度的嚴重影響，這會使識別入侵者變得更加困難，甚至可能導致錯過重要的安全警報。

隨著安全需求上升，如何有效透過 AI 技術以增強軍事安全，成為重要研究課題。因此，本研究旨在探討 AI 技術導入陸軍智慧型警監系統的可行性及其效益，分析目前警監系統現狀，並提出具體應對策略，將 AI 技術匯入警監系統，以有效降低、甚至取代傳統警監系統須以人員判讀監視畫面的工作負荷，以提升陸軍安全防護能力之目的。然 AI 技術為現行發展最新技術，仍有許多值得深入探討之方向，未來可針對智慧型警監法規分析、辨識技術運用評估、生成式 AI 運用等實施進一步研究，冀以提升智慧型警監系統運作效率，並確保其在法律範疇內的合規性。

4 Noah Sulman; Thomas Sanocki; Dmitry Goldgof; Rangachar Kasturi, "How Effective is Human Video Surveillance Performance" 2008 19th International Conference on Pattern Recognition (Tampa, FL, USA : IEEE Xplore , 08-11 December 2008), p1



AI 辨識技術概述

一、AI技術演進

人工智慧(Artificial Intelligence, AI)是計算機科學的一個分支，專注於解決與人們智慧相關之認知挑戰，例如學習、創造和圖像辨識。它透過多種來源蒐集大量數據資料，包括人類製造內容、監控設備、智慧感測器及系統日誌等。AI 核心目標是開發能夠自我學習的系統，這些系統從收集數據中提取有價值訊息，並且利用這些訊息以仿似人類之方式解決新問題。⁵

艾倫·圖靈(Alan Mathison Turing)於 1950 年提出「圖靈測試」(Turing Test)，為現正進行的人工智慧科學提供創新的理念及構思。1980 年代，AI 領域在此時期開始蓬勃發展，其中大衛·魯梅爾哈特(David Rumelhart)和約翰·霍普菲爾德(John Hopfield)發表了關於深度學習技術的論文，內文中表明了「電腦可以從經驗中學習」。

1990 年迄 2000 年初，AI 發展進入了新的領域，並且在眾多領域中獲得重要成就。受益於運算能力進步和大數據可用性之推動，2010 年代見證了深度學習的蓬勃發展。這個時代，人工智慧在自然語言處理、影像辨識和自動駕駛汽車等領域有了驚人進展(如圖 2)。隨著機器學習進步，基於邏輯的人工智慧逐漸消失，此時系統更專注於從數據資料庫進行統計推斷，取代了由人類所定義之規則。⁶

圖 2 AI 發展簡史



資料來源： 洪文彬，人工發展簡史，中台山月刊，246 期

5 (什麼是人工智慧 (AI)?)《Amazon》，<https://aws.amazon.com/tw/what-is/artificial-intelligence/>，檢索日期：2024年1月7日。

6 The Evolution and Future of Artificial Intelligence: A Student's Guide，< <https://www.calmu.edu/news/future-of-artificial-intelligence>>，檢索日期：2025年2月2日。



人工智慧（AI）可理解為具變革性、普遍性和顛覆性的新技術，用以執行通常需要人類智慧之任務，特別是當機器從資料中學習如何執行這些任務時。然而人工智慧技術的普及，從民間企業延伸到國防運用，各先進國家尋求在各種軍事方面使用人工智慧，包括網路作戰、遠程和自主系統、戰場覺知、任務規劃和目標定位、作戰分析和兵棋推演，以及戰術、作戰和戰略層面的軍事決策程序。

二、AI辨識技術運用

隨著時間推移，人工智慧技術逐年成熟，圖像辨識、影像處理及自然語言處理等領域的運用也日益增多。特別是在影像辨識技術方面，得益於視覺處理器（Graphics Processing Unit, GPU）的進步，早期僅能進行文字識別之影像辨識技術，如今已能夠精確識別動態影像，這一進展顯著提升影像辨識的能力和應用範圍。

AI 影像辨識技術應用範圍相當廣泛，不僅包含基本人臉和車牌辨識，還擴展至入侵偵測、醫療行為、互動遊戲、農業生產、商場行為分析、運動教學輔助、跌倒偵測以及產線公共安全等。這些技術能夠自動進行安全分析和異常事件的檢測與通報，進而大幅減少人力監控監視器之需求和時間。

AI 影像辨識技術主要依賴於機器學習和深度學習演算法的發展，為影像辨識帶來了重大變革。這些演算法允許系統自動從大量資料中挖掘和學習特徵，透過多層神經網路架構，AI 影像辨識技術能夠處理更加複雜之影像，並在各種應用場景中顯著提高識別準確度和速度。

影像辨識較常使用的卷積神經網路（Convolutional Neural Networks, CNN），在處理簡單圖像分割問題時已經展現出良好的性能。然而，當面對更為複雜圖像分割挑戰時，U-Net 出現顯得尤為關鍵。自 2015 年首次提出以來，U-Net 已被廣泛應用於生物醫學圖像的分割任務中，並因其高效性能而受到重視。⁷

YOLOv4(You Only Look Once)於 2020 年推出，因其能夠處理超過 60 幀每秒（Frames Per Second, FPS）的即時影像辨識問題而受到廣泛推崇。這一模型框架不僅延續了以往靜態影像分析技術，還在此基礎上進行了更為複雜的設計，使其在動態視覺應用中展現出更高效率和準確性。YOLOv4 出現標誌著電腦視覺技術在即時影像分析領域的重大進步，擴展了其在各種應用場景中之潛力，如交通監控和社交距離偵測等。⁸

7 鄭錦桐，〈坡地監測預警新技術-人工智慧影像辨識之應用〉，《坡地監測與防災預警技術、臺灣海域地質資源》，第40卷第3-4期，2021年，頁71，《臺灣地質知識服務網》

8 同註6



2024 年 9 月 30 日，ultralytics 官方團隊宣布 YOLOv11 正式發布，即時目標檢測器又一次重大升級，透過結合速度、精確度和多功能性，提升其前代產品功能。它採用重構架構和增強資料處理技術，在識別各種應用程式中複雜視覺模式方面提供無與倫比的性能。⁹YOLOv11 可在低光照條件或能見度較差環境下，仍可進行資料處理，如霧、或是夜間等惡劣條件下實施影像辨識。¹⁰

然而在即時影像辨識技術中，為確保目標偵測的迅速與正確，較常藉由 Precision(精確度)、Recall(召回率)、F1-score(F1 分數)、FPS(每秒幀數) 等指標實施判斷，提供有關其檢測準確性、靈敏度和一致性的見解。在 Luhao He、Yongzhang Zhou 的眾多學者研究當中，均發現 YOLOv11 為當前影像辨識技術，在準確性、泛化性和穩健性之間提供了最佳平衡。¹¹

三、各國AI影像辨識技術運用現況

人工智慧技術快速發展，影像辨識技術已成為各行各業的重要工具，並且其準確性和效率不斷提升，以下就先進國家藉由 AI 辨識技術運用於軍事領域之案例：

(一)美國

1.美國陸軍正在測試一種命名「Scylla」為新人工智慧產品(如圖 3)，據稱該產品可以識別一英里外之威脅。¹²負責核子事務的國防部副助理部長德魯·沃爾特(Drew·Walter)所描述這個虛構場景展示了人工智慧所展示之能力-即時學習能力和減少滋擾警報能力——這些警報會讓安全人員感到疲勞並抑制對合法威脅的反應——解決了物理安全方面長期存在的挑戰，美國國防部正在研究人工智慧增強現有監視和威脅偵測的能力，以配合該部門在其業務中整合數據、分析和人工智慧更廣泛的策略。¹³

9 Asif Razzaq, "YOLO11 Released by Ultralytics : Unveiling Next-Gen Features for Real-time Image Analysis and Autonomous Systems," Marktechpost, <https://www.marktechpost.com/2024/10/03/yolo11-released-by-ultralytics-unveiling-next-gen-features-for-real-time-image-analysis-and-autonomous-systems/>,檢索日期：2025年2月1日。

10 Deep Chokshi, "Understanding YOLOv11: The Future of Real-Time Object Detection" Zenithfuture, <https://zenithfuture.com/understanding-yolov11-the-future-of-real-time-object-detection/>,檢索日期：2025年4月23日。

11 Luhao He, Yongzhang Zhou, Lei Liu, Yuqing Zhang, Jianhua Ma, "Application of the YOLO v11-seg algorithm for AI-based landslide detection and recognition" National Library of Medicine, <https://pmc.ncbi.nlm.nih.gov/articles/PMC11992019/#CR76>,檢索日期：2025年5月20日。

12 Brandon Vigliarolo, "US Army turns to 'Scylla' AI to protect depot", The register, Tue29Oct2024, https://www.theregister.com/2024/10/29/us_army_scylla_ai/,檢索日期：西元2024年11月29日。

13 Army Maj. Wes Shinego, "Defense Department Tests AI Software, Advances to Improve Physical Security Posture", U.S. Department of Defense, 28Oct2024, <https://www.defense.gov/News/News-Stories/Article/Article/3946607/defense-department-tests-ai-software-advances-to-improve-physical-security-post/>,檢索日期：西元2024年11月29日。



圖 3 Scylla 偵測入侵者

資料來源：〈Defense Department Tests AI Software, Advances to Improve Physical Security Posture〉

2.美國陸軍物理安全企業與分析小組(The U.S. Army's Physical Security Enterprise and Analysis Group)於 2024 年起發起了為期兩年的系統測試，該安全系統是一種商用現貨專有產品，提供即時模組化的物理威脅監測。藉由人工智慧和深度學習的電腦視覺技術，通過識別物體、入侵者、槍械、打鬥、滑倒和跌倒情況，以及煙霧和火災發生，並進行臉部辨識和異常行為監控，來完成電子安全系統的現代化。¹⁴

(二)英國

英國國防科學技術研究室(Dstl)與 L3Harris、Marlborough Communications Ltd 和 AeroVironment (Tomahawk Robotics) 合作進行了試驗，以機器犬拆除炸彈，使用機器人上的感測器進行遠端分類和識別威脅，這些測試將最大限度地減少軍事人員暴露於危險之中，提高執行任務效率及維護安全。¹⁵

(三)以色列

以色列媒體「+972 Magazine」和「Local Call」報導指出，以色列軍方正在使用一種名為「福音」(Gospel, Habsora)的人工智慧目標設定系統(如圖 4)，此系統能夠分析大量數據以識別模式並確定攻擊目標。該 AI 平台幾乎具備自主確定目標的能力，其運作速度顯著超過以往，能夠更迅速地選擇對加薩之轟炸目標，並在攻擊前預測可能造成的死亡人數。¹⁶

14 〈Testing of AI software for security and protection taking place at BGAD〉，《U.S.ARMV》，https://www.army.mil/article/275213/testing_of_ai_software_for_security_and_protection_taking_place_at_bgad，檢索日期：西元2025年4月27日。

15 〈New robots lead the way in bomb disposal innovation〉，《GOV.UK》，<https://allisrael.com/idf-uses-ai-facial-recognition-tech-to-identify-terrorists-in-gaza>，檢索日期：西元2025年4月27日。

16 〈顛覆傳統戰 以色列在加薩戰爭的AI運用〉，《中央廣播電台》，<https://www.rti.org.tw/news/view/id/2191578>，檢索日期：西元2025年4月27日。

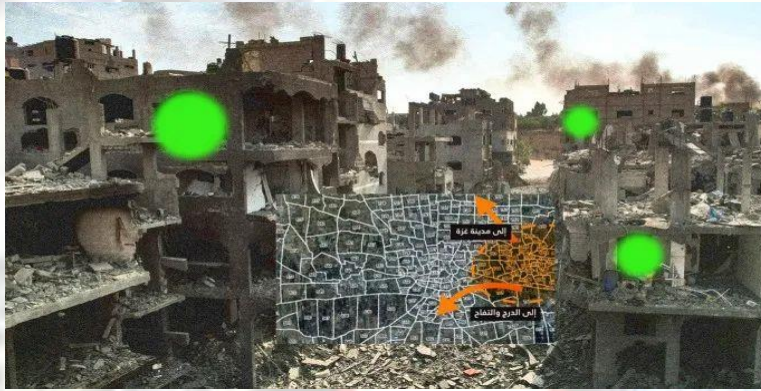


圖 4 福音人工智慧系統

資料來源：安全內參<加沙戰場上的“殺戮算法”：以色列“福音”(Gospel)人工智能平台>

以色列藉 AI 影像辨識技術，來識別巴勒斯坦恐怖份子，尤其是 2024 年 10 月 7 日大屠殺，以色列公司 Corsight AI 開發了一種可以與 Google 應用程式（Google Photos App）配合使用的臉部識別技術，以色列國防軍在戰場上利用 Google 高級照片搜尋功能來識別某人為恐怖組織成員。¹⁷

(四)中共

AI 影像辨識技術在中國大陸應用非常廣泛，為了維護社會治安和穩定，中共政府近年來積極推動人臉識別系統建設，稱為「天網工程」是目前世界上最龐大的監控系統，已在 16 個省、市、自治區安裝了超過 1 億 7,000 萬個攝影鏡頭，這些鏡頭隨處可見，系統利用動態人臉識別和大數據分析技術，能在最短 3 秒內對拍攝畫面進行精確識別，一旦通緝犯影像被捕捉到，系統會立即通知最近的警察，迅速展開逮捕行動。¹⁸



圖 5 中共天網工程

資料來源：自由時報<制裁、貿易限制接踵而至 中國「天網」工程快崩壞>

17 〈IDF uses AI facial recognition tech to identify terrorists in Gaza〉，《allisraelnews》，<https://allisrael.com/idf-uses-ai-facial-recognition-tech-to-identify-terrorists-in-gaza>，檢索日期：西元2025年4月27日。

18 〈中國6億支「天眼」監控 記者實測7分鐘就遭逮〉，《遠見》，<https://www.gvm.com.tw/article/60799>，檢索日期：西元2025年2月2日。



(五)我國

我國在 AI 影像辨識技術運用隨著技術進步，逐漸在各個領域中展開應用，然國防部考量現代戰場環境變化快速於 114 年 2 月 24 日公開徵集民間企業針對「衛星影像 AI 自動辨識」提供企劃書，因應新興國防挑戰，期藉快速開發及導入應用，有效提升軍事作戰與戰備整備效能。¹⁹

陸軍營區警監系統導入 AI 辨識技術之可行性

隨著科技迅速發展，人工智慧（AI）技術在各行各業的應用越來越廣泛，特別是在安全監控領域。陸軍營區安全管理面臨著日益增長的挑戰，傳統監控系統已無法滿足現代化需求，這些間、空隙統往往依賴人工操作，無法及時反應潛在安全威脅，導致反應時間延遲，增加安全風險。

AI 技術導入不僅能夠自動化監控過程，還能通過高效數據分析，及時識別可疑行為和異常事件。這樣的系統能夠整合影像辨識、行為分析等多種技術，提供更全面之安全防護。此外，AI 系統還能學習和適應不同環境變化，隨著時間推移，提升其識別準確性和反應速度，這不僅減輕戰情官工作負擔，還能確保營區安全管理更加高效、可靠，為日常運作提供強有力的支持。因此，導入 AI 辨識技術以提升營區安全性和管理效率，成為一項重要之研究課題。

一、智慧型警監架構

鑑於近年屢有不明人士對營區進行情報蒐集和偽裝，試圖闖入重要機敏處所，另為因應國軍組織精簡，營區衛哨勤務之執行密度不復以往，國防部爰於 108 年提出「重要防護營區智慧警監系統」。²⁰智慧型警監系統架構由中央監控系統、智慧型警監系統、影像監控傳輸系統、維護報修系統 4 大系統組成，以下針對智慧型警監架構實施說明。

(一)中央監控系統

建置於營區戰情室，置情態牆以顯示中央監控平台和遙控站，執行緊急狀況的通訊。中央監控平台採用圖形化管理介面，主要操作界面以營區電子地圖呈現，並能迅速整合多方資訊。系統會即時彈出警報視窗，提供入侵影像、時間、地點及應對標準作業流程等資訊，以協助管理者進行應變處理。²¹

19 〈國防部發布新聞稿，針對「國防創新小組公開徵集」乙情說明〉，《中華民國國防部》，<https://www.mnd.gov.tw/Publish.aspx?p=84060&title=%E5%9C%8B%E9%98%B2%E6%B6%88%E6%81%AF&SelectStyle=%E6%96%B0%E8%81%9E%E7%A8%BF>，檢索日期：西元2025年4月27日。

20 立法院，〈國防部主管113年度單位預算評估報告〉，頁1，<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=46442&pid=232638>，檢索日期：西元2025年2月4日

21 中科院，〈國軍「重要防護營區智慧型警監系統建置案」-第二階段110年擴大教育訓練資料〉，2021年，頁 8-9。



(二)智慧型警監系統

具備入侵偵測、車牌辨識、環控系統等 3 種功能，能夠主動發出警報，實時掌握狀況，有效監控營區狀況，增強危險事件的取證能力，減少誤判並降低人力負擔，以提升安全警戒之防護效果。²²

1.入侵偵測：透過 3 種不同類型的攝影機進行偵測(如表 2)，監視鏡頭均具圍牆入侵偵測功能，可主動告警並即時通報，以防範不明人士入侵營區。

表 2 各監視鏡頭介紹

各式攝影機	功能
固定式攝影機	具夜視及影像辨識功能，可自動調整光圈，建置於圍牆週邊(每 30 公尺建置乙支為原則)。
旋轉型攝影機	無影像辨識功能，輔助固定式攝影機不足範圍(建置於營區圍牆、空曠無遮蔽區域)，具備手動控制鏡頭 360 度旋轉功能。
熱顯像攝影機	具影像辨識功能，佈建於圍牆周邊(濃霧或長時間低光源處所)，感應監控區域周遭熱源據以成像。

資料來源：中科院，國軍「重要防護營區智慧型警監系統建置案」-110 年擴大教育訓練資料

2.車牌辨識：建置於大門衛哨口，具備全天候辨識能力，透過車牌辨識攝影機捕捉即時動態影像，快速獲取車牌號碼並透過車牌辨識軟體進行資料庫比對，確認是否為合法車輛，並將結果顯示於哨口螢幕，輔助營門執勤人員，達到有效管理車輛進出。

3.環控系統：建置於重要及高價值軍品庫房等處所，能有效偵測環境維安因子，另於油彈庫建置防爆型攝影機，可阻絕殼內電器部件之火花，避免於易燃易爆環境造成重大災損。²³

(三)影像監控傳輸系統

基礎設施將外圍設備的信號傳送回機房，並在營區內部建立環場光纖及網路傳輸系統。其中環場光纖的佈建設置了網路節點（大型拉線箱），用以容納資訊和電力線路，並透過工業級交換器進行數據傳輸；而營外的連接則形成獨立的監控網域，利用國軍的環島頻寬系統實現跨營區的網路連接，上級單位可監看轄下營區影像及告警資訊。²⁴

²² 同註19，頁12。

²³ 同註19，頁13-15。

²⁴ 同註19，頁20-22。



(四)維護報修系統

藉由線上系統報修維護機制，由營區使用者登入系統，進行線上報修與記錄查詢，報修後即啟動維修機制，亦可同步掌握報修資訊。²⁵

二、運用現況

智慧型警監之影像辨識功能因對環境的反應過於敏感，如營區圍牆附近居民於周圍散步或機車騎士經過等無侵入動作，均會頻繁觸發假警報；為避免以偏概全，認為建置智慧型警監之營區均有此狀況，以及使本研究案更臻完善，分別對南部單位智慧型警監維管人員、空軍某單位通信官及中科院警監案南部承辦參謀等 10 員實施訪談，藉由各單位維管經驗與角度瞭解運用現況，作為後續分析之參據(如表 3)。

表 3 智慧型警監系統功能與運用現況對照

系統功能	系統能力	運用現況
對於人形辨識、異常行為，辨識有無侵入之虞	入侵偵測、減少誤判	營區圍牆附近居民於附近散步，系統均實施告警，無法有效判斷侵入或是破壞營區之異常行為。
對於可疑行為之告警提示	可主動告警並即時通報	具告警功能，然其告警設定過敏感(警報是藉由設定警監虛擬界範圍實施告警，非以異常行為分析實施警報)
車牌辨識功能	快速獲取車牌號碼並透過車牌辨識軟體進行資料庫比對，確認是否為合法車輛	0 與 O 無法精準正確辨識，且無具備非該營區車輛停留超過 1800(預估會客人員或維修廠商需離營之時間)之提示。
高價值軍品庫房等處所，具偵測環境維安因子	建置於重要及高價值軍品庫房處所，能有效偵測環境維安因子	僅設置於庫房門口，無法針對庫房內裝備囤儲狀況實施偵測，且無法辨識進入庫房是否為經查核人員，有無竊盜軍品之虞。
維護報修系統	進行線上故障報修與記錄查詢，報修後即啟動維修機制	提供網址時有無法連線狀況，單位透過其他方式(如 line、公文)實施報修。

資料來源：本研究整理

²⁵ 同註19，頁23。



三、智慧型警監導入AI辨識技術之探討

隨著近期外部威脅增加，不管是民眾闖入營區，或是可疑人士於營區周圍窺探軍事資訊之行為，這不僅對軍事安全構成威脅，也引發社會對於營區安全管理的關注，以現行智慧型警監系統之監控方式已無法滿足現代軍事需求，系統在面對突發事件反應能力和靈活性仍有提升空間。

Anduril 為美國成立於 2017 年的國防技術公司，並於 2020 年展示 Lattice 系統，該系統提供一系列自主防禦系統，軍事威脅不斷演變的狀況下，必須以有限人力應對，此系統可在戰術邊緣提供跨陸地、海上和空中綜合、持續之感知和安全；在官方演示中，當卡車靠近軍事基地時，Standard Range Sentry Tower (AI 監視塔)會將它識別為威脅，派出無人機監控，並在對方放出無人機時發動攻擊擊毀。過程中，值班人員只需點擊滑鼠，授權 AI 執行。²⁶

其他國家已利用 AI 技術執行軍事安全維護的前例，我軍如何藉由 AI 影像辨識技術來補足現行智慧型警監不足，成為當前亟需解決問題，AI 影像辨識技術能夠提供優勢：

(一)提升即時監控能力

AI 影像辨識技術能夠即時分析監控畫面，快速識別可疑行為或異常活動。這種技術可以自動檢測人員進出、聚集或其他可疑行為，並即時發出警報，從而提高對潛在威脅的反應速度，其優勢主要體現：

1.提高準確性

藉導入 AI 影像辨識技術，利用人工智慧和機器學習技術，使智慧型警監系統可透過分析歷史數據來改善監控效果。系統可以處理大量影像資料，自動調整監控參數，並持續增強對潛在威脅的識別能力。隨著時間推移及資料蒐整，使系統智能化程度和準確性顯著提升。

2.即時反應

智慧型警監系統利用先進影像處理和分析技術，可實時辨識異常行為，如自動識別可疑活動，例如入侵、打鬥或者可疑人士徘徊時間過長，並立即發出警報，這種即時反應能夠大幅縮短處理時間，從而有效降低事故發生率。

3.增強預警系統

透過 AI 辨識技術，能實時監測可疑行為或人員異常行為，從而顯著提高整體營區安全，且戰情官可及早獲得準確地告警訊號，同步實施危險事件處

26 〈Anduril's Lattice: a trusted dual use — commercial and military — platform for public safety, security, and defense〉，《anduril》，<https://www.anduril.com/article/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security/>，檢索日期：西元2025年4月27日。



理，以增強防範能力。

(二)減少人力需求

AI 影像辨識技術的引入可以減少對人力依賴，降低戰情官時時監看畫面的工作，使其能夠專注於戰情官本身需要執行的工作，其優勢體現：

1.減少重複性工作

現行智慧型警監系統其告警無法確實辨別危險事件，造成聲音告警頻繁，戰情官需以人為方式判斷該告警是否真具有潛在之危險，這不僅間接增加戰情官工作量，也可能導致重要事件的反應延遲；隨著科技進步，藉由 AI 影像辨識技術，使告警系統可更精準識別具危險之動作、人員、車輛等，進而減少戰情官重複性之判別工作，降低誤判風險(如待命班和營區應變部隊出勤)。

2.提升工作效率

AI 影像辨識技術另一優勢在於其高效性，相比人工操作，AI 技術能藉由系統，以更快速度分析龐大數據，因戰情官減少重複性判別之動作，從而減少人力成本和錯誤率，也因準確的影像識別，為營區安全提供更有效之保障。

導入 AI 辨識技術之限制

在當今數位化和智能化的時代，人工智慧（AI）技術快速發展在各行業帶來變革，尤其是軍事和安全領域，陸軍營區警監系統導入 AI 辨識技術，旨在提升監控效率 and 安全性，然而這一過程中也伴隨著多種技術風險和限制。

一、數據資料偏差

偏差可能出現在人工智慧流程運作中各個階段，這種偏差主要來源之一是資料蒐集。如果用於訓練人工智慧演算法的資料不夠多樣化或缺乏代表性，那麼最終輸出可能會有偏差。²⁷

許多人認為 AI 演算法所產生的結果是客觀且中立，這是一種錯誤觀念。AI 演算法結果可能因多種因素而出現偏差和偏誤，例如訓練 AI 所使用之數據庫可能本身就存在偏誤，或是資料不夠全面，未能涵蓋所有可能的情況。此外，間接資料可能無法準確代表所需計算的資訊，並且有時候會因為特定目的操作而導致 AI 運算結果出現有意之偏差。²⁸

麻省理工學院研究員喬伊·布奧拉姆維尼（Joy Buolamwini）指出，由於 AI 訓練所用資料缺乏多樣性，三家知名科技公司臉部辨識系統在識別深膚色女性

27 “Bias in AI”, Chapman University, <https://www.chapman.edu/ai/bias-in-ai.aspx>, 檢索日期：西元2025年2月3日。

28 楊宏文，〈AI又不是真的人，為什麼會有偏見？〉，《緯育TibaMe》<https://blog.tibame.com/?p=23197>，檢索日期：西元2025年2月2日。



時錯誤率超過 20%。相比之下這些系統在識別淺膚色男性時的錯誤率僅為 0.8%，這可能是因為在訓練初期就獲得了大量相關資料。此外 2015 年 Google 影像辨識系統曾將非裔用戶錯誤標記為「大猩猩」，並因此公開道歉，這些例子顯示辨識系統在識別深膚色人群時存在明顯的種族歧視問題。²⁹

首先，在數據不完整或是資料不夠齊全的狀況下，可能不具有代表性，而造成資料不平衡，資料庫內某些群體樣本數量遠遠超過其他群體，這就使得 AI 系統更容易偏向這些群體，而對其他群體忽略不計；或是資料庫內的數據集，包含人類世界本來就存在偏差，故 AI 系統運作時，所產出結果也會造成偏差。

其次，如果程式設計者對相同標籤有不同解釋，則可能會引入偏差，演算法設計合理性與否，對於 AI 偏差也至關重要，如果模型設計不當，或過度依賴某些特定特徵，那麼就會增加偏差產生的可能性。

二、辨識系統合法性

隨著人工智慧（AI）技術快速發展，AI 影像辨識系統，特別是人臉辨識技術，在各種應用中變得越來越普遍，這些技術在執法、公共安全及商業監控等領域之使用引發廣泛的法律與倫理爭議。1890 年美國可藉由拍照，將瞬間影像留存下來，而開始興起隱私權運動，而人臉辨識技術不僅是拍照，更能藉由辨識將一個人的行蹤與行為記錄下來。³⁰

自 2018 年蘋果公司推出 iPhone X 並引入 Face ID 解鎖功能以來，人臉辨識技術迅速成為日常生活中不可或缺的工具。隨著生物辨識技術快速進步，越來越多企業開始投入資源，在確定使用臉部辨識技術時，必須解決許多問題，這些問題應包括：誰被允許使用這些技術，誰被允許蒐集和處理生物特徵數據，是否應該承擔風險，人臉辨識使用應如何符合資料最小化、資料準確性、儲存限制、資料安全和問責的要求，以及合法、公平和透明，並遵循特定、明確且合法之目的。³¹

AI 辨識技術使用常常涉及到個人隱私的侵犯，然而，許多 AI 系統在運作過程中，可能會在未經個人同意下，蒐集和處理個人數據，這將導致法律責任，例如某些城市使用人臉辨識技術進行公共監控，這可能導致對個人自由的侵犯，為避免智慧型警監導入 AI 辨識技術，造成人權侵害案件發生，相對應監督管制措施也必須與時俱進。目前針對保護個人數位資料和隱私的規範，為歐盟

29 柳欣宇、黃英哲，〈AI不中立？—探討AI偏見帶來的影響〉，《科技大觀園》檢索日期：西元2025年2月2日。

30 陳箴，〈人臉辨識技術之風險與管制：微軟企業觀點〉，《臺灣人工智慧行動網1》<https://ai.iias.sinica.edu.tw/facial-recog-tech-risk-and-regulation-microsoft/>,2020/3/6，檢索日期：西元2025年2月3日。

31 Mais Qandeel，〈Facial recognition technology: regulations, rights and the rule of law〉，《PubMed Central》<https://pmc.ncbi.nlm.nih.gov/articles/PMC11183273/pdf/fdata-07-1354659.pdf>,2024/6/4,p12，檢索日期：西元2025年2月3日



2018 年 5 月實施《一般資料保護規則》(General Data Protection Regulation, GDPR)。不過 GDPR 所保護對象僅限於歐洲地區的居民。³²

我國個資法在面對 AI 影像辨識技術時，需加強對資料蒐集、處理及保護的規範，透過完善法律和技術結合，可以更有效保障個人隱私權益，促進 AI 技術負責任之使用。隨著技術進步，我國於民國 112 年 12 月 5 日成立「個人資料保護委員會籌備處」，針對數位人權已將設置個人資料保護獨立監督機關列為優先推動事項，³³持續更新和調整法律框架將是必要的，以確保個資法能夠有效應對未來挑戰。

三、人員培訓與適應性問題

儘管 AI 影像辨識技術導入各行業警監系統，均展現出顯著優勢，但其成功仍需依賴各監看人員培訓與適應能力。然陸軍現行人員編現比不高前提下，部隊長可能會優先考慮保持現有人力資源，例如單位正面臨緊急任務或戰備需求，主官可能會選擇確保部隊能夠隨時投入任務，而不願意將人員送訓抑或優先派訓主戰裝備(如武器及車輛等)操作訓練；惟為確保操作人員能夠熟練警監系統，人員必須進行專門培訓，部隊長面臨單位人員編現不足、多重任務與派訓之要求下，參訓人員的素質與遴選顯得格外重要，這不僅涉及技術層面挑戰，還需要考慮單位整體人員培訓與適應性問題。

四、國軍網路頻寬及資安風險

隨著國軍未來計畫將網路雲端化，頻寬需求和資安風險將成為亟待關注的議題。首先雲端化將顯著增加對頻寬需求，來自各種傳感器、無人機和其他作戰設備的實時訊息，這些數據傳輸需要穩定且高速之網路支持，然而，現行營區軍網若非重要據點，頻寬約 10M 以內，固有網路頻寬無法滿足這一需求，特別是在高強度作戰環境中，頻寬不足可能導致訊息延遲，進而影響指揮決策的效率和準確性。

其次，資安風險也是雲端化過程中不可忽視的問題。隨著軍事數據轉移至雲端，數據洩露和未經授權訪問之風險將顯著增加。雲端環境的開放性使得黑客攻擊可能性上升，特別是在當前全球網路攻擊頻繁之狀況下，陸軍敏感訊息可能成為攻擊目標。此外雲端服務供應商若未能提供足夠安全的防護措施，將進一步加大資安風險。過去案例顯示，許多國家在雲端服務中遭遇數據洩露事

32 甘偵蓉，〈個人隱私在AI時代面臨哪些風險？資料治理的重要性〉，《科學月刊》<https://www.scimonth.com.tw/archives/6173>，檢索日期：西元2025年4月27日。

33 個人資料保護委員會籌備處，〈最新消息-設置個人資料保護獨立監督機關加強個人資料保護行政院院會通過「個人資料保護委員會組織法」草案及「個人資料保護法」部分條文修正草案〉，https://www.pdpc.gov.tw/News_Content/20/907/，檢索日期：西元2025年4月27日。



件，這對國家安全構成嚴重威脅。

五、小結

現行營區智慧型警監的距離告警，數據設置過於敏感，將造成警報疲勞，這種疲勞不僅影響值班人員警覺性，也可能導致真正安全威脅被忽視；監視器識別技術未能有效區分正常行為與潛在威脅，這使得系統在面對日常活動時反應過度，為了解決這些問題，系統需要進一步優化，提升對行為的識別能力，並調整告警靈敏度，以確保能夠準確反映出真正安全威脅。

在科技不斷日新月異下，AI 技術持續進步，操作人員需要持續學習以跟上技術發展，這對於人員專業素養和學習能力要求更高，鑑於部隊編現不足與多重任務考量，應朝專業訓練常態化、全員普訓及階段評鑑等方式實施。面對國軍網路雲端化過程，人員的資安意識和管理能力也需同步提升，若操作人員對雲端技術理解不足，或未能遵循相應資安規範，將可能導致內部數據洩露。

AI 影像辨識技術在警監系統應用具有極大潛力，但同時也面臨法律、數據和人員培訓等多方面挑戰，為了有效克服這些限制，應建立完善法律框架、提高技術準確性、加強數據管理以及整合資源等解決方案，進而提升營區安全防護的管理效能。

結論與建議

一、結論

AI 影像辨識技術在智慧型警監系統的應用，能夠顯著提升營區安全防護能力，透過即時監控、預警系統、減少人力需求、提高資料分析能力，這些優勢將有助於陸軍更有效應對日益複雜之安全挑戰。

推動智慧型警監加入 AI 影像辨識技術應採分階段方式進行，短期(1-6 個月)內專注原型開發、數據蒐集與測試，中期(6-18 個月)置重點於實地部署與使用者回饋收集(試行驗證)，長期(18-36 個月)則朝系統全面擴展與整合，並透過明確的關鍵績效指標(KPI)，以確保每個階段目標能夠有效達成。

隨著人工智慧技術快速發展，該技術廣泛運用於醫學、農業、政府及警界，藉以提升工作效能，相信未來在中科院及司令部等相關單位研究與執行，將逐步實現智慧型警監 AI 影像辨識技術之願景。

二、建議

(一)廣泛數據蒐集，提升系統可靠性

避免系統出現辨識偏差，造成無效告警，需確保資料庫數據多樣性為關鍵，數據集應涵蓋不同的年齡、性別、體型、車輛、危險動作和環境樣本，以減少



偏差風險，這些可以透過不同營區周圍環境影像數據來蒐集，數據的多樣性能夠顯著提高 AI 系統準確性，並降低數據偏差。

(二)強化政策支持，完善法規體系

影像辨識技術導入警監系統所造成個人隱私法律問題，可僅將營區現職人員臉部輸入系統，避免判別民人面部資料；另應該進一步強化對收集到的影像數據之保護措施。這些措施應包括對數據進行加密，限制對數據訪問權限，並定期與保防官共同進行安全檢查，以防止數據洩露或被不當使用。此外，應該建立數據刪除機制，確保人員離退時從資料庫刪除，不再需要使用這些數據時，能夠及時、安全地刪除，從而減少潛在隱私風險。

(三)結合科技現況，提升人員專業

實務操作訓練是提升人員技能的重要環節，中科院及相關研發單位應設置模擬環境，讓學員在真實情境中進行操作，熟悉系統各項功能和應用。這不僅能提高學員操作熟練度，並增強其對系統的信任感和使用意願。隨著技術快速發展，相關人員專業知識和技能必須與時俱進，以確保系統有效運行和管理。

(四)邊緣運算，降低資安風險

邊緣 AI 在資料產生現場進行即時資料處理，即時性使得值班人員可在重要情況下立即做出決策，進而有效提升維護營區安全效率。大量資料需要上傳至雲端進行分析，這無疑會消耗大量網路頻寬，邊緣 AI 若於本地進行處理，減少對雲端依賴，只將關鍵資料傳輸至雲端，從而有效節省頻寬成本，同時減少資料傳輸過程風險，提升資料保護的有效性。

參考文獻

一、中文部分：

(一)期刊專題

1.鄭錦桐，〈坡地監測預警新技術-人工智慧影像辨識之應用〉，《坡地監測與防災預警技術、臺灣海域地質資源》，第 40 卷第 3-4 期，2021 年，頁 71，《臺灣地質知識服務網》。

(二)官方文件

1.立法院，〈國防部主管 113 年度單位預算評估報告〉，頁 1，<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=46442&pid=232638>，檢索日期：西元年 2025 年 2 月 4 日。

2.中科院，〈國軍「重要防護營區智慧型警監系統建置案」-第二階段 110 年擴大教育訓練資料〉，2021 年，頁 8-9。



3.個人資料保護委員會籌備處，〈最新消息-設置個人資料保護獨立監督機關加強個人資料保護行政院院會通過「個人資料保護委員會組織法」草案及「個人資料保護法」部分條文修正草案〉，https://www.pdpc.gov.tw/News_Content/20/907/，檢索日期：西元 2025 年 4 月 27 日。

4.立法院，〈114 年度中央政府總預算案整體評估報告〉，頁 3-4，<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=55648&pid=243255>，檢索日期：西元年 2025 年 5 月 20 日。

(三)網際網路

1.柯永森，〈即時評析-國軍面對人力變化的轉機〉，《國防安全研究院》，2023 年 10 月 2 日，<https://indsr.org.tw/focus?typeid=26&uid=11&pid=2669>，檢索日期：2024 年 10 月 10 日。

2.(產品介紹-資訊科技)《中山科學研究院》，https://www.ncsist.org.tw/csi/stdup/products/product.aspx?product_Id=70&catalog=12，檢索日期：2024 年 10 月 10 日。

3.(什麼是人工智慧 (AI) ?)《Amazon》，<https://aws.amazon.com/tw/what-is/artificial-intelligence/>，檢索日期：2024 年 11 月 7 日。

4.〈中國 6 億支「天眼」監控 記者實測 7 分鐘就遭逮〉，《遠見》，<https://www.gvm.com.tw/article/60799>，檢索日期：西元 2025 年 2 月 2 日。

5.楊宏文，〈AI 又不是真的人，為什麼會有偏見？〉，《緯育 TibaMe》<https://blog.tibame.com/?p=23197>，檢索日期：西元 2025 年 2 月 2 日。

6.柳欣宇、黃英哲，〈AI 不中立？—探討 AI 偏見帶來的影響〉，《科技大觀園》檢索日期：西元 2025 年 2 月 2 日。

7.陳箴，〈人臉辨識技術之風險與管制：微軟企業觀點〉，《臺灣人工智慧行動網 1》<https://ai.ias.sinica.edu.tw/facial-recog-tech-risk-and-regulation-microsoft/>,2020/3/6，檢索日期：西元 2025 年 2 月 3 日。

8.甘偵蓉，〈個人隱私在 AI 時代面臨哪些風險？資料治理的重要性〉，《科學月刊》<https://www.scimonth.com.tw/archives/6173>，檢索日期：西元 2025 年 4 月 27 日。

9.〈顛覆傳統戰 以色列在加薩戰爭的 AI 運用〉，《中央廣播電台》，<http://www.rti.org.tw/news/view/id/2191578>，檢索日期：西元 2025 年 4 月 27 日。

10.〈國防部發布新聞稿，針對「國防創新小組公開徵集」乙情說明〉，《中華民國國防部》，<https://www.mnd.gov.tw/Publish.aspx?p=84060&title=%E5%9C%8B%E9%98%B2%E6%B6%88%E6%81%AF&SelectStyle=%E6%96%B0%E8%81%9E%E7%A8%BF>，檢索日期：西元 2025 年 4 月 27 日。



二、外文部分：

(一)研討會論文

1.Noah Sulman; Thomas Sanocki; Dmitry Goldgof; Rangachar Kasturi,” How Effective is Human Video Surveillance Performance” 2008 19th International Conference on Pattern Recognition(Tampa, FL, USA : IEEE Xplore, 08-11 December 2008),p1。

(二)網際網路

1.The Evolution and Future of Artificial Intelligence: A Student’ s Guide , < <https://www.calmu.edu/news/future-of-artificial-intelligence>>,檢索日期：2025 年 2 月 2 日。

2.Asif Razzaq, “YOLO11 Released by Ultralytics : Unveiling Next-Gen Features for Real-time Image Analysis and Autonomous Systems,” Marktechpost, <https://www.marktechpost.com/2024/10/03/yolo11-released-by-ultralytics-unveiling-next-gen-features-for-real-time-image-analysis-and-autonomous-systems/>,檢索日期：2025 年 2 月 1 日。

3.Brandon Vigliarolo, “US Army turns to 'Scylla' AI to protect depot” , The register, Tue 29 Oct 2024,https://www.theregister.com/2024/10/29/us_army_scylla_ai/,檢索日期：西元 2024 年 11 月 29 日。

4.Army Maj. Wes Shinego, “Defense Department Tests AI Software, Advances to Improve Physical Security Posture” , U.S. Department of Denfense, 28 Oct 2024, <https://www.defense.gov/News/News-Stories/Article/Article/3946607/defense-department-tests-ai-software-advances-to-improve-physical-security-post/>,檢索日期：西元 2024 年 11 月 29 日。

5. “Bias in AI” ,Chapman University, <https://www.chapman.edu/ai/bias-in-ai.aspx>,檢索日期：西元 2025 年 2 月 3 日。

6.Mais Qandeel ,〈Facial recognition technology: regulations, rights and the rule of law〉,《PubMed Central》<https://pmc.ncbi.nlm.nih.gov/articles/PMC11183273/pdf/fdata-07-1354659.pdf>,2024/6/4,p12,檢索日期：西元 2025 年 2 月 3 日。

7. 〈Testing of AI software for security and protection taking place at BG AD〉,《U.S.ARMV》, https://www.army.mil/article/275213/testing_of_ai_software_for_security_and_protection_taking_place_at_bgad , 檢索日期：西元 2025 年 4 月 27 日。

8. 〈New robots lead the way in bomb disposal innovation〉,《GOV.UK》, <https://allisrael.com/idf-uses-ai-facial-recognition-tech-to-identify-terrorists-in-gaza> , 檢索日期：西元 2025 年 4 月 27 日。



9.〈Anduril's Lattice: a trusted dual use — commercial and military — platform for public safety, security, and defense〉，《anduril》，<https://www.anduril.com/article/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security/>，檢索日期：西元 2025 年 4 月 27 日。

10. Luhao He, Yongzhang Zhou, Lei Liu, Yuqing Zhang, Jianhua Ma, “Application of the YOLOv11-seg algorithm for AI-based landslide detection and recognition” National Library of Medicine, <https://pmc.ncbi.nlm.nih.gov/articles/PMC11992019/#CR76,p22> 檢索日期：2025 年 5 月 20 日。

作者簡介

吳佳紋少校，陸軍官校正 78 期資訊系、通資電正規班 103 年班，曾任連長、教官、通信官、研究教官，現就讀於國防大學陸軍指揮參謀學院正規班。

王昱翔，指職軍官 92 年班、陸軍砲兵訓練指揮部野砲正規班 199 期、國防大學陸院指揮參謀學院 105 年班、國防大學戰爭學院 113 年班，曾任營長、砲訓部射擊組教官、軍備局研發參謀官、戰規司計畫官；現職為國防大學管理學院武獲組上校教官。