Regular Paper

Communications of the CCISA
Vol. 31 No. 2 May 2025

基於 AI 驅動之 HoneyDrone 系統於現代戰場與資安防禦中的應用

蔡尚恩[1*]、安明軒[2]
[12]長榮大學資訊工程學系
[1]sean@mail.cjcu.edu.tw、[2]111B16885@mailst.cjcu.edu.tw

摘要

隨著人工智慧 (Artificial Intelligence; AI) 與無人機 (Unmanned Aerial Vehicle; UAV) 技術的快速發展，國防與網絡安全領域正邁向智能化防禦的新時代。HoneyDrone 作為結合蜜罐技術 (Honeypot Technology) 與無人機欺騙防禦 (Deception-based UAV Defense) 的創新解決方案，具備自主學習與適應能力，能夠有效應對分佈式阻斷服務攻擊 (Distributed Denial-of-Service; DDoS)、GPS 欺騙攻擊 (GPS Spoofing) 及中繼攻擊 (Relay Attack) 等多種資安威脅。

本研究探討了 HoneyDrone 的核心技術架構，並評估其在國防應用中的優勢與挑戰。透過深度強化學習 (Deep Reinforcement Learning; DRL) 最佳化戰術決策，電腦視覺 (Computer Vision) 提升環境感知能力，及賽局理論 (Game Theory) 計算最優防禦策略，HoneyDrone 能夠根據敵方行為模式動態調整誘捕機制與防禦對策。此外，HoneyDrone 採用蜂群智能 (Swarm Intelligence) 技術，使多機協作架構能夠實現即時情報共享，提升整體作戰效能。

透過分析近期國際案例，包括俄烏戰爭中的無人機電子戰、美國關鍵基礎設施遭受的網絡攻擊，以及亞太地區的高級持續性威脅 (Advanced Persistent Threat; APT)，本研究驗證了 HoneyDrone 在現代戰場與資安領域的應用價值。隨著 AI 與 UAV 技術的不斷發展，HoneyDrone 不僅能提升國防自主防禦能力，還能為關鍵基礎設施的安全維護提供前瞻性解決方案。

關鍵詞：HoneyDrone、蜜罐技術、無人機安全、人工智慧、賽局理論

* 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol. 31 No. 2 May 2025

Deployment of the AI-Driven HoneyDroneSystem for Modern Battlefield and Cybersecurity Defense

Tsai, Shang-En[1*], Aun, Meng-Hing[2]
[12]Department of Computer Science and Information Engineering, Chang Jung Christian University,
[1]sean@mail.cjcu.edu.tw, [2]111B16885@mailst.cjcu.edu.tw

Abstract

With the rapid advancements in Artificial Intelligence (AI) and Unmanned Aerial Vehicle (UAV) technology, the fields of national defense and cybersecurity are entering a new era of intelligent defense mechanisms. HoneyDrone, an innovative integration of honeypot technology and deception-based UAV defense, possesses autonomous learning and adaptive capabilities, enabling effective countermeasures against cybersecurity threats such as Distributed Denial-of-Service (DDoS) attacks, GPS spoofing, and relay attacks.

This study examines the core technological framework of HoneyDrone and evaluates its advantages and challenges in defense applications. By leveraging Deep Reinforcement Learning (DRL) for tactical optimization, Computer Vision for enhanced environmental perception, and Game Theory for computing optimal defense strategies, HoneyDrone dynamically adjusts its deception mechanisms and countermeasures based on adversarial behavior patterns. Additionally, it employs Swarm Intelligence to facilitate multi-drone collaboration, enabling real-time intelligence sharing and improving overall operational efficiency.

Through an analysis of recent international cases—including UAV electronic warfare in the Russia-Ukraine conflict, cyberattacks on critical U.S. infrastructure, and Advanced Persistent Threats (APT) in the Asia-Pacific region—this research validates HoneyDrone's strategic value in modern warfare and cybersecurity. As AI and UAV technologies continue to evolve, HoneyDrone not only enhances autonomous defense capabilities but also offers a forward-looking solution for safeguarding critical infrastructure.

Keywords: HoneyDrone, Honeypot, UAV Security, Artificial Intelligence, Game Theory

壹、前言

隨著現代戰爭模式的演進與網路攻擊技術的持續精進，無人機 (Unmanned Aerial Vehicle, UAV) 於國防與資訊安全領域之應用已逐步邁向智慧化與自主化。HoneyDrone 作為一種結合蜜罐 (Honeypot) 技術與人工智慧 (Artificial Intelligence, AI) 之創新型無人載具系統，不僅能誘捕並追蹤網路攻擊行為，亦可於數位與實體空間同步執行監控、情報蒐集及防禦任務。此項技術的發展為強化國防作戰效能與資安防禦機制提供嶄新解方，並可能成為未來智慧防衛體系之關鍵方向。

傳統蜜罐技術主要應用於網路安全領域，其核心概念在於模擬真實系統環境，以誘引並引導攻擊者進行滲透行為，進而解析其攻擊模式，據以制定精準防禦策略。隨著人工智慧技術之進展，HoneyDrone 不僅具備智慧型蜜罐的欺敵與誘捕功能，並透過無人機之部署將應用場景拓展至戰場偵察、網路防護及敵情監控等任務，同時可結合深度強化學習 (Deep Reinforcement Learning, DRL) 以優化作戰決策，強化防禦體系之應變能力與適應性。

當前全球安全局勢趨於複雜，各國軍事機構積極發展無人機技術與智慧型防禦架構，以因應來自國家與非國家行為體之複合型威脅。近期俄烏戰爭中所展現之電子作戰 (Electronic Warfare, EW) 與網路攻擊情境，進一步突顯無人機於現代戰場中所扮演之關鍵角色。亞太地區亦持續面臨高階持續性滲透 (Advanced Persistent Threat, APT)、分散式阻斷服務攻擊 (Distributed Denial-of-Service, DDoS) 及供應鏈攻擊等重大資安挑戰。

在此背景下，HoneyDrone 可部署於戰略關鍵區域，如軍事設施、關鍵基礎建設及邊境安全防線，並藉由 AI 驅動之分析系統即時掌握敵方動態、計算最適防禦策略，並依據不同攻擊模式進行動態防禦調整。在資訊安全層面，HoneyDrone 能模擬軍用無人機之飛行軌跡與通訊行為，誘導敵方發動網路攻擊，進而蒐集攻擊樣態資料，優化整體資安防禦架構。此一結合人工智慧與欺敵防護之技術，不僅提升無人機之自主性與作戰效能，亦為當前與未來國防安全與資通安全領域帶來戰略性價值。

貳、HoneyDrone 的發展

蜜罐 (Honeypot) 系統及其延伸技術如 HoneyDrone，已逐漸成為國防與資訊安全領域中的關鍵組件。此類技術之演進，不僅有助於偵測與防禦分散式阻斷服務攻擊 (Distributed Denial-of-Service, DDoS)，亦可強化網路安全之主動防禦機制 [21]。透過結合無人機系統與欺敵防禦技術 (Deception Defense Technology)，HoneyDrone 提供一套新型資安架構，能於實體與數位空間中同步執行偵監與防禦任務，對於保護關鍵基礎設施之安全形成明顯戰略優勢 [2]。

2.1 蜜罐技術與 HoneyDrone 的發展

蜜罐技術 (Honeypot) 的概念可追溯至 1980 年代，美國研究員 Cliff Stoll 在一次網路入侵調查中首次實作此概念，並在後續文獻中加以闡述 [18]。蜜罐係指一種模擬真實系統環境之誘捕架構，其目的在於吸引惡意攻擊者進行滲透，藉此觀察其行為、蒐集相關威脅情報並分析攻擊模式。隨著網路攻擊技術的快速演進，蜜罐技術亦隨之發展出更進階之虛擬化、雲端化與自動化欺敵防禦機制。例如，開源工具 Honeyd 可模擬多種作業系統與網路服務，協助資安團隊有效識別入侵行為並強化整體防護體系 [21]。

在上述技術基礎上，HoneyDrone 應運而生，作為蜜罐系統與無人機技術 (Drone Technology) 融合之創新架構。HoneyDrone 不僅可於網路空間中誘捕網路入侵行為，更可擴展至實體空間，透過無人機進行地面監控與威脅來源追蹤。舉例而言，將 HoneyDrone 部署於關鍵基礎設施周邊，可有效誘引與偵測敵方駭客或網路攻擊行為，進而紀錄其攻擊模式，提升資安防禦之精準度與預警能力。HoneyDrone 配備人工智慧 (Artificial Intelligence, AI) 模組，可自主分析環境特徵、動態規劃飛行航徑，並與其他無人載具協同運作，為現代化國防建構提供更具彈性之應用模式。

2.2 台灣資安與國防挑戰

作為亞太地區的科技樞紐，臺灣長期面臨來自國家級與非國家級行為體的網路威脅，涵蓋高階持續性滲透 (Advanced Persistent Threat, APT)、分散式阻斷服務攻擊 (Distributed Denial-of-Service, DDoS) 以及供應鏈滲透等資安問題 [12]。尤其自 2020 年代起，數位轉型加速與物聯網 (Internet of Things, IoT) 裝置迅速普及，使得臺灣之關鍵基礎設施（如電力系統、交通網絡及金融體系）日益成為敵對勢力之攻擊焦點 [20]。

根據我國資安單位之公開報告顯示，每年偵測到之惡意攻擊企圖高達數十億次，當中不乏涉及國際駭客組織或由特定國家支持之滲透行動 [17]。此類威脅不僅對政府運作與企業營運構成重大干擾，更可能危及國家整體安全。因此，發展具備前瞻性與主動防禦能力之資安技術，已成為當前我國國防與資訊安全政策的優先重點。

HoneyDrone 作為結合人工智慧與欺敵誘捕的資安防禦技術，能提供高度自動化與動態反應之應變機制，有助於提升臺灣面對多元化網路威脅時之整體安全韌性與戰略應對能力。

2.3 近期全球相關事故

近年來多起重大網路安全事件突顯了蜜罐技術與 HoneyDrone 在戰略安全領域中的潛在價值，舉例如下：

一、俄烏戰爭中的網路作戰

俄羅斯針對烏克蘭發動大規模分散式阻斷服務攻擊 (DDoS) 與供應鏈滲透行動，並運用電子作戰技術 (Electronic Warfare) 干擾其通訊與指揮系統。此類攻擊模式顯示出網路作戰已成為現代戰爭中不可或缺的戰略工具。

二、美國能源基礎設施遭攻擊

2021 年 Colonial Pipeline 遭遇勒索軟體 (Ransomware) 攻擊事件，導致美國東岸大範圍燃油供應中斷，突顯關鍵基礎設施面對網路威脅時的高度脆弱性與迫切防護需求。

三、亞太地區之 APT 攻擊活動

中國駭客組織多次針對臺灣及周邊國家之政府機關與企業發動高階持續性滲透 (APT) 攻擊，試圖竊取敏感資料，並干擾關鍵基礎設施之正常營運。

上述案例顯示，在當前全球網路安全威脅日益嚴峻的情勢下，導入更具前瞻性之欺敵防禦技術（如人工智慧驅動的 HoneyDrone 系統），可望有效降低攻擊成功率，並顯著提升國家資安韌性。

在現代國防與資安體系中，蜜罐技術的應用已不再侷限於傳統靜態網路環境，而是透過與無人機科技的融合，形成一種涵蓋實體與虛擬空間的整合式安全解決方案。HoneyDrone 的技術特性不僅可有效彌補數位空間與實體空間間的安全落差，亦能藉由人工智慧與分散式協同運算技術，強化整體戰術靈活性與防禦效能。對於臺灣而言，面對愈發複雜多變的資安與國防挑戰，積極發展如 HoneyDrone 等新型態防禦架構，將是確保國家整體安全的核心戰略方向之一 [20]。

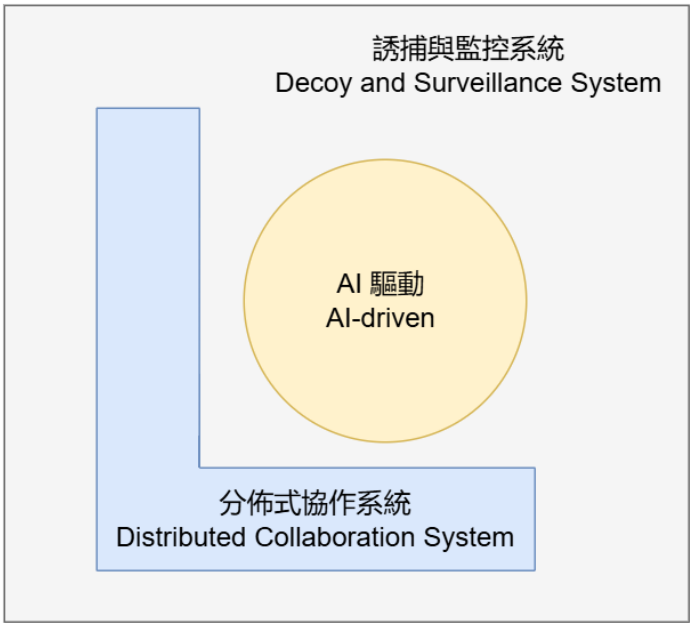
叁、技術原理與運作機制

HoneyDrone 為一種融合蜜罐技術 (Honeypot Technology) 與無人飛行載具 (Unmanned Aerial Vehicle, UAV) 技術之智慧型防禦系統，主要應用於國防與網路安全領域。其核心運作原理與傳統蜜罐架構相似，透過模擬軍用通訊系統與無人機行為模式，吸引敵方發動干擾與滲透攻擊，進而記錄其行動特徵，作為威脅分析與模式建構之依據 [8]。

3.1 HoneyDrone 的基本運作原理

相較於傳統靜態蜜罐系統易於被識破，HoneyDrone 結合高機動性與分散式協同機制，能於多變環境中進行動態部署，執行更精準之欺敵誘捕與戰術情報蒐集任務 [21]。

HoneyDrone 技術架構由三大核心模組所構成（見圖一）：



圖一：HoneyDrone 核心模組

一、誘捕與監控系統 (Deception and Surveillance System)
此模組模擬無人機在正常作戰條件下之運作行為，以主動吸引敵方發動干擾或攻擊，並即時記錄與監控其行動軌跡，利於後續威脅評估與攻擊情境重建。
二、AI 驅動之資料分析與決策引擎 (AI-driven Data Analysis and Decision Engine)
本模組負責對所蒐集之敵對行為資料進行分類建模，結合人工智慧訓練模型進行預測性分析，並依據不同攻擊樣態即時調整防禦參數，強化整體應變能力。
三、分散式協作系統 (Distributed Collaboration System)
此模組支援多架 HoneyDrone 間之實時協同作業，透過蜂群智慧 (Swarm Intelligence) 進行資源分配與戰術協調，提升作戰彈性與防禦整合效能 [7]。

3.2 AI 在無人機欺騙防禦中的應用

HoneyDrone 透過人工智慧 (Artificial Intelligence, AI) 技術之整合，大幅強化其自主學習與決策能力，使其能即時因應敵方攻擊行動，並擬定最佳防禦策略。AI 在 HoneyDrone 系統中之應用主要涵蓋三大核心技術領域：深度強化學習 (Deep Reinforcement Learning, DRL)、電腦視覺 (Computer Vision) 與威脅識別與預測 (Threat Detection and Prediction) [11]。

首先，HoneyDrone 採用如 Asynchronous Advantage Actor-Critic (A3C) 等深度強化學習演算法，透過持續互動學習以掌握敵方行動特徵，並依其行為動態調整誘捕策略。舉

例而言，當敵方對無人機通訊網絡發動 DDoS (Distributed Denial-of-Service) 攻擊時，HoneyDrone 可即時調整無線電通訊頻率與功率設定，以降低被敵方發現與干擾之風險 [21]。此外，AI 模型亦可根據歷史攻擊樣態進行趨勢預測與風險建模，使 HoneyDrone 在執行任務時得以適應多變且複雜的威脅環境 [2]。

其次，在電腦視覺與威脅識別應用方面，HoneyDrone 可搭載多光譜攝影機 (Multispectral Cameras) 與 AI 影像辨識技術 (AI-based Image Recognition)，以即時感知環境變化與偵測潛在敵對行動。系統能自動識別如 GPS 欺騙攻擊 (GPS Spoofing)、中繼攻擊 (Relay Attack)、及無人機蜂群攻擊 (Swarm Drone Attack) 等高風險事件，並透過 AI 驅動之影像分析模組進行攻擊類型判別與優先排序。人工智慧在網路防護上的應用，特別是在威脅預警與主動防禦上，展現出高度潛力與作戰效能 [19]。

AI 技術的導入不僅提升了 HoneyDrone 在複雜戰術環境下的任務執行能力，亦使其能於敵方電子戰 (Electronic Warfare, EW) 干擾條件下維持穩定運作與即時反應，強化其作為國防資安體系中前線防護節點的戰略價值 [12]。

3.3 HoneyDrone 與賽局理論在 DDoS 防禦中的應用

為有效應對分散式阻斷服務攻擊 (Distributed Denial-of-Service, DDoS)，HoneyDrone 結合賽局理論 (Game Theory) 與人工智慧技術，建構動態應變模型，藉以計算最適防禦策略，並自主調整其作戰模式，以降低攻擊所造成之實際損害 [11]。其中，Nash 均衡 (Nash Equilibrium) 與機率回應均衡模型 (Quantal Response Equilibrium, QRE) 可應用於預測攻擊者行為模式，協助 HoneyDrone 在多變攻擊場景中制定最佳應對機制 [5]。

在 Nash 均衡模型之應用上，HoneyDrone 可模擬敵方攻擊者之策略選擇歷程，預測其可能採取之行動，進而調整誘捕或反制策略。例如，面對 UDP Flooding 類型攻擊時，HoneyDrone 可運用 Nash 模型分析攻擊者行為邏輯，進而決定是否執行訊號跳頻 (Frequency Hopping) 或轉換誘捕通訊協定，藉此分散攻擊焦點與降低效能消耗 [11]。

進一步而言，透過 QRE 模型，HoneyDrone 可根據歷史攻擊資料與敵方應對傾向，進行策略調整，以最小化系統風險並提升誘捕準確率。舉例而言，當面臨高頻率且具變化性的 DDoS 攻擊時，QRE 模型可協助系統預判攻擊者是否可能改變手段，並主動部署應對措施，如分散式頻譜管理 (Distributed Spectrum Management) 或跳頻干擾技術 (Hopping Interference Techniques)，以維持網路通訊穩定性。

這類建構於賽局理論之 AI 防禦模型，使 HoneyDrone 即便處於敵情複雜且資源受限的戰術環境下，仍能保持高度運作效率與策略靈活性，有效提升國防安全體系之韌性與適應能力。隨著人工智慧、無人機與網路攻擊技術持續演進，HoneyDrone 將進一步優化其行為模型與應變邏輯，以因應未來日益升高之國家級資安威脅。

肆、HoneyDrone 在戰場與網絡防禦中的應用

4.1 應用 HoneyDrone 於戰場監控

HoneyDrone 憑藉其高度機動性與自主決策能力，在戰場監控任務中扮演關鍵角色。其應用範疇涵蓋邊境巡邏、戰場偵察、軍事基地防衛及戰略情報蒐集等多個層面。透過搭載高解析度光學與紅外線攝影模組，HoneyDrone 能全天候監測戰場環境，並即時辨識與分析戰術態勢，自動標記可疑活動區域。人工智慧演算法亦強化其自主導航與任務規劃能力，使其在面對複雜戰場場景時，展現更高之任務適應性與即時反應效率 [6]。

在高威脅作戰情境中，結合主動式防禦技術與機動型無人機平台，有助於提升無人載具於多域作戰環境中的生存能力與戰術彈性 [9]。例如，於潛在敵對行動熱區預先部署 HoneyDrone，可有效執行前線偵察與早期威脅感知，並透過 AI 演算法評估最佳戰術應對方案，使作戰單位得以即時調整部署與資源配置，提升任務成功率。

此外，HoneyDrone 所具備之分散式協作技術 (Swarm Intelligence)，可促成多架無人機間即時情報共享與協同任務執行，達成跨載具協同監控與區域聯防之效。此種蜂群式運作模式除能強化戰場感知範圍，亦有助於降低敵方對指揮通訊鏈之干擾風險，提升整體戰場穩定性與決策韌性。

4.2 AI 驅動的欺騙防禦降低國防網絡風險

隨隨著網路戰 (Cyber Warfare) 型態持續演進，人工智慧驅動的 HoneyDrone 系統已被視為降低國防網路風險的創新技術。透過深度學習 (Deep Learning) 與行為分析 (Behavioral Analysis) 演算法，HoneyDrone 不僅可模擬合法網路流量以主動吸引惡意攻擊者，亦能即時蒐集其攻擊手法與行為特徵，作為後續風險預測與對策調整之依據。

該系統結合機器學習 (Machine Learning) 與誘捕策略 (Deceptive Engagement Strategy)，在架構設計上強化無人機於軍事偵監任務中的威脅辨識精度與主動防禦效率 [20]。此種「誘捕即防禦」的作法，使 HoneyDrone 能在無需直接接觸敵方的情況下掌握潛在攻擊態勢，提升資訊優勢與應變時效。

進一步而言，HoneyDrone 可部署於軍事網路環境及關鍵基礎設施 (Critical Infrastructure) 周邊區域，並透過偽裝流量 (Decoy Traffic) 引導敵方駭客進入虛擬環境 (Cyber Deception Zone)，以有效分散與隔離高階持續性威脅 (Advanced Persistent Threat, APT) 或供應鏈攻擊 (Supply Chain Attacks) 之真實衝擊面。此種偽裝式架構亦具備高度彈性，適用於不同層級之國防通訊與資安設施。

HoneyDrone 亦可整合區塊鏈 (Blockchain) 技術，以建立防禦資料之分散式儲存機制，確保其完整性與可追溯性。區塊鏈特有之不可竄改性 (Immutability) 與時間戳記功能，將有助於強化攻擊紀錄之證據力，並提升整體國防網路防禦機制之透明度與韌性。

4.3 從俄烏戰爭看無人機與網絡戰的未來趨勢

俄烏戰爭突顯無人飛行載具 (Unmanned Aerial Vehicles, UAVs) 技術與網路戰 (Cyber Warfare) 深度融合之趨勢，尤其在電子作戰 (Electronic Warfare)、情報蒐集 (Intelligence Gathering) 與遠端打擊 (Remote Strike Capabilities) 等層面展現明顯戰略價值。烏克蘭武裝部隊廣泛運用商用無人機 (Commercial UAVs) 執行偵察與精確打擊任務，並整合人工智慧演算法以提升影像判讀與戰場資訊處理之準確度。

烏軍亦導入機器學習技術建構敵方行動模式模型，使指揮中心得以預測敵軍動態並即時調整作戰策略。其有效整合 AI 驅動技術於戰術決策流程中，不僅提升資訊處理效率，亦增強作戰單位之即時應變能力與戰場感知能力 [16]。

另一方面，俄羅斯則運用廣泛之電子干擾與網路攻擊技術，試圖癱瘓烏克蘭無人機之指揮鏈與衛星通訊系統。俄軍部署針對 UAV 系統的多重網路干擾措施，結合電子戰手段，意圖削弱烏軍於空中之情報優勢與作戰效率。此衝突案例清楚顯示，未來戰爭形態將愈加仰賴人工智慧無人機 (AI-Powered UAVs) 執行戰術調整，並透過自適應演算法 (Adaptive Algorithms) 進行快速決策與調度。

隨著 UAV 技術不斷演進，未來軍事衝突所面臨之無人機資安風險 (UAV Cybersecurity Threats) 亦日益嚴峻。其中，如何強化無人機系統之防駭能力 (Anti-Hacking)、抗電子干擾機制 (Anti-Electronic Warfare) 與惡意劫持防禦 (Anti-Hijacking Defense)，已成為下一世代國防技術發展之核心課題。

舉例而言，量子加密技術 (Quantum Encryption) 可用於強化 UAV 通訊安全性，有效抵禦中間人攻擊與通訊竄改；AI 驅動的入侵偵測系統 (AI-driven Intrusion Detection Systems, IDS) 則可於無人機運行中即時辨識異常流量與惡意行為，進一步提升系統整體防禦深度。此類技術整合與升級，預示著 AI 無人機將於未來資訊戰與混合戰爭中占據戰略核心地位。

伍、HoneyDrone 的優勢與挑戰

5.1 AI 結合 HoneyDrone 與傳統蜜罐技術的比較

相較於傳統靜態蜜罐技術 (Static Honeypot Systems)，HoneyDrone 在機動性、智慧決策能力與環境適應性等層面展現出顯著優勢。傳統蜜罐多依賴靜態伺服器或虛擬環境模擬真實系統，以誘導攻擊者進行滲透行為，其部署方式通常受限於固定網路空間，不僅缺乏空間靈活性，亦易遭敵方偵測與繞過，進而降低誘捕與蒐證效果。

相對地，HoneyDrone 結合無人機平台之高機動特性與人工智慧 (AI) 所支援之即時運算能力，具備可動態部署於實體空間之能力，並可搭配任務需求進行策略性誘捕作業。系統能透過主動威脅分析 (Proactive Threat Analysis)、行為模式識別 (Behavioral Pattern

Recognition) 與資料關聯分析技術 (Correlative Data Analysis)，提升攻擊溯源精度與即時防禦反應速度。

舉例而言，HoneyDrone 可依據攻擊者之歷史行為特徵自動調整誘捕策略與模擬行為，實現誘敵深入與資訊誘導效果。此種高適應性與高度欺敵效能，對於高風險戰術環境中的資訊優勢建構具有關鍵意義。進一步而言，AI 驅動之自主無人機系統可於無需人為操作下執行多樣化情境預測與防護決策，顯著提升國防系統之作戰效率與任務彈性。

整體而言，HoneyDrone 融合 AI 技術後已突破傳統蜜罐於空間部署與互動反應上的限制，使其在軍事與國安應用中展現更高之戰略價值與實戰應用潛力 [6]。

表一：傳統靜態蜜罐技術與 HoneyDrone (AI 驅動) 的比較

技術特性	**傳統靜態蜜罐技術**	**HoneyDrone (AI 驅動)**
運行環境	靜態網絡架構	動態機動環境
適應性	固定配置，較易被識破	AI 驅動動態調整，提高欺敵能力
威脅分析	依賴人工分析，反應較慢	AI 進行即時威脅識別與防禦
應用範圍	網絡資安領域	軍事防禦、戰場監控與資安防禦

透過 AI 驅動的 HoneyDrone 技術，無人機不僅能有效識別與攔截敵方攻擊，還能提高威脅預測與應對能力，使其在國防與資安領域具備高度應用潛力。

5.2 無人機欺騙防禦技術的潛在風險

雖然 HoneyDrone 在國防與資訊安全領域中展現出高度戰略潛力，然其技術應用仍面臨多重挑戰，涵蓋 AI 演算法之可靠性、無人機網路安全風險以及能源供應限制等層面。

首先，人工智慧演算法的可靠性為首要技術風險來源。由於 AI 模型仰賴大量訓練資料，其學習結果可能因資料偏誤 (Bias) 或樣本不均 (Class Imbalance) 而導致判斷失準。HoneyDrone 若無法正確區辨正常操作與惡意行為，將可能因誤報 (False Positives) 或漏報 (False Negatives) 而導致戰術誤判。特別是在敵對環境中，自主系統若因 AI 模型誤分類或遭遇對抗樣本 (Adversarial Examples) 而將中立目標誤判為威脅，或忽略實際攻擊行動，皆可能對任務成果造成災難性影響 [14]。

其次，無人機網路安全性問題亦不容輕忽。敵方可能透過逆向工程 (Reverse Engineering) 技術分析 HoneyDrone 之通訊協定、感測器輸出與 AI 模型邏輯，進而發

動對抗樣本攻擊，使 AI 系統於辨識階段產生錯誤分類。此外，訊號干擾 (Jamming) 與全球定位系統 (GPS) 欺騙攻擊 (GPS Spoofing) 亦為目前無人機部署於實戰環境中最常見之風險來源，可能癱瘓其導航與資料回傳功能。部分研究指出，可透過賽局理論 (Game-Theoretic Modeling) 對 GPS 欺騙情境進行風險建模與動態因應，有助於提升 HoneyDrone 在敵對環境中之穩定性與韌性 [4]。

因此，能源供應限制構成 HoneyDrone 技術擴展的核心瓶頸。現行多數無人機系統受限於鋰電池容量，續航時間有限，難以支援長時間偵察或監控任務。若無法導入無線充電、模組化電池更換或高能量密度電池技術，HoneyDrone 在高風險環境下將受限於作業時間與航程半徑，進而降低其戰術部署之靈活性與持久性。能源效率與續航力之提升，將是未來 HoneyDrone 技術落地部署前須優先解決之關鍵課題。

5.3 HoneyDrone 發展的趨勢

隨著無人機技術與人工智慧 (Artificial Intelligence, AI) 的加速融合，AI 驅動的無人載具已逐漸成為現代戰爭中具有決定性影響力的核心技術。透過強化無人機自主決策能力，此類系統能執行即時戰術調整 (Real-Time Tactical Adaptation)，顯著提升戰場適應性，並減少對人為遠端操作的依賴 [15]。進一步而言，蜂群智能作戰技術 (Swarm Intelligence Combat Systems) 賦予無人機群協同作戰的能力，使其可同步執行多點部署、動態威脅識別與情報共享，提升整體戰術靈活性與作戰效率。

為因應日益複雜的敵情態勢與 AI 化攻擊手法，未來的軍事戰略規劃應全面考量 AI 無人機之自主決策特性，並發展相應之偵測、反制與欺敵機制。從 HoneyDrone 現階段發展所面臨的技術瓶頸出發，AI 分析能力與威脅識別準確性亟待強化。透過深度學習 (Deep Learning) 與集成學習 (Ensemble Learning) 技術的導入，可有效提升 HoneyDrone 在惡意行為辨識與異常網路流量偵測上的精度，降低誤判與漏報的機率。結合蜜罐技術與決策演算法，可強化無人機在分散式攻擊情境下的應變效能，進一步提升整體資安防禦韌性 [13]。此外，運用對抗式機器學習 (Adversarial Machine Learning) 方法，能提升模型對於敵方操弄樣本的抵抗力，降低誤導風險，並強化 AI 模型在戰術環境下的穩健性與實用性。若能進一步整合強化學習 (Reinforcement Learning) 與行為建模 (Behavioral Modeling) 機制，HoneyDrone 便可依據即時情資與戰場變數進行自主調整，有效提升其欺敵效能與作戰決策準確性。

在系統架構方面，分散式協作與資安防護能力亦為未來發展之關鍵。可透過區塊鏈技術 (Blockchain Technology) 建立多架 HoneyDrone 間的安全通訊協議，確保任務資訊與資料交換具備不可竄改性與可追溯性，進而防堵敵方竄改、攔截或偽造通訊內容之可能。發展蜂群式協同演算法，亦能提升無人機在無中央節點環境下的資源分配效率與威脅感知靈敏度，建構出具備彈性與擴張性的去中心化戰術協同架構。

在能源供應層面，HoneyDrone 若要實現長時間部署與巡邏任務，仍需克服電池續航力之限制。未來可望透過開發無線電力傳輸技術 (Wireless Power Transfer, WPT)，使無人機能於任務期間主動補充能源，降低任務中斷風險。同時，若能結合太陽能模組 (Solar Power Modules) 作為備用能源來源，亦可有效降低對單一電池模組的依賴，強化無人機於戰術環境中之能源自主性與持續作戰能力。

陸、全球主要國家的無人機與欺騙防禦技術發展現況

當前，美國、中國及俄羅斯等主要軍事強權，皆積極推進無人機與人工智慧 (AI) 技術之整合，並深化欺敵防禦機制 (Deception Defense Mechanisms) 於電子戰與網路作戰領域中的佈局。各國戰略技術呈現不同發展重點，反映其國防科技政策與戰略文化的差異。

6.1 美國 (United States)

美國國防部 (Department of Defense, DoD) 近年來積極主導 AI 無人機技術的研發與戰術部署，持續投入大量資源於具備人工智慧驅動能力之無人飛行載具 (AI-Powered UAVs)，並以建構自主威脅辨識、即時任務調整與戰術決策功能為核心目標。此類系統透過感測器融合技術、深度學習演算法與分佈式指揮控制架構的整合，不僅強化其於高威脅環境中的任務適應能力，更有效提升整體部隊的戰場存活率與決策速度。AI 無人機平台也可依任務需求模擬不同作戰場景，靈活調整應對策略，展現出高度任務彈性與作戰效能。

在跨域作戰架構的整合方面，美軍推動的「聯合全域指揮與控制」(Joint All-Domain Command and Control, JADC2) 計畫，為當前國防作戰數位轉型的關鍵工程。該計畫致力於將無人機、AI、感測器網絡與雲端通訊平台相互整合，建構一套橫跨陸、海、空、太空與網路空間的即時資訊鏈結系統。JADC2 平台強調資料融合、人機協同與決策即時化，尤其在面對電子干擾、高強度衝突與多重威脅情境下，能有效強化無人機的資訊傳遞韌性與網路抗干擾能力，進一步支撐整體戰場感知與即時指揮控制。

在發展自主作戰無人機 (Autonomous Combat Drones) 領域方面，美國更以長遠戰略視角投入高智能作戰載具的研製。代表性機型如 XQ-58A「女武神」(XQ-58A Valkyrie) 由美國空軍研究實驗室 (Air Force Research Laboratory, AFRL) 所領導開發，定位為低成本、遠程飛行且具備匿蹤特性的戰術無人機。該機採用模組化設計，可依任務需求裝載電子欺敵系統、智慧型感測裝置與分佈式 AI 演算模組，並具備與傳統戰機協同作戰的「忠誠僚機」(Loyal Wingman) 功能。此類平台未來可望成為空優作戰之中樞節點，實現人機混合作戰的戰術升級。

6.2 中國 (China)

中國在無人機戰略技術發展上持續加速，尤以蜂群作戰 (Drone Swarming) 與自主編隊能力之研發為核心。近年來，中國大力投入發展具自適應性的無人機編隊系統，提升戰場滲透力與多點同步打擊的戰術效能。目前所部署之無人機型號涵蓋翼龍系列、彩虹系列、雙尾蠍 (Twin-tailed Scorpion)、利劍 (Li Jian)、FH-97 高速偵察機以及無偵系列 (WZ) 等，類型完整且多元，涵蓋戰術偵察、精準攻擊、電子干擾與匿蹤突穿等多重功能，顯示其空中無人戰力體系已具多域聯合作戰之實戰條件。

在通訊安全與抗干擾能力方面，中國針對蜂群作戰中對通信穩定性的高需求，積極導入量子亂數產生器 (Quantum Random Number Generator, QRNG) 及跳頻展頻技術 (Frequency-Hopping Spread Spectrum, FHSS)。這些技術的整合可有效降低蜂群無人機在高電磁干擾或電子戰環境中遭到敵方攔截、破解或通信阻斷的風險，進一步強化無人機集群之自主協同與任務資料同步的穩定性與保密性 [3]。

在面對高威脅空域作戰需求的情境下，中國也同步推進隱形攻擊型無人機的研製，特別是針對台灣及第一島鏈地區防空網密集性高的特性。「利劍」無人機即為一例，其結合雷達匿蹤構型與人工智慧導向戰術模組，設計上專注於突破敵方防空識別區並執行高風險精準打擊任務，展現出跨域滲透與低可偵測性技術的融合應用。

此外，中國亦發展具戰略用途之高空長時偵察 (HALE) 與高超音速無人機系統。FH-97 與無偵-7 (WZ-7) 具備長程滯空監控與電子作戰能力，作戰性能類似美國 RQ-4 全球鷹，廣泛應用於電子情報蒐集與區域戰場監控。更具突破性者為無偵-8 (WZ-8)，其據稱可達五馬赫以上，並採火箭助推與母機高空拋射模式發射，具備雷達匿蹤與極高速滲透能力。該型號被認為是中國對美軍印太地區空中優勢進行戰略抗衡的關鍵裝備，亦為未來高強度衝突中搶佔制空權的核心無人平台之一。

6.3 俄羅斯 (Russia)

俄羅斯在烏克蘭戰爭中積極運用電子戰 (Electronic Warfare, EW) 與資訊作戰技術，發展出多元且高效的反制無人機攻擊模式，展現其對抗 AI 無人機與無人作戰系統的作戰成熟度。其中，GPS 訊號干擾 (GPS Jamming) 與無線電訊號攔截 (Radio Signal Interception) 已成為俄軍擾亂烏克蘭無人機部隊的關鍵戰術。傳統無人機通訊鏈在面對高強度電子干擾與信號操控攻擊下，容易出現定位錯亂或失去控制，進一步凸顯建立具量子隨機特性的抗干擾通訊架構之必要性 [3]。俄軍目前部署之「Leer-3」與「Krasukha-4」系統，具備強大電子干擾能力，除可中斷衛星導航系統外，亦能釋放虛擬 GPS 訊號 (Spoofed GNSS Signals)，使敵方無人機誤判定位、偏離航線或自毀，大幅削弱敵方無人編隊之作戰準確性與協同能力。

同時，俄羅斯也加速推動 AI 無人機的軍事部署與應用。根據俄國防部長安德烈·貝

洛烏索夫 (Andrei Belousov) 公開聲明，俄軍已於烏克蘭東部、以及本土的別爾哥羅德與庫爾斯克地區實地部署具備人工智慧模組的自主無人機系統。這些無人機具備自主辨識與精準打擊能力，可在不依賴遠端人工操作下，自主完成目標識別與攻擊任務。俄方計劃至 2025 年底擴編無人機總量至 140 萬架，顯示其以大規模智能無人系統建構新世代作戰樣態的戰略野心。

此外，俄方亦發展地面型反無人機載具以加強其多層次防禦能力。由俄羅斯國防企業 Rebovets 研製的「瓦力」 (Wall-E) 地面自走平台，即為典型代表。該系統搭載名為「Fumigator」 的戰術電子戰模組，能在 250 至 300 公尺範圍內釋放高強度干擾訊號，形構「電子圓頂」屏障，有效阻斷敵方無人機與其遠端操控者間的通訊鏈。此舉不僅可導致敵方無人機因失控而迫降或返回基地，亦對無人機蜂群構成戰術干擾，顯示俄方正積極發展跨領域、系統化的反無人機作戰體系。

柒、結論與建議

HoneyDrone 技術在當前軍事作戰與網絡防禦領域中已成為關鍵性創新。其結合高機動性、人工智慧 (Artificial Intelligence, AI) 驅動之智慧決策模組與進階欺敵防禦機制，不僅展現卓越的戰術靈活性，也在資安應變與即時威脅處理層面展現高度潛力。隨著 AI 技術的不斷成熟，HoneyDrone 已可支援即時情報蒐集、威脅辨識與行動調度，進一步提升國軍在複雜與高壓環境下的作戰持續力與決策效率 [19]。其結合實體偵察與網路誘捕的多模態作戰能力，使之成為聯結物理空間與數位空間之關鍵防禦節點，有效建構具韌性、具預警性之國防科技體系。

鑒於當前國際間網絡安全挑戰與地緣政治張力持續升溫，國際合作與技術標準的協同建構愈發重要。各國應積極參與國際性網絡安全聯盟及標準制定組織，如 ISO/IEC、NATO CCDCOE 等，協力推動針對 AI 無人機與欺敵技術之跨域作業指引與安全標準。此舉可確保相關技術具備可擴展性、跨平台互通性，並共同強化全球資安治理體系之韌性 [1]。

就台灣而言，面對高階持續性威脅 (APT)、分散式阻斷服務攻擊 (DDoS) 及複合型滲透行動等資安壓力，HoneyDrone 的導入與本土化發展將具高度戰略意涵。針對現階段挑戰與機會，建議可從以下四個面向強化技術應用與政策規劃。

首先，應於關鍵戰略區域部署 AI 無人機以執行前線監控。透過在海岸防線、邊境哨所與軍事基地周邊建置 HoneyDrone 系統，並整合雷達、光學影像、多源感測與通訊數據，可建立即時監控與戰術預警機制，強化對敵方無人機活動及可疑行動之辨識效能 [10]。

其次，建議強化本土自主型欺敵防禦技術之研發能力。透過跨部會整合資安技術與 AI 行為建模能力，推動具適應性與高敏感度之蜜罐誘捕系統，將有助於即時偵測高階威脅來源，並強化對 APT 與複合型網攻行為的識別與回應效能，降低通訊中斷或基礎設

施癱瘓之風險。

第三，可推動 HoneyDrone 技術朝向蜂群智能架構與分佈式協同作戰方向發展。透過人工智慧模型自動調度任務分配，使多架無人機能進行同步偵查、即時資料融合與行動決策，有效提升戰場感知與防禦能力，實現戰術層級之自主協作運作。

最後，應積極投入新一代能源供應技術的整合與研發。面對現行無人機續航力不足之限制，可優先發展無線能量傳輸 (Wireless Power Transfer)、氫燃料電池及高效率太陽能模組等替代方案，以強化 HoneyDrone 系統於長時間巡邏與高密度任務執行中的持續性與部署靈活性。

參考文獻

[1] A. Adeyeri, H. Abroshan, “Geopolitical ramifications of cybersecurity threats: State responses and international cooperations in the digital warfare era,” *Information*, 15(11), Article 682, 2024.

[2] P. P. Datta, “Cyber security issues and blockchain-deep learning based solutions for UAV and internet of drones (FANETs),” *arXiv preprint*, arXiv:2404.16848, 2024.

[3] J. de Curtò, I. de Zarzà, J. C. Cano, C. T. Calafate, “Enhancing communication security in drones using QRNG in frequency hopping spread spectrum,” *Future Internet*, 16(11), Article 412, 2024.

[4] A. Eldosouky, A. Ferdowsi, W. Saad, “Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing,” *IEEE Internet of Things Journal*, 7(4), 2840–2854, 2019.

[5] M. Iqbal, S. Suhail, R. Matulevicius, “DECEPTWIN:Proactive security approach for IoV by leveraging deception-based digital twins and blockchain,” *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–11, 2024.

[6] A. Joshi, A. Spilbergs, E. Miķelsone, “AI-enabled drone autonomous navigation and decision making for defence security,” *Environment Technology Resources, Proceedings of the International Scientific and Practical Conference*, 4, 138–143, 2024.

[7] Y. Li, C. Pu, “Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack,” *2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE),* 92–97, 2020.

[8] B. Lutkevich, “How to build a honeypot to increase cybersecurity,” *TechTarget.* Retrieved on April 12, 2025, URL: https://www.techtarget.com/whatis/feature/How-to-build-a-honeypot-to-increase-network-security.

[9] C. Lyu, R. Zhan, “Global analysis of active defense technologies for unmanned aerial vehicle,” *IEEE Aerospace and Electronic Systems Magazine*, 37(1), 6–31, 2022.

[10] D. W. Majors, R. P. O'Neil, "Integration of radar sensor data with situational awareness tools to respond to an unmanned aerial threat Doctoral dissertation," *Naval Postgraduate School*, Monterey, *CA,* 2021.

[11] A. Mairaj, A. Y. Javaid, "Game theoretic solution for an unmanned aerial vehicle network host under DDoS attack. *Computer Networks*," 211, Article 108962, 2022.

[12] Y. Mekdad, A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lazzeretti, A. S. Uluagac, "A survey on security and privacy issues of UAVs," *Computer Networks*, 224, Article 109626, 2023.

[13] M. A. O. Rabah, H. Drid, Y. Medjadba, M. Rahouti, "Detection and mitigation of distributed denial of service attacks using ensemble learning and honeypots in a novel SDN-UAV network architecture," *IEEE Access*, 12(99):128929-128940, 2024.

[14] P. Radanliev, O. Santos, "Adversarial attacks can deceive AIsystems, leading to misclassification or incorrect decisions," *Computer Science and Mathematics,* 2023.

[15] M. Radovanovic, A. Petrovski, A. Behlic, M. Z. Chaari, E. G. Hashimov, R. Fellner, A. Agbeyangi, "Unleashing autonomous forces: Integrating AI-driven drones in modern military strategy," *Системи управління, навігації та зв'язку. Збірник наукових праць,* 3(77), 55–69, 2024.

[16] J. M. Rickli, F. Mantellassi, "The war in Ukraine: Reality check for emerging technologies and the future of warfare," *Geneva: Geneva Centre for Security Policy*, 2024.

[17] N. A. Sabuwala, R. D. Daruwala, "Drones: Architecture, vulnerabilities, attacks and countermeasures," *International Conference on Intelligent Vision and Computing*, *Cham: Springer Nature Switzerland*, 220–232, 2022.

[18] C. Stoll, "The cuckoo's egg:Tracking a spy through the maze of computer espionage," *New York: Simon and Schuster*, 2024.

[19] F. Tlili, S. Ayed, L. C. Fourati, "Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions," *Internet of Things*, 27, 10128, 2024.

[20] Z. Wan, J. H. Cho, M. Zhu, A. Anwar, C. Kamhoua, M. Singh, "Optimizing effectiveness and defense of drone surveillance missions via honey drones," *ACM Transactions on Internet Technology*, 24(4), 1–26, 2024.

[21] Y. Wang, Z. Su, A. Benslimane, Q. Xu, M. Dai, R. Li, "Collaborative honeypot defense in UAV networks: A learning-based game approach," *IEEE Transactions on Information Forensics and Security*, 19, 1963–1978, 2023.