從美伊衝突解讀 AI 驅動的現代超限戰，以及對台灣智慧解決方案產業的戰略啟示

前言：當政策禁令趕不上戰場演算法

2026 年初爆發的美伊武裝衝突，留下了這個時代最具象徵性的矛盾畫面：川普政府一方面頒布行政命令，全面禁止聯邦機構使用 Anthropic 的 Claude 模型；另一方面，美軍中央司令部（CENTCOM）卻在同一時間窗口內，持續倚賴 Claude 執行伊朗目標識別與戰場模擬任務。

這個「政策禁令 vs. 戰場剛需」的矛盾，精準地揭示了一個新時代的到來：**AI 已從後勤支援工具，正式躍升為第一線戰術決策引擎。**對於 TSSA 的軟體開發商、硬體製造商與系統整合商而言，這不只是一則遠方的軍事新聞，而是直接影響商業策略、產品設計與市場定位的結構性訊號。

一、上帝之腦與上帝之眼：感知與決策的極速融合

大型語言模型進駐作戰指揮中心

在此次衝突中，最令業界震撼的技術披露，是 Palantir Maven 平台整合 Claude 語言模型作為情報分析核心的實戰部署。這套系統的運作邏輯，與企業級大數據分析（Big Data Analytics）極為相似，但輸出的不是商業洞察，而是**即時的致命火力決策。**

具體運作流程如下：系統同步接收三類原始數據 — 波斯語通訊攔截訊號、衛星光學影像，以及分布在廣域戰場上的邊緣感測器數據。這些數據流經 Palantir AIP / Claude 核心進行多維融合後，針對高價值目標輸出精準的殺傷鏈打擊方案。傳統情報流程需要數百名分析官耗費數月才能完成的研判工作，AI 系統僅需 6 秒。

對照商業應用的視角，TSSA 會員不難發現：這正是工業物聯網（IIoT）感測器融合、邊緣運算與自然語言介面的深度軍事化應用。那些在智慧工廠、智慧城市中每天優化生產效率的核心技術，在戰場上已化身為毫秒間的生死判官。

低軌衛星（LEO）：從商業頻寬到戰場骨幹

SpaceX 的軍用級 Starshield 系統，在此次衝突中扮演了「上帝之眼」的角色。透過衛星節點之間的光學雷射通訊，Starshield 提供了幾乎無法被傳統電子干擾癱瘓的即時戰場 3D 建模與指揮通訊能力。

這對台灣的啟示是雙重的。其一，台灣現有高度集中於海底電纜的國際通訊架構，在衝突發生時存在致命的單點失效風險；其二，低軌衛星通訊技術的軍民兩用潛力，為台灣的電信與航太產業提供了明確的技術升級路徑。

二、JADC2 與任務網路即服務：戰場的雲端化轉型

美軍在此次衝突中全面驗證了 JADC2（聯合全領域指揮與控制）架構的實戰效能。JADC2 的核心理念，是打破陸、海、空、太空、網路等各軍種之間的數據孤島，將所有感測器與射手整合進一個統一的 AI 驅動網路。

支撐這一架構的基礎建設，是斥資 90 億美元打造的 JWCC（聯合作戰雲端合約）基礎設施。這個以嚴格零信任（Zero-Trust）資安架構為基礎的全球可存取雲端平台，以「任務網路即服務（Mission Network-as-a-Service）」的模式運作。

對 TSSA 中的雲端服務商與系統整合商而言，這個架構等同於極端環境下的 **5G/6G 超低延遲物聯網與邊緣運算骨幹。**能夠在斷網、強干擾、高威脅環境下仍維持服務韌性的系統設計能力，將成為進入全球國防工業基地（DIB）供應鏈的核心門票。

三、OODA 循環的崩潰：人類被排在決策迴圈之外

理解此次衝突的最重要概念框架，是 OODA 循環（觀察-定向-決策-行動）的三階段演化。**OODA 循環**（OODA loop）代表**觀察（Observe）、判斷（Orient）、決策（Decide）與行動（Act）**，這是一個用來思考與分析在戰區中如何進行決策的框架。

在現代軍事與人工智慧科技的發展下，OODA 循環有以下幾個關鍵的轉變：

- **決策時間極度壓縮**：在被稱為「超高超戰（Hyperwar）」的未來衝突型態中，人類的決策幾乎完全從 OODA 循環中被移除，這導致執行一次 OODA 循環的時間被壓縮到**近乎即時的反應。**
- **從人類循環轉向數位循環**：傳統由人類執行的 OODA 循環較為脆弱，而數位循環則快速且靈活。現代科技顛覆了傳統單一的決策結構，將 OODA 循環擴展為具備韌性、可擴展且適應性強的「擊殺網（kill webs）」，讓自動化系統能以比人類對手更快的速度選擇、鎖定並打擊敵軍。
- **作為區分武器自主等級的標準**：OODA 循環也常被用來協助區分武器系統的自主化程度。例如：
- **Phase 1 — 迴圈內（In the Loop）**：AI 標記目標，人類確認後才能開火。這是 Project Maven 初期的半自主模式。
- **Phase 2 — 迴圈上（On the Loop）**：機器自行判斷開火，人類僅保留否決權。如方陣快砲（CIWS）防空系統。
- **Phase 3 — 迴圈外（Out of the Loop）**：AI 群飛無人機獨立完成「發現、定位、決策、摧毀」全程，**完全排除人類干預。**

以色列的「薰衣草（Lavender）」AI 系統在此次衝突相關的城市戰中，曾於短短 20 秒內確認並標記了 37,000 個潛在打擊對象。當戰場節奏已快過人類的神經反應速度，人類的介入反而成為作戰效能的「瓶頸」。這意味著，**時間本身已成為一種武器。**

四、終端打擊力：YOLO 演算法與無人機蜂群的戰場革命

此次衝突中，自主無人機的大規模部署，是最直接衝擊台灣產業界視野的戰術現實。

搭載 YOLO（You Only Look Once）電腦視覺演算法的小型四軸無人機與遊蕩彈藥，即便在完全無 GPS 訊號、遭受嚴重電磁干擾的環境下，仍能獨立辨識並分類地面目標，精準區分民用車輛與輕型裝甲車。

更具顛覆性的是蜂群（Swarm）邏輯的實戰驗證。LOCUST 等去中心化蜂群系統，能協調數十至數百架低成本無人機，以飽和攻擊癱瘓傳統防空系統的攔截能力。這正是自動駕駛汽車的感知融合技術，以及智慧城市車牌辨識系統的武器化應用。

對 TSSA 的硬體廠商而言，這意味著：邊緣 AI 晶片（Edge AI Chip）、微型慣性導航模組、低功耗感測器融合處理器，正在成為全球國防供應鏈最渴求的稀缺零組件。

五、網路與實體的界線消失：午夜之錘行動的戰略意義

在動能打擊（實體炸彈）發動之前，美國網路司令部先行執行了代號「午夜之錘（Operation Midnight Hammer）」的上游癱瘓作戰。這次行動的目標，不是伊朗的核設施本身，而是其防空系統所依賴的**網路拓撲關鍵節點**——路由器與伺服器。

透過入侵這些節點並注入惡意代碼，美軍在不發一彈的情況下，數位化地使伊朗防空雷達陷入盲目，讓隨後進入領空的隱身戰機面對的不是飛彈，而是沉默。網路武器從此不再是「點綴」，而是**與動能打擊等量齊觀的決定性戰力。**

對 TSSA 電信與網路安全業者的警示是深刻的：海底電纜遭切斷、數據中心遭實體打擊、路由器遭植入後門，這三種攻擊向量在此次衝突中全部出現。集中式基礎設施不再是效率優勢，而是**戰略弱點。**

六、演算法的陰暗面：幻覺、數據中毒與黑箱風險

平衡的分析必須指出，AI 軍事化的過程並非沒有代價與危機。

AI 幻覺（Hallucinations） 問題在戰場上已造成真實傷害：系統曾將步槍誤判為直升機，缺乏人類常識的演算法無法辨識刻意的戰術偽裝。深度學習的「黑箱」特性，使得指揮官在戰後無法解釋 AI 為何選擇特定目標，戰爭責任歸咎因此陷入法律真空。

更深層的戰略風險，來自 AI 對穩定性的侵蝕。當 AI 驅動的精準情報使任何機動核資產都無所遁形，「相互保證毀滅（MAD）」的威懾邏輯開始動搖。壓縮至毫秒級的決策窗口，可能讓系統因錯誤的雷達雜訊而自動觸發核武反擊。這些，是 AI 優先戰略帶給人類文明的存在性風險。

七、對台灣智慧解決方案產業的三大戰略機遇

機遇一：從「企業級」到「國防級」資安標準的全面升級

敵手早已不區分政府與企業目標。TSSA 會員的商業產品若想進入全球防務供應鏈，必須將以下能力內建為產品設計的基礎架構：

- **元數據屏蔽**（Metadata Shielding）：傳統端到端加密已不足夠。未加密的元數據（通訊對象、時間戳、地理位置）是敵方重建組織圖譜的主要漏洞。
- **零信任架構**（Zero-Trust Architecture）：隨著 AI 深偽（Deepfake）技術的普及，持續驗證身份已成為所有重大政府與國防合約的基本要求。
- **密碼敏捷性**（Cryptographic Agility）：「現在竊取、未來解密（Harvest Now, Decrypt Later）」的後量子威脅，要求系統設計必須具備快速切換加密演算法的能力。

機遇二：國防工業基地（DIB）供應鏈的台灣機會

台灣作為全球高階晶片、伺服器與網通設備的製造核心，已不可避免地處於全球 AI 軍備競賽的戰略中心。西方盟國軍方正積極尋求可信賴的軍民兩用（dual-use）技術合作夥伴，以下領域的需求最為迫切：

- **安全微電子與邊緣 AI 晶片**：JADC2 架構對能在極端環境下運行的低功耗、高效能推理晶片需求龐大。
- **無人系統零組件**：自主蜂群所需的感測器融合模組、邊緣運算處理器與抗干擾通訊模組。
- **去中心化通訊基礎設施**：光學雷射通訊、衛星地面終端設備與分散式網狀網路（Mesh Network）解決方案。

機遇三：「斷網續存」能力的系統設計革命

Starshield 的實戰驗證，以及台灣自身的海底電纜斷纜風險，共同指向同一個技術命題：**智慧解決方案必須具備「斷網續存**（Graceful Degradation）**」能力**，在主幹網路中斷時，仍能透過邊緣運算維持核心功能的自主運作。

這個設計哲學的改變，將深刻影響從工業控制系統、醫療設備到金融交易平台的所有產品架構。

結語：在超限戰的時代，運算力即是威懾力

美伊衝突最終留給世界的，不僅是一場地區性的軍事衝突，而是一次 **AI 驅動的現代戰爭的全**

球公開課。它清晰地告訴我們：未來的戰場是軟體定義、演算法驅動、高度自主的；而科技公司，正在成為一種新型態的戰略資產與武器供應商。

對於 TSSA 的會員而言，這場衝突揭示的機遇與責任同樣深重。台灣的智慧解決方案與硬體製造實力，不僅是商業利益的來源，更是維繫全球民主陣營戰略穩定的關鍵基礎設施。

在演算法即戰力的時代，**掌握演算法、確保數據韌性、主導硬體供應鏈——這是台灣在全球 AI 賽局中，最強大的戰略話語權。**

而人類的最終挑戰，不是製造更聰明的武器，而是在擁抱 AI 前沿技術的同時，堅守讓人類永遠保有最終裁決權的道德底線。

本文基於公開情報資料及相關研究報告撰寫，供台灣智慧解決方案協會（TSSA）會員參考。文中引用之具體作戰數據均來自開源情報（OSINT）分析，不代表官方軍事立場。

- TSSA_智慧部落格_AI 如何改變現代戰爭

本文由台灣智慧解決方案協會（TSSA）智慧部落格編輯部整理撰寫，僅供會員參考，不代表任何政治立場。

發布日期：2026 年 2 月 19 日