

# 國防安全雙週報

## 第 108 期

- |                                  |     |    |
|----------------------------------|-----|----|
| 美國「史詩怒火行動」對台海安全的啟示與影響            | 鍾志東 | 1  |
| 「各司其職」：史詩怒火行動中的 AI Agents 作戰分工模式 | 黃政勛 | 11 |
| 軍事作戰模式模擬：人工智慧時代的轉型與挑戰            | 林超倫 | 19 |
| 川普 2.0 網路戰略下的安全意涵與未來發展趨勢         | 曾敏禎 | 27 |
| 中共黨報宣傳將領落馬的要點與觀察                 | 梁書瑗 | 35 |
| 歐盟造船戰略下低排放與數位變生的結合               | 賀增原 | 43 |

臺北市博愛路 172 號  
電話 (02) 2331-2360  
傳真 (02) 2331-2361

2026 年 3 月 23 日發行



財團法人國防安全研究院  
Institute for National Defense and Security Research

# Contents

<b>The Impact and Implications of the U.S. “Operation Epic Fury” on Taiwan Strait Security</b> <i>William Chih-Tung Chung</i> .....	<b>1</b>
<b>“Division of Roles”: Task Allocation among AI Agents in Operation Epic Fury</b> <i>Cheng-Hsun Huang</i> .....	<b>11</b>
<b>Military Operation Modeling Simulation: Transformation and Challenges in the Era of Artificial Intelligence</b> <i>Chau-Luen Lin</i> .....	<b>19</b>
<b>Security Implications and Future Development Trends under Trump 2.0 Cyber Strategy</b> <i>Min-Chen Tseng</i> .....	<b>27</b>
<b>The Propaganda Model of the Leading Party Newspapers in the Corruption Scandals of the PLA</b> <i>Shu-Yuan Liang</i> .....	<b>35</b>
<b>Integration of Low Emissions and Digital Twins under the EU Shipbuilding Strategy</b> <i>Tzeng-Yuan Heh</i> .....	<b>43</b>

# 美國「史詩怒火行動」對台海安全的影響 與啟示

鍾志東

國防戰略與資源研究所

焦點類別：國防戰略、國際情勢、台海情勢

## 壹、前言

美國總統川普（Donald Trump）以伊朗威脅美國國家安全為由，於 2026 年 2 月 28 日聯合以色列採取「史詩怒火行動」（Operation Epic Fury）對伊朗進行大規模軍事攻擊，伊朗最高領袖哈米尼（Ayatollah Ali Khamenei）及多名軍政高層領袖在首波精準「斬首」攻擊中喪生，此為動盪許久中東區域安全投下關鍵新變數。

相較於 2025 年 6 月 22 日美國針對伊朗核武設施攻擊的「午夜之錘行動」（Operation Midnight Hammer），「史詩怒火行動」作戰規模與目標，已不僅僅侷限於摧毀核武設施，而是企圖癱瘓甚至一勞永逸地推翻反美伊朗神權政府，進而建立川普所認可的友美新政府。川普多次呼籲伊朗人民藉機起義推翻伊朗政府，並在 2026 年 3 月 6 日宣稱，他只接受伊朗「無條件投降」，而投降定義由他決定；對此，伊朗總統裴澤斯基安（Masoud Pezeshkian）反擊稱，川普要求伊朗無條件投降，那是「癡人說夢話」。<sup>1</sup>

隨著美伊戰爭逐步升級，其對全球影響亦隨之擴大，除了衝擊國際能源市場之外，更涉及地緣政治的大國競爭。基於美國在台海

---

<sup>1</sup> 〈美國用兵伊朗目標又改 川普要對方無條件投降〉，《中央社》，2026 年 3 月 6 日，<https://www.cna.com.tw/news/aopl/202603070046.aspx>；〈川普拒談判 伊朗總統：要無條件投降是癡人說夢話〉，《中央社》，2026 年 3 月 7 日，<https://www.cna.com.tw/news/aopl/202603080088.aspx>。

安全的關鍵角色，美伊戰爭不論是涉及美中大國競爭關係、還是此現代化戰爭所提供經驗，都將對台海安全將產生深遠影響。

## 貳、安全意涵

### 一、川普主義展現積極運用軍事手段特色

川普 2.0 上任一年來，在過去短短不到兩個月內，接連對委內瑞拉與伊朗發動軍事攻擊，並劍指宿敵古巴進行公開軍事脅迫，展現川普大膽運用軍事手段追求政治目標的強勢風格。自從 1979 年伊朗伊斯蘭革命成功後，伊朗神權政府視美國為「撒旦」與「伊斯蘭敵人」，後因伊朗綁架美國外交官人質事件，美國於 1980 年 4 月宣布與伊朗斷交以來，美伊衝突不斷並陷入長期軍事對峙緊張關係。對此，伊朗積極發展核武反制美國與以色列威脅，但華府對使用軍事手段解決伊朗核武問題始終持高度謹慎態度，希望透過經濟制裁與外交談判解決。

不過川普總統明顯有著不同看法。2017 年川普上任不久，立即宣布退出已達成的《伊朗核協議》，其強硬立場導致美國與其歐洲盟友關係緊張，此也預告他將採取軍事手段解決延宕多時的伊朗核武問題。美國駐聯合大使華爾滋（Mike Waltz）正當化川普軍事行動稱，美伊戰爭早就開始於 1979 年，因此川普只是要終結伊朗長期以來的對美國攻擊。<sup>2</sup>

川普積極使用軍事力量，對中國武力犯台會產生一定的嚇阻效果。儘管川普始終不願就軍事協防台灣表態，不過他不畏懼以軍事手段打破政治僵局的伊朗經驗，讓北京當局決定片面使用武力解決

---

<sup>2</sup> Alexander Hall, "Waltz Shuts down NBC Anchor, Arguing Trump is Ending a War Iran Started with the US in 1979," *Fox News*, March 9, 2026, <https://www.foxnews.com/media/waltz-shuts-down-nbc-anchor-arguing-trump-ending-war-iran-started-us-1979>.

台灣問題上，不得不嚴肅面對美國軍事介入台海可能性大幅提高的挑戰。事實上，川普過去即曾軍事恫嚇中國不要在台海安全生事。根據美國《有線電視新聞網》(CNN)報導，川普 2024 年於選舉募款活動告訴支持者，他曾警告習近平，若中國入侵台灣，美國將以轟炸北京作為回應。川普談到習近平時說，「他覺得我瘋了。」隨後補充說，「但我們從沒出過問題。」<sup>3</sup>

川普斷然以軍事手段解決糾結以久美伊衝突，顯示川普不是光說不練的人，北京當局應會更認真面對川普的軍事警告。美國《2025 國家安全戰略》強調「以實力維持和平」，同時明確指出台灣在全球產業供應鏈與地緣戰略上攸關美國國家利益，川普在伊朗問題上展現捍衛美國利益的強硬立場，無疑也增加他以武力維持台海現況決心的可信度。

## 二、川普運用「有限戰爭」成為介入台海典範

美國「史詩怒火行動」顯示，川普大膽運用軍事手段同時，積極避免戰事擴大與延長。此也反映於川普在此次軍事行動上，目前仍侷限於海空軍與飛彈運用，對派遣地面部隊雖不排除但始終持保留審慎態度，同時暫時迴避全面攻擊伊朗經濟命脈的煉油基礎設施。戰爭部長赫格塞斯 (Pete Hegseth) 2026 年 3 月 2 日記者會上表示，「那些叫囂『無止境戰爭』的媒體和左派人士，閉嘴！這不是伊拉克戰爭，也不會是無休止戰爭。」<sup>4</sup>

川普對伊朗戰爭目標設定，不斷有新說法，在於維持其戰略彈性，同時反映他企圖將戰爭置於可管控範圍。2026 年 3 月 2 日川普

---

<sup>3</sup> Adam Cancryn, "Trump Said He Threatened to Bomb Moscow if Putin Attacked Ukraine, 2024 Fundraiser Tapes Show," *CNN*, July 8, 2025, <https://edition.cnn.com/2025/07/08/politics/trump-tape-putin-bomb-fundraiser>.

<sup>4</sup> 〈五角大廈：美國不會陷入新的無休止戰爭〉，《中央社》，2026 年 3 月 3 日，<https://www.cna.com.tw/news/aopl/202603030023.aspx>。

在白宮表示，此次對伊朗軍事行動的 4 大目標，第一，摧毀伊朗的飛彈能力；第二，殲滅伊朗海軍；第三，確保「這個全球頭號恐怖主義贊助國」永遠無法取得核武；最後，確保伊朗政權無法繼續在其境外武裝、資助並指揮恐怖主義武裝組織。<sup>5</sup>川普於 2026 年 3 月 10 日記者會宣稱，軍事行動非常成功，美伊戰爭將「很快結束」。<sup>6</sup>儘管川普曾要求伊朗「無條件投降」，但此應可視為川普極限施壓伊朗以儘快結束戰爭的談判策略。

川普此次主要透過海空軍運用，決定性地集中打擊軍事目標，企圖在最短時間內摧毀伊朗戰爭機器作戰能力，進而獲取有利談判地位以達成政治目標，是典型「有限戰爭」(limited war) 運用。此種有限度的軍事介入方式，也極有可能成為美軍反制解放軍攻台的模式。

如果美中在台海軍事衝突無可避免，美國《2026 國防戰略》(2026 National Defense Strategy, 2026 NDS)「拒止防衛」(denial defense) 沒有明說的另一戰略目標，就是避免與中國全面開戰，以防止兩大核武強權陷入毀滅性對決。<sup>7</sup>根據美國戰爭部主管政策事務的次長柯伯吉 (Elbridge Colby)，其「拒止戰略」是以防禦為主的區域軍事力量運用，戰略目標在於阻止對手使用軍事力量達成決定性政治成果，而非追求全面碾壓式勝利。<sup>8</sup>因此，「拒止防衛」其實就是避免「全面戰爭」(total war) 的「有限戰爭」運用，在有限的戰

---

<sup>5</sup> 侯姿瑩，〈川普：攻打伊朗有 4 大目標 美軍有能力打超過 4 週〉，《中央社》，2026 年 3 月 3 日，<https://www.cna.com.tw/news/aopl/202603030009.aspx>。

<sup>6</sup> 〈特朗普稱美以伊戰爭「很快結束」，油價稍回落〉，《BBC 中文網》，2026 年 3 月 10 日，<https://reurl.cc/ep8Y2W>。

<sup>7</sup> 鍾志東，〈《鍾志東觀點》美國《2026 國防戰略》看破不說破的台灣角色〉，《Newtalk 新聞》，2026 年 1 月 27 日，<https://newtalk.tw/news/view/2026-01-27/1016986>。

<sup>8</sup> Elbridge A. Colby, "The Strategy of Denial," *Australian Army Research Centre*, 2021, [https://researchcentre.army.gov.au/library/land-power-forum/strategy-denial?utm\\_source=chatgpt.com](https://researchcentre.army.gov.au/library/land-power-forum/strategy-denial?utm_source=chatgpt.com).

略目標設定下，刻意克制軍事行動的規模與方式，同時將戰場侷限於特定區域，以避免戰事全面擴大。<sup>9</sup>

### 三、情報工作攸關台海攻防決定性角色

美以在首波攻擊得以成功斬首伊朗政軍高層，率先癱瘓伊朗軍政機制正常運作，情報工作居功厥偉，並為其後續軍事行動與政治談判提供有利條件。美以情報工作成就，主要反映於人員滲透與科技優勢。根據英國《金融時報》(*Financial Times*)報導，以色列情報機構摩薩德(Mossad)長年滲透德黑蘭「天網」，透過駭入全城所有交通號誌監視器取得影像，再利用人工智慧(AI)演算法將大量影像建檔轉為情資，從而掌握伊朗最高領袖哈米尼行程及其貼身保鏢的住址、通勤路線與護衛對象；結合美國中央情報局(CIA)提供最關鍵的遭滲透伊朗線民情資，美以完成交叉驗證情報後，才得以發動斬首攻擊一舉擊斃哈米尼。<sup>10</sup>中國輿論分析，則是聚焦於伊朗情報系統與高階官員遭嚴重滲透所扮演關鍵角色。<sup>11</sup>簡言之，沒有情報工作的前置作業，美以聯軍是無法一舉殲滅被嚴密保護的伊朗軍政高層，進而達成癱瘓伊朗軍政指揮系統的作戰目標。

大軍未動，情報先行。「史詩怒火行動」初步能取得重大成果，美以聯軍情報工作的亮眼表現，扮演著核心的關鍵角色。無疑地，這也提供解放軍攻台時的教科書式經驗示範，同時成為國軍進行反滲透與防衛作戰的嚴肅挑戰。

在人員滲透上，前軍情局局長劉德良將軍在「淺談共諜對台滲

---

<sup>9</sup> 鍾志東，〈《鍾志東觀點》美國《2026 國防戰略》看破不說破的台灣角色〉，《Newtalk 新聞》，2026 年 1 月 27 日，<https://newtalk.tw/news/view/2026-01-27/1016986>。

<sup>10</sup> 〈美以獵殺哈米尼內幕曝！以色列滲透德黑蘭天網 CIA 人肉情報成關鍵助攻〉，《聯合新聞網》，2026 年 3 月 3 日，<https://udn.com/news/story/124061/9356650>。

<sup>11</sup> 〈伊朗領導人喪命 中國輿論聚焦情報系統遭嚴重滲透〉，《中央社》，2026 年 3 月 2 日，<https://www.cna.com.tw/news/acn/202603020069.aspx>。

透狀態」指出，根據前國防部副部長林中斌於 2007 年回覆美國《國防新聞周刊》所透露，當時潛伏在台灣共諜至少就有 5000 人，18 年後的今天，共諜應該只會更多不會少。<sup>12</sup>這些滲透於全台灣包括軍中的共諜，勢將成為中國武力犯台時裡應外合的關鍵破壞力量。在科技運用上，聯合作戰（joint operations）的多域態勢感知（multi-domain awareness），在未來台海防衛不對稱作戰扮演關鍵角色，而此攸關情報的獲取、掌控與運用優勢，則將決定聯合作戰成敗。沒有情報優勢，無法進行精準打擊、難以摧毀隱匿設施、也難以預測敵軍攻擊。從戰前準備到戰爭執行，「史詩怒火行動」以實戰驗證，情報工作的關鍵性影響。

## 參、趨勢研判

### 一、對台海安全影響程度將取決於戰事長短

「史詩怒火行動」外溢效果（spillover effect）將影響美中兩國實力消長，進而對台海安全產生影響。美國智庫「哈德遜研究所」（Hudson Institute）一份研究報告即從美中「大國博弈」角度指出，美伊戰爭本質是美中對抗，中國近年來利用伊朗問題，大幅地分散並消耗美國在印太地區反制中國的軍事與財政資源，因此伊朗問題從不只是關於伊朗，而中東問題走向，將決定美國能否在反制中國武力犯台這場「本世紀決定性衝突」勝出。<sup>13</sup>此論述能否成立的前提在於，華府要能見好就收，於短期內結束美伊戰爭並達成川普所提 4 大作戰目標。否則隨著戰事延長與擴大，美國勢將陷入猶如資源消耗黑洞的另一場越南、伊拉克、或阿富汗戰爭，不僅未能享受戰爭

---

<sup>12</sup> 〈中國對台滲透嚴重 前軍情局長劉德良呼籲：應實質強化反滲透戰力〉，《自由時報》，2025 年 8 月 16 日，<https://def.ltn.com.tw/article/breakingnews/5145993>。

<sup>13</sup> Zineb Riboua, “The Iran Strike Is All About China,” *Hudson Institute*, March 1, 2026, <https://www.hudson.org/national-security-defense/iran-strike-all-about-china-zineb-riboua>.

紅利，還將遭受戰爭惡果反噬。如果美國陷入對伊朗戰爭延長與失利態勢，敵消我長之下，中國將坐享隔山觀火漁翁之利，更有底氣地在台海安全上與美國進行對抗。

美伊戰事能縮短並取得預期戰果，將對川普涉入台海安全的意願與能力產生正面影響。反之，則將大幅降低川普軍事介入台海安全可能性。美國對伊朗戰爭的勝利，象徵著美國國力與川普聲望將達到前所未有新高點，華府也將得以更集中全力於印太區域對付中國。相較下，中國不僅將損失在中東地區最重要地緣戰略盟友，在經貿上也將蒙受重大損失，因為無法再從伊朗取得廉價原油，而中國於伊朗巨額投資也將損失慘重。<sup>14</sup>

值得注意的是，美國對伊朗開戰前 48 小時，就消耗了約 48 億美元彈藥，驚人的戰爭成本已引發美國國會關切外，美軍最先進的武器庫存正被快速消耗，也將危及美軍在其他潛在衝突中的備戰狀態。事實上，美軍已開始抽調在韓國的愛國者（Patriot）與薩德（THAAD）防空飛彈、以及駐日兩棲艦及陸戰隊增援到中東備戰。<sup>15</sup>可預期地，隨著美伊戰事延長，美國在難以兼顧下，台海安全所承受的戰略風險也將隨之升高。

## 二、防空飛彈系統使用成本效益將成無可迴避挑戰

戰事延長陷入消耗戰態勢，武器使用成本效益，將在戰場攻防上扮演關鍵性角色。俄烏戰爭早已顯示，誰能在武器成本使用效益獲得優勢，誰就能在消耗戰中取得相對優勢。在人工智慧輔助下，擁有極高性價比的無人載台（unmanned vehicle, UV）的大量運用，

---

<sup>14</sup> 〈紐時：中國在伊朗投資巨大 若戰爭持續恐損失慘重〉，《中央社》，2026 年 3 月 10 日，<https://www.cna.com.tw/news/acn/202603100209.aspx>。

<sup>15</sup> 〈48 小時狂燒 1800 億彈藥 美軍攻伊恐牽動印太部署〉，《自由時報》，2026 年 3 月 10 日，<https://def.ltn.com.tw/article/breakingnews/5365200>。

經實戰驗證已被視為現代戰爭不可或缺一部分，甚至有可能成為改變戰爭態勢的決定性武器。資源相較缺乏國家要能以小搏大，武器使用的成本效益尤顯至關重要。

「史詩怒火行動」中，攻方的美軍採取高低配，首度啟用自殺式無人機 FLM136，削弱敵方防空能力，再搭配高精準武器完成打擊，同時尋求烏克蘭提供反制無人機經驗。<sup>16</sup>守方伊朗，海陸空軍主要武器載台遭美軍摧毀後，其反擊方式主要在於運用價廉、大量、持續的「見證者」(Shahed) 系列自殺無人機 (UAV)，並輔以機動式以及藏匿於地下碉堡的巡弋與彈道飛彈，攻擊美軍以及周遭國家的美軍基地、防空雷達、能源設施等。特別值得注意的是，伊朗運用廉價無人機與低端彈道飛彈，正消耗美軍高端、價昂、數量有限的防空飛彈。伊朗此種成本效益的不對稱消耗戰，形成美軍於彈藥耗損與作戰成本的沉重壓力。<sup>17</sup>

無論是美軍高低配攻擊、還是伊朗無人機飽和攻擊運用，由成本效益觀點檢視防空武器系統運用，將提供台灣寶貴經驗。根據美國《有線電視新聞網》(CNN) 報導，面對伊朗飛彈與無人機攻擊，在美國與伊朗開戰僅四天後，美國一個波灣盟國已經開始缺乏用於攔截伊朗飛彈與無人機攻擊的關鍵攔截飛彈，因此已向美國緊急要求補充攔截飛彈。<sup>18</sup>

中共解放軍所擁有各式飛彈與攻擊無人機群，無論在質與量都遠非伊朗所能比擬。儘管台灣在美國支援下，正積極籌建「台灣之

---

<sup>16</sup> 〈反制伊朗無人機 烏克蘭經驗急送中東〉，《自由時報》，2026 年 3 月 12 日，<https://news.ltn.com.tw/news/world/paper/1746495>。

<sup>17</sup> 〈川普打伊朗 6 天燒掉 3612 億元！還沒算前置成本 實際開支恐更高〉，《聯合報新聞網》，2026 年 3 月 12 日，<https://udn.com/news/story/124061/9375082>；〈「史詩怒火」行動首日 美軍耗費 240 億 航母一天就花 2 億〉，《Newtalk 新聞》，2026 年 3 月 3 日，<https://newtalk.tw/news/view/2026-03-03/1022399>。

<sup>18</sup> Sean Lyngaas, Kylie Atwood, Isabelle Khurshudyan, “The Iran War’s Troubling Missile Math,” *CNN*, March 4, 2026, <https://edition.cnn.com/2026/03/04/politics/missiles-weapons-stockpile-iran-us-war>.

盾」防空系統反制中國解放軍飛彈與無人機攻擊。不過考量防空飛彈價格高昂、數量有限、補給不確定等限制，台灣建構多層次防空系統攔截來襲各式攻擊，宜將武器使用的成本效益納入考量，以極大化價昂的防空飛彈效益。除此之外，伊朗將武器深藏於地下化碉堡，成為伊朗得以持續反擊關鍵。因此在「戰力保存」考量下，如何透過機動化、地下化、碉堡化軍事基礎設施、分散部署等被動防禦作為，以提升防空與反擊系統存活率，同時也將是國軍必須面對的嚴肅挑戰。



# 「各司其職」： 史詩怒火行動中的 AI Agents 作戰分工模式

黃政勛

國防戰略與資源研究所

焦點類別：軍事科技、數位發展

## 壹、前言

2026年2月28日，美國與以色列對伊朗發動高強度空襲行動，美方代號為「史詩怒火行動」(Operation Epic Fury)。<sup>1</sup>行動除以斬首伊朗最高領袖哈梅內伊(Ayatollah Ali Khamenei)為主要目標外，亦打擊伊朗伊斯蘭革命衛隊(Islamic Revolutionary Guard Corps, IRGC)的指揮控制設施、防空系統、飛彈與無人機發射場及軍事機場等關鍵目標，<sup>2</sup>以削弱伊朗政權的安全體系，此次行動不僅具有重大戰略意義，亦展現人工智慧在真實戰爭情境下的作戰成熟度。

在此背景下，本文嘗試分析人工智慧在「史詩怒火行動」中的運作角色，並梳理其作戰分工模式。此次行動整合多個AI相關系統平台，包括SpaceX的Starshield與MILNET衛星通訊系統、Anthropic的Claude人工智慧模型、Palantir的Maven Smart System作戰決策支援平台、Anduril的Lattice自主作戰管理系統、Shield AI的Hivemind自主飛行系統，以及SpektreWorks的LUCAS無人攻擊系統，<sup>3</sup>使各系統在情報蒐集、目標辨識與作戰決策等環節各司其職，形成AI Agents協同運作的作戰工作流。此一模式已顯示AI逐步成為現代從情報到打擊「殺傷鏈」(Kill Chain)的核心運作要素。

---

<sup>1</sup> 以色列行動代號則稱為「咆哮之獅」(Operation Roaring Lion)。

<sup>2</sup> Marisa Garcia, "Operation Epic Fury: How the US & Israeli Attack on Iran Unfolded," *Aerospace Global News*, March 2026, <https://reurl.cc/18Yvo9>.

<sup>3</sup> 〈美伊戰爭揭 AI 軍備時代降臨：Claude 解讀波斯語機密，Palantir 工程師嵌入美軍司令部〉，《星島日報》，2026年3月2日，<https://reurl.cc/M2dgYp>。

## 貳、安全意涵

### 一、人工智慧系統的作戰分工與功能應用

在此次行動中，人工智慧系統被廣泛運用（如表 1 所示）。首先，低軌衛星網路成為關鍵通訊基礎，提供「永遠在線」的通訊能力。SpaceX 的 Starshield 與 MILNET 衛星星座在地面通訊受干擾時仍能維持低延遲與加密連線，使 Maven 系統的資料分析、Claude 的推理運算及無人機協同指令得以即時傳輸，<sup>4</sup>此種分散式衛星通訊架構降低對地面站的依賴，使戰場指揮與管制由傳統集中式模式轉變為支援「聯合全域指揮管制」（Combined Joint All-Domain Command and Control, CJADC2）的分散式決策網絡，<sup>5</sup>並實現「決策壓縮」，將軍事計畫週期從數週縮短至分鐘級。

在穩定的通訊與資料傳輸基礎上，AI 系統進一步承擔戰場資訊分析與決策支援功能。其中，Palantir 的 Maven Smart System 負責整合衛星影像、無人機偵察與各類感測資料，建構即時戰場態勢圖；<sup>6</sup>而 Anthropic 的 Claude 則作為核心推理模型，對大量情報資料進行語意解析與模式辨識。透過 AI 推理與演算法分析，系統可自動生成潛在目標清單，並依威脅程度與作戰優先順序進行排序，同時提供多種打擊方案與風險評估。<sup>7</sup>此種 AI 驅動的目標生成與決策支援機制，大幅縮短原本依賴人工分析的作戰流程，進一步提升「殺傷鏈」（Kill Chain）中目標識別與決策環節的效率。

---

<sup>4</sup> 王白石，〈中東變局 | 伊朗全國斷網點知行蹤早被「星盾」鎖定〉，《香港經濟日報》，2026 年 3 月 11 日，<https://reurl.cc/X2kMde>。

<sup>5</sup> “How US Military Used Claude AI to Plan and Execute 1,000 Iran Strikes within a Single Day,” *Times Now*, 2026, <https://reurl.cc/qpgV53>。

<sup>6</sup> T Tara Copp, “The AI Tool Central to US Campaign in Iran,” *Mumbai Mirror*, March 5, 2026, <https://reurl.cc/WbLmNZ>。

<sup>7</sup> 同註 5。

表 1、史詩怒火行動中 AI 系統角色與功能概覽

供應商	系統名稱	功能	實際應用
SpaceX	Starshield (MILNET)	<ul style="list-style-type: none"> <li>• 軍事衛星通訊傳輸</li> <li>• 低延遲戰場通信網路</li> </ul>	提供戰場衛星通訊與資料傳輸
Anthropic	Claude Gov	<ul style="list-style-type: none"> <li>• 自然語言理解與推理</li> <li>• 情報資料分析與目標排序</li> </ul>	分析大量情報並生成目標建議
Palantir Technologies	Maven Smart System (MSS)	<ul style="list-style-type: none"> <li>• 多來源戰場資料整合</li> <li>• 目標識別與態勢分析</li> </ul>	整合戰場資料並支援即時決策
Anduril Industries	Lattice	<ul style="list-style-type: none"> <li>• 感測資料整合與控制</li> <li>• 多無人系統協同作戰</li> </ul>	整合感測與無人系統進行協同
Shield AI	Hivemind	<ul style="list-style-type: none"> <li>• 無人系統自主導航</li> <li>• 多平台協同作戰</li> </ul>	支援無人系統自主任務執行
SpektreWorks	LUCAS	<ul style="list-style-type: none"> <li>• 自主導航與目標打擊</li> <li>• 群體式無人系統作戰</li> </ul>	執行低成本自主攻擊任務

資料來源：本表由作者綜整。

在完成通訊基礎與生成式 AI 導入後，戰場系統仍須確保各來源資訊能持續流通並即時整合，使分析結果能在前線迅速轉化為作戰行動。為此，美軍透過 Anduril 的 Lattice 操作系統與 Palantir 的 Maven 平台建立跨平台資料融合架構，將衛星、無人機、地面雷達與信號情報設備整合為統一的感測器網絡，以支援戰場資訊的即時共享與協同運作。<sup>8</sup>同時，藉由部署邊緣運算 (Edge Computing)，<sup>9</sup>前線設備如無人機、戰術中繼站與野戰指揮所可在本地即時處理資料，完成目標分類、追蹤與優先排序，<sup>10</sup>確保前後方部隊資訊的一致

<sup>8</sup> Don Bradford, "Anduril and Palantir: AI-Enabled Transformation of U.S. Defense," *Lodi411 LodiEye*, February 25, 2026, <https://reurl.cc/lpdW16>.

<sup>9</sup> "Anduril Lattice: The Open OS That Brings Autonomy to Combat," *War Wings Daily*, October 1, 2025, <https://reurl.cc/53q9p6>.

<sup>10</sup> Maximilian Schreiner, "US Military Uses Anthropic's Claude for AI-Driven Strike Planning in Iran War," *The Decoder*, March 4, 2026, <https://reurl.cc/bdRrMy>.

性與協同效能。<sup>11</sup>

在作戰協調與無人系統運用層面，隨後將前述決策轉化為實際軍事行動。其中，Anduril 的 Lattice 與 Shield AI 的 Hivemind 形成關鍵作戰架構，使多個無人平台即使在通訊受干擾或 GPS 遭拒止的環境下，仍能維持協同作戰能力。Hivemind 使無人機無需依賴 GPS 導引即可自主飛行並執行預設任務，確保在通訊中斷時仍能維持戰術行動的連續性。<sup>12</sup>在實戰中，美軍首次大規模部署由 SpektreWorks 開發的低成本無人攻擊系統 LUCAS (Low-Cost Unmanned Combat Attack System)，單機成本約 3.5 萬美元，主要用於對伊朗防空設施與軍事基礎設施實施群體式打擊。<sup>13</sup>根據既有資料推估，LUCAS 可依據 Lattice 下達的任務資料自主導航至目標區域，<sup>14</sup>並透過機載光電及紅外線 (EO/IR) 感測器完成目標識別與定位，隨即實施攻擊。

15

上述各系統雖各有分工，但並非孤立運作，而是透過 AI Agents 的協同機制形成連貫的作戰流程，以下進一步說明。

## 二、人工智慧 Agents 的作戰流程與協同運作

在前述系統分工的基礎上，本節進一步以生成式 AI Agents 理論框架對「史詩怒火行動」的實際運作邏輯進行詮釋，說明各系統如何在 SpaceX 的 Starshield 與 MILNET 衛星網路提供的通訊基礎上，形成「推理 (Reason) — 資料檢索 (Access Memory) — 行動 (Act) — 持續優化 (Learn & Reflection)」的循環機制 (如圖 1 所

---

<sup>11</sup> “Project Maven, “Wikipedia,” accessed March 2026, [https://en.wikipedia.org/wiki/Project\\_Maven](https://en.wikipedia.org/wiki/Project_Maven).

<sup>12</sup> “Shield AI and Airbus Complete Successful Autonomous Flight with DT25 Target Drone,” *Shield AI*, September 23, 2025, <https://reurl.cc/WbLK15>.

<sup>13</sup> Aspen Pflughoeft, “Use of LUCAS Drones in Iran Puts Focus on Affordable, Fast-Moving Acquisition,” *Aerospace America*, March 4, 2026, <https://reurl.cc/kp0K6G>.

<sup>14</sup> “Anduril Lattice: The Open OS That Brings Autonomy to Combat,” *War Wings Daily*, October 1, 2025, <https://reurl.cc/xW0qZz>.

<sup>15</sup> 同註 13。

示)，由此推論 AI Agents 在現代戰場的具體樣貌。

首先，在推理（Reason）階段，Palantir 的 Maven Smart System 整合衛星影像與各類感測資料建構即時戰場態勢圖，Anthropic 的 Claude 則負責語意解析與目標清單生成，並依威脅程度提出多種打擊方案，使情報分析轉化為 AI 輔助的快速決策機制。

在資料檢索（Access Memory）階段，Anduril 的 Lattice 與 Palantir 的 Maven 平台透過跨平台資料融合，將衛星、雷達、無人機與信號情報整合為統一感測器網路，並藉邊緣運算於前線即時完成態勢同步，確保推理結果能即時轉化為可執行指令。

在行動（Act）階段，Anduril 的 Lattice 與 Shield AI 的 Hivemind 協調無人機平台完成任務分配，SpektreWorks 的 LUCAS 則透過「感測器到射手」（Sensor-to-Shooter）管道自主導航並實施打擊。

在持續優化（Learn & Reflection）階段，作戰過程中蒐集的戰場資料即時回傳系統，驅動模型更新與戰術調整，形成動態優化的作戰循環。

透過上述四個階段的協同運作，「史詩怒火行動」展示了 AI Agents 在現代戰場的完整作戰鏈，戰場決策與作戰行動逐漸形成一套可持續運作與動態調整的智慧化作戰體系。



圖 1、史詩怒火行動 AI Agents 作戰流程圖

資料來源：本圖由作者透過 AI 生成。

## 參、趨勢研判

### 一、AI Agents 作戰架構的發展趨勢與戰略啟示

從「史詩怒火行動」中可以觀察到，人工智慧在現代戰場的角色已從單一分析工具，演進為整合作戰流程的核心架構。此次行動中，Claude、Maven、Lattice、Hivemind 等 AI 系統依情報分析、決策支援與作戰執行等功能分工協作，形成完整的多 Agent 協同體系，大幅壓縮決策與行動之間的時間差。此一趨勢意味著未來戰場指揮模式將逐步由傳統層級式結構，轉向以資料整合與演算法分析為核心的分散式決策體系。

對臺灣而言，在高度資訊化與多領域作戰環境下，如何整合人工智慧、感測器網絡與無人系統，建立具備快速決策與即時反應能力的作戰架構，將成為未來防衛體系的重要發展方向。特別是在可能面臨高密度飛彈、無人機與資訊戰等複合威脅情境下，AI Agents

所帶來的快速決策與跨系統整合能力，不僅有助於提升指揮管制效率與整體作戰韌性，亦可能成為影響未來戰場節奏與主導權的重要關鍵。

## 二、從問答式AI到Agentic AI的作戰應用轉變

從技術演進的角度來看，「史詩怒火行動」亦顯示生成式 AI 技術正從傳統問答式 AI（Chat-based AI）逐步演進為具備自主任務能力的 Agentic AI。過去以大型語言模型為代表的生成式 AI，多應用於文件整理、資料摘要與決策輔助等日常工作情境，主要仍由人類主導操作；然而在此次行動中，Claude 等生成式 AI 已被整合至戰場系統之中，與 Maven、Lattice 與 Hivemind 等平台共同形成 AI Agents 作戰架構，使 AI 不僅能進行情報分析與目標生成，更能參與任務規劃與作戰流程運作。

此一轉變亦反映出人工智慧技術正由「工具型 AI」邁向「任務型 AI」，並呈現出民用科技向軍事領域擴散的趨勢。未來隨著生成式 AI、感測器網絡與無人系統持續整合，AI Agents 將可能在情報分析、作戰協調與無人系統控制等環節扮演更關鍵的角色，並進一步改變現代戰爭的運作模式。



# 軍事作戰模式模擬： 人工智慧時代的轉型與挑戰

林超倫

網路安全與決策推演研究所

焦點類別：作戰概念

## 壹、前言

2026年2月28日，美國軍方在針對伊朗的軍事行動中，首次大規模將 Anthropic 科技公司的人工智慧工具 Claude 整合進入「Maven Smart System」的數據分析平台，進行威脅目標識別與攻擊排序，將原本需耗時數週的作戰計畫縮短至即刻（Real time）可以進行。<sup>1</sup>可見當前競爭激烈的全球地緣政治環境下，軍事作戰的性質正經歷先進科技的重大變革，而人工智慧（AI）則是這場變革的主角。未來的戰場將是「演算法戰場」（Algorithmic Battlefield），跨越陸、海、空、太空與網路等多重作戰領域。美國與中國等大國正投入龐大預算於軍民兩用的 AI 應用，關鍵在於誰能夠最快掌握決策優勢。

軍事決策過程（Military Decision-Making Process, MDMP）與作戰模式模擬是決定戰爭勝負的關鍵因素之一。過往指揮官與參謀們需要耗費數天甚至數月來進行情報準備、行動方案（Course of Action, COA）預擬及兵棋推演。然而，現代戰場之威脅與變化節奏極為快速，光靠過去的人力作業流程已經無法跟上戰場變化。因此，將 AI 引入軍事作戰模式模擬，已是各國軍隊現代化的首要任務。

---

<sup>1</sup> Gerrit De Vynck, “Anthropic Says it Disrupted an Iranian AI influence Campaign,” *Washington Post*, March 4, 2026, <https://www.washingtonpost.com/technology/2026/03/04/anthropic-ai-iran-campaign/>.

今（2026）年 1 月，美國國防部發布最新的《國防部人工智慧戰略》，明確宣示要將美軍轉型為「AI 優先」（AI-first）的作戰部隊，不僅將 AI 視為尖端科技的較量，更是一場「採用與擴散速度」的競賽。該戰略中，美國國防部推出了七項「指標性專案」（Pace-Setting Projects, PSPs），其中直接針對軍事作戰模式模擬的專案，計有包括加速 AI 軍事作戰模式模擬能力的「安德的鑄造廠」（Ender's Foundry），以及推動戰鬥管理與決策支援的「代理網路」（Agent Network）等兩項。<sup>2</sup>

同時，美國陸軍也正積極實驗如「COA-GPT」這類 AI 系統，透過將作戰準則輸入大型語言模型，可以依據地形、敵我軍力與任務目標等各種變數之不同，在幾秒鐘內自動產生多種作戰行動方案，同時也可以在軍事作戰模式模擬環境中對所選擇之行動方案進行效能評估。<sup>3</sup>不過，此類人工智慧的引入，除了帶來前所未見的速度與效能優勢，也引發許多安全的隱患、倫理道德的爭議，以及對國際法規的挑戰。後續將就安全意涵與趨勢研判實施探討。

## 貳、安全意涵

AI 導入軍事作戰模式模擬，必將大幅縮短「觀察、定向、決定、行動」的「OODA 循環」，但以下風險必須正視。

### 一、AI 模型的技術問題

AI 軍事作戰模式模擬依賴機器學習（ML）與深度學習（DL）等模型，這些模型透過分析龐大數據來識別模式並做出預測，但有

---

<sup>2</sup> Nooree Lee et al., "Pentagon Releases Artificial Intelligence Strategy," *Inside Government Contracts*, February 3, 2026, <https://www.insidegovernmentcontracts.com/2026/02/pentagon-releases-artificial-intelligence-strategy/>.

<sup>3</sup> Michael Gallitelli, "The AI Arms Race: Assessing the Impact of Artificial Intelligence on the Future of Great Power Competition," *Journal of Advanced Military Studies*, Vol. 16, No. 2, 2025, [https://www.usmcu.edu/Portals/218/JAMS\\_Fall%202025\\_16\\_2\\_Gallitelli.pdf](https://www.usmcu.edu/Portals/218/JAMS_Fall%202025_16_2_Gallitelli.pdf).

以下兩個技術問題。首先，當 AI 模型過度適應有限的訓練數據時，會失去對真實世界的理解能力。在完美的模擬環境中，AI 可以產出無懈可擊的作戰方案，但真實戰場充滿變數與干擾，一旦面臨意料之外的戰場條件（如感測器被干擾或敵軍偽裝等），AI 模型可能發生嚴重誤判，導致誤擊友軍或平民。其次是黑箱作業問題，AI 模型自行使用各種演算法處理非常複雜之數據，使決策過程對人類而言極度不透明，各級指揮官會收到 AI 模型產生的敵目標清單或作戰行動，卻無法回溯如何得到這些結論，久而久之這種不透明，將導致指揮官在高壓戰場下盲目信任或過度依賴 AI 模型。<sup>4</sup>

## 二、AI模型採用量化指標的迷思

當前的 AI 軍事作戰模式模擬（如 COA-GPT）在評估行動方案時，過度依賴量化指標，例如殲滅敵軍或奪取地形給予正分（+1），友軍損失給予負分（-1），這種運算邏輯似有過度依賴數學模型的隱憂。例如，軍事理論家克勞塞維茨（Clausewitz）曾警告，戰爭充滿各種不確定性，以及諸如人類的意志力與士氣等無法量化的「摩擦」（friction）；<sup>5</sup>而目前的 AI 模型則可以預設出一個具有確定性的戰爭，完全排除各種可能的戰場摩擦。另外，若以敵軍傷亡作為 AI 模型的「獎勵函數」，則與越戰時期美國國防部長麥納馬拉（McNamara）依賴「殲敵計數」（body count）來衡量勝利的邏輯如出一轍，這種計算邏輯將導致 AI 模型選擇能在戰術上殺死最多敵人，但在戰場上可能引發大量平民傷亡之損害。<sup>6</sup>

## 三、國際人道法與責任機制的挑戰

近年的烏俄戰爭與以色列加薩衝突中，AI 軍事作戰與模式模擬

---

<sup>4</sup> *Ibid.*, p. 109-113.

<sup>5</sup> *Ibid.*, p. 125.

<sup>6</sup> *Ibid.*, p. 125.

（如以色列的 Habsora/Gospel 系統）據信已投入戰場，這似乎對《日內瓦公約》與《第一附加議定書》構成相當程度的挑戰。第一，AI 模型能否準確區分戰鬥人員與平民？在進行攻擊「比例原則」評估時，能否真正衡量附帶損害與預期軍事優勢之間的道德比重？缺乏人類直覺的演算法是否在人口密集的城市戰中，極易引發人道災難？其二，當 AI 模型出現錯誤並導致戰爭罪行時，責任該歸咎於誰？《羅馬規約》第 28 條規定的「指揮官責任」難以適用於 AI 模型與演算法。同時，民間國防承包商與演算法開發者不直接受國際人道法拘束，導致追究個體刑事責任與國家責任時將面臨各種實質證據與程序上的障礙；第三，《第一附加議定書》第 36 條要求各國在部署新武器前進行合法性審查。然而，各國對其 AI 模型是否經過此審查幾乎完全保密，這種缺乏透明度的作法亦會有重大影響。<sup>7</sup>

#### 四、AI 模型依賴與資安威脅

美國國防部的 AI 戰略強制推行「數據法令」(Data Decrees)，要求各軍種必須向 AI 模型開發者全面開放資料。然而，強制的數據共享極可能大幅增加網路攻擊的接觸面與反情報作為之相關風險。<sup>8</sup>如果系統安全工程未能跟上數據共享的節奏，那麼敵方（如具有國家背景的駭客）可以透過各種方式，進入訓練資料庫中植入惡意參數，導致 AI 模型在關鍵時刻做出致命的建議。另外，隨著量子運算的發展，現有傳統加密的通訊與資料庫均面臨被破解的風險，相關資訊安全保護措施，已成為迫切的國安問題。<sup>9</sup>

---

<sup>7</sup> Muthulakshmi A, "Reassessing International Legal Norms on Autonomy and Accountability in the Laws of War in the Age of Artificial Intelligence," *International Journal of Law*, Vol. 12, Issu. 1, 2026, p. 266, <https://www.lawjournals.org/assets/archives/2026/vol12issue1/12052.pdf>.

<sup>8</sup> Lee et al., "Pentagon Releases Artificial Intelligence Strategy,"

<sup>9</sup> Lisyah Bahar Manoah, "Rising Defense Spending: Fueling A Deep Tech Boom In 2026," *Forbes*, March 3, 2026, <https://www.forbes.com/councils/forbesfinancecouncil/2026/03/03/rising-defense-spending-fueling-a-deep-tech-boom-in-2026/>.

## 參、趨勢研判

從烏俄戰爭、以色列加薩衝突，以及美國對委內瑞拉總統的斬首行動，再加上今（2026）年 2 月 28 日起，美國與以色列聯手攻擊伊朗的作戰行動中，我們處處可以看到 AI 模型的身影，可見軍事作戰模式模擬的重大變革早已勢不可擋。以下探討其相關發展趨勢。

### 一、技術架構必須修正

未來的 AI 模型不應將戰爭視為「完美棋局」的封閉性演算架構，而是必須容納不確定性（複雜變數、戰爭中的摩擦）的複雜架構。為了應對戰爭之霧，未來的 AI 模型必須結合「馬可夫決策過程」（MDP）<sup>10</sup>、「貝氏網路」（Bayesian networks）<sup>11</sup>與「蒙地卡羅模擬」（Monte Carlo simulations）。AI 模型產出的作戰方案不再只給予「分數」，而是必須附帶「信心區間」與「風險機率」之評估內涵。此外未來 AI 模型不會只在任務前只給出一套不可改變的命令，而是必須「持續監聽」與「始終在線」，AI 模型隨著部隊持續之推進，即時納入無人機、衛星與各種前線感測器（如雷達、各種情報）的回饋，進行動態修正。再來為了打破「黑箱」作業，美國國防高等研究計畫署（DARPA）的 XAI 計畫可以讓指揮官透過熱點圖或決策樹，清楚看到 AI 模型提出某個行動方案是基於哪些情報之假設與數據，從而進行有意義的人力調整。<sup>12</sup>

### 二、採購流程必須加速與精簡流程

前述美國國防部在 2026 年的《國防部人工智慧戰略》確立「採用速度」為主之競爭模式，故開始採用「戰時」標準來打破拖累 AI

---

<sup>10</sup> 馬可夫決策過程（Markov decision process, MDP）是離散時間隨機控制過程，它提供一個數學框架，用於在結果部分隨機且部分受決策者控制的情況下對決策建模。

<sup>11</sup> 貝氏網路（Bayesian Network）：一種圖形化機率模型，用於表示和推理變數之間的條件依賴關係，能夠根據新證據更新風險與成功率的機率。

<sup>12</sup> Gallitelli, “The AI Arms Race,” p. 124.

模型整合的官僚體制，在過往需要耗時數月至數年的安全認證（如 FedRAMP）將被大幅壓縮，首席數位與 AI 官員（CDAO）獲得授權建立「障礙消除委員會」，有權豁免非法律規定的相關要求，並強制實施「授權營運（ATO）互惠」，確保 AI 模型能即時投入實戰。<sup>13</sup>此外，美國國防部不再依賴耗時數年開發的軍用專屬封閉系統，而是規定未來在採購 AI 模型時，必須確保在商業最新版本公開發布的 30 天內，軍方就能將其部署給各級作戰部隊。<sup>14</sup>另在作戰模擬系統方面規定強制使用開放架構，允許軍方在不依賴原廠（Prime Contractor）的情況下，以商用軟體更新的速度快速替換底層的 AI 組件與演算法。

### 三、強化軍隊體制改革

為了確保 AI 模型能真正發揮效用而不致引發人道災難，美國國防部透過「準則、組織、訓練、裝備、領導及教育、人員、設施與政策」（DOTMLPF-P）架構進行全面改革。<sup>15</sup>首先是更新作戰準則與控制層級。作戰準則必須明確將 AI 模型定位為「協助生成與測試 COA 的工具」，而非「決策者」。作戰準則也嚴格界定「迴路內的人」（Human-in-the-loop, HITL）與「迴路上的人」（Human-on-the-loop, HOTL）的適用場景；<sup>16</sup>在充滿道德模糊與平民傷亡風險的城鎮戰中，必須強制維持 HITL；而在防空反導彈等極度壓縮時間的戰場，則可適度依賴 HOTL。其次，傳統龐大的指揮所極易成為敵方

---

<sup>13</sup> Wiley Robinson, "The Algorithmic Battlefield: Forging The U.S. Army's Future Dominance With A New Breed Of Acquisition Leader," *USAASC*, March 2, 2026, <https://asc.army.mil/web/the-algorithmic-battlefield/>.

<sup>14</sup> U.S. Department of War, "Artificial Intelligence Strategy for the Department of War: Accelerating the Safe and Responsible Integration of AI into National Defense," January 9, 2026, <https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF>.

<sup>15</sup> DOTMLPF 是 Doctrine, Organization, Training, Material, Leadership & Education, personnel, Facility and Policy 的縮寫。Gallitelli, "The AI Arms Race," p. 119.

<sup>16</sup> Gallitelli, "The AI Arms Race," p. 120.

精準打擊的目標，若透過 AI 模型承擔繁重的情報統整與計畫擬定任務，未來的指揮所將更加小型化、機動化且具備高度生存力。第三，組織架構上，美軍將設立專門的跨學科「AI 紅軍」部隊，融合機器學習與電子戰專家，透過模擬數據進行對抗性演練，以利在實戰之前主動尋找 AI 模型之認知錯誤。<sup>17</sup>最後則是強化採購人員與指揮官的「AI 素養」。採購人員必須從傳統的合約管理者轉型為懂數據科學、網路安全與能源市場的採購專家；同時，指揮官雖不必是程式設計師，但必須受過 AI 素養訓練，具備挑戰機器輸出、識破演算法偏見的能力，並持續透過包含 AI 模型參與的「實兵對抗兵推」來磨合人機信任。

#### 四、國防工業生態重塑

當前全球軍費飆升（2025 年達到 2.7 兆美元），國防科技已成為資本市場（包括家族辦公室、創投與私募股權）的要角。如 Anduril 與 Palantir 等具備矽谷背景的新創科技公司，正以其精準、快速與深厚的軟體實力，打破傳統軍工巨頭的壟斷，這類公司已在美軍推動無人機蜂群的「複製者計畫」（Replicator）及各式 AI 專案中扮演核心角色。儘管資本湧入，但硬體製造仍是瓶頸，據美國國會研究處指出，原定於 2025 年夏季部署數千架無人機的「複製者計畫」，因技術故障、指揮軟體整合困難以及成本過高（例如單架彈簧刀 600 無人機成本超過 10 萬美元）而進度落後。<sup>18</sup>顯示未來國防工業的挑戰將會是如何將成熟的 AI 模型模擬能力，順利連接並量產廉價且具備韌性的實體無人系統。

---

<sup>17</sup> Gallitelli, “The AI Arms Race,” p. 121.

<sup>18</sup> Stavroula Pabst, “DoD Promised a ‘Swarm’ of Attack Drones. We’re Still Waiting,” *Responsible Statecraft*, October 28, 2025, <https://responsiblestatecraft.org/replicator/>.

## 五、國際法規的探討

在美國國防部在 2026 年戰略中，可以看出明確反對將意識形態或過度的社會公平（DEI）指標強加於 AI 模型上，其定義的「負責任 AI」是指「客觀真實且允許在合法戰爭規範內進行任何戰鬥用途的 AI 能力」，以確保 AI 模型「不會妨礙你打仗」。面對此種可能的 AI 責任模糊真空，國際法學界與多邊論壇（如聯合國 LAWS 政府專家小組）正推動對《第一附加議定書》增加新議定書。未來的趨勢可能包括強制要求所有 AI 模型掌控之武器在關鍵決策點維持可驗證的人類監督，禁止完全脫離人類介入的致命決策，並推動類似國際原子能總署（IAEA）的獨立技術審查與武器登記制度，以確保透明度與建立互信。<sup>19</sup>

## 六、對我國的啟示

面對「人工智慧與演算法」的快速崛起，台灣應積極將之導入「軍事作戰模式模擬」決策過程，藉此迅速縮短「OODA 循環」，在不對稱防衛作戰中搶占先機。當然，借鏡美軍體制改革，利用 AI 模型處理作戰、情報等任務乃是勢在必行，但是更重要的是國軍必須在作戰準則上明確界定 AI 模型僅為輔助決策工具，並嚴格制定「人機協同」之規範，以防範 AI 模型帶來的致命誤判；此外台灣具備全球科技與晶片發展之優勢，更應善加利用及整合，方能厚植真正的國防韌性。

---

<sup>19</sup> Muthulakshmi, “Reassessing International Legal Norms,”

# 川普 2.0 網路戰略下的安全意涵 與未來發展趨勢

曾敏禎

網路安全與決策推演所

焦點類別：網路戰、網路安全

## 壹、前言

美國 2026 年 3 月 6 日發布《川普總統美國網路戰略》( *President Trump's Cyber Strategy for America* ) ( 以下簡稱《戰略》 )<sup>1</sup> 相較於拜登政府 2023 年的《國家網路安全戰略》<sup>2</sup> 此份《戰略》在戰略思維、政策工具與作戰模式上有著鮮明的轉變 ( 如表 1 )，呈現更強烈的進攻性與主動威懾特徵。

表 1、拜登與川普政府有關網路戰略對照表

比較項目	2023 年拜登政府 《國家網路安全戰略》	2026 年 《川普總統美國網路戰略》
核心	數位生態系統的「韌性」與「長期協作」	「美國優先」與展現「美國力量」
政策支柱	1、捍衛關鍵基礎設施 2、擾亂和摧毀威脅行為者 3、塑造市場力量推動安全 4、投資具韌性的未來 5、建立國際夥伴關係	1、塑造對手行為 2、推動常識性監管 3、現代化與保護聯邦網路 4、保護關鍵基礎設施 5、維持關鍵與新興技術優勢 6、建立人才與能力
對抗手段	透過執法與國際合作「擾亂」威脅者	運用「整套攻防行動」主動「干擾、擾亂與迷失」對手
監管立場	強化市場責任，推動軟體供應商法律責任	「去管制化」，移除負擔重且無效的規定以提升敏捷性

<sup>1</sup> “White House Unveils President Trump’s Cyber Strategy for America,” *The White House*, March 6, 2026, <https://www.whitehouse.gov/articles/2026/03/white-house-unveils-president-trumps-cyber-strategy-for-america/>.

<sup>2</sup> “FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy,” *The American Presidency Project*, March 2, 2023, <https://www.presidency.ucsb.edu/documents/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy>.

技術重心	投資具韌性未來技術、雲端安全	代理型 AI (Agentic AI)、生成式 AI 與後量子加密 (Post-quantum cryptography, PQC)
私營部門關係	透過市場力量與法規要求推動產業安全	建立公私協作，透過激勵機制釋放私營部門潛力
國際觀點	謀求共同目標國際夥伴關係	確保標準符合美國價值，對抗外國監控技術
威懾策略	提高網路犯罪難度與成本	施加「最慘重且可怕代價」，動用所有國家權力工具

資料來源：作者自行綜整。

## 貳、安全意涵

### 一、由防禦走向主動威懾：網路攻勢能力成為國家權力延伸

美國網路安全戰略已由過去偏重於防禦與事件回應模式，逐步轉向以「主動威懾」(active deterrence) 為核心的攻防整合策略。

《戰略》指出，美國將運用「政府全部工具」(all instruments of national power)，包含網路攻擊、制裁、外交壓力與執法行動，以「塑造對手行為」(Shape Adversary Behavior)，亦即在敵方攻擊發生之前削弱其能力與意圖，顯示美國不再僅追求網路系統防護與復原，而是透過主動干預與先制行動，在威脅形成初期即加以遏制。

此一轉變反映出網路空間已被視為與傳統陸、海、空及太空領域同等重要的戰略競爭場域。過去美國網路政策多集中於保護政府網路與關鍵基礎設施，但新《戰略》更強調透過例如摧毀詐騙與駭客網絡、追捕駭客與間諜，並對外國駭客組織或相關企業施加制裁等攻勢行動直接削弱敵方能力，使網路攻勢逐漸成為常態化的國家政策工具。近期案例即針對委內瑞拉總統馬杜羅 (Nicolás Maduro) 行動中，美方透過網路手段干擾對手系統，<sup>3</sup>使敵方在關鍵時刻陷入

<sup>3</sup> “U.S. Space and Cyber Commands Support Massive Air Assault to Capture Maduro,” *SATNEWS*, January 5, 2026, <https://news.satnews.com/2026/01/05/u-s-space-and-cyber-commands-support-massive-air-assault-to-capture-maduro/>.

「失明與混亂」狀態，凸顯網路作戰已成為支援實體軍事與執法任務重要工具。

此外，《戰略》亦凸顯「跨領域整合」（cross-domain integration）重要性。美國政府明確表示，回應網路威脅的方式不會侷限於網路空間，而將延伸至外交、經濟與軍事領域，例如透過金融制裁、供應鏈限制、國際執法合作或公開揭露敵對行為等方式，全面提高對手進行網路攻擊成本。

整體而言，美國此一「以攻為守」戰略思維，旨在透過持續施壓與能力展示，使潛在敵人必須考量到攻擊美國後續付出的高昂代價。對台灣而言，此一發展亦具有重要啟示。面對日益頻繁的國家級網路攻擊，若僅依賴防禦性資安架構，將難以有效因應複雜威脅。未來除強化基礎資安防護外，也需逐步建立主動防禦與反制能力，並透過與盟友深化情報共享與聯合行動機制，以提升整體網路威懾力與國家安全韌性。

## 二、科技供應鏈安全化：數位基礎設施成為地緣政治競爭核心

《戰略》明確指出，美國將逐步「遠離敵對國家供應商與產品」，並透過政策支持、市場誘因與產業合作，推動以本土技術為核心的可信供應鏈體系，顯示美國已將科技供應鏈視為國家安全防線的一部分，而非單純經濟或產業議題。換言之，未來科技競爭不僅是市場競爭，更是國家安全與制度競爭延伸。

在此框架下，美國特別重視人工智慧、量子運算、雲端基礎設施、半導體及資料中心等關鍵技術領域，並透過政策與投資確保自身技術優勢，同時限制潛在對手在全球數位基礎設施中的影響力，這種作法本質核心目標在於建立由民主國家主導的安全技術生態系。《戰略》同時警告部分國家正透過輸出監控技術與數位治理模

式，推動具備審查與監控能力的「數位威權技術」，因此美國未來將透過外交合作與國際規範推動，強化以民主價值為基礎科技標準與網路治理模式。

從安全實務層面觀察，美國亦強調關鍵基礎設施與數位系統必須採取更嚴格的安全架構，例如推動「零信任架構」(Zero Trust Architecture)及供應鏈安全審查機制。透過強化能源電網、金融系統、電信網路、資料中心與水資源系統等關鍵基礎設施防護，美國正試圖在其數位邊界周圍建立更具韌性安全體系。上述反映美國認為網路安全漏洞往往源自對外部技術的依賴，因此安全不再僅是軟體層面防護，而是涵蓋從晶片設計、硬體製造到雲端服務的整體供應鏈「可信度」。

此一「去風險化」(de-risking)與供應鏈重組政策，也將對全球數位秩序產生深遠影響。未來全球科技供應鏈或逐漸形成兩個主要陣營：一方是以美國與其盟友為核心的「可信科技聯盟」，另一方則以威權國家為主導建立替代性技術體系，此種趨勢將促使全球數位經濟逐步走向分化與碎片化，各國在技術標準與供應鏈合作上恐被迫做出戰略選擇。

對台灣而言，由於在半導體與高科技產業鏈中具有關鍵地位，未來在美國科技安全戰略中角色將更加重要。然而，這同時也意味台灣將面臨更高程度地緣政治壓力與供應鏈重組風險，因此如何在維持產業競爭力同時強化供應鏈韌性、深化與民主科技聯盟合作，將成為未來國家安全與產業政策的重要課題。

## 參、趨勢研判

### 一、AI主導自動化網路戰：演算法與算力競賽的新戰場

《戰略》明確指出，美國將快速導入「生成型人工智慧」

(Generative AI) 與「代理型人工智慧」(Agentic AI)，並利用 AI 技術來「偵測、轉向與欺騙」威脅行為者，同時大幅提升網路防禦與攻擊能力，顯示未來網路衝突將逐漸從傳統人力主導模式，轉向高度自動化與演算法驅動作戰形態，使網路攻防競爭更接近一場「機器對機器」演算法競賽。

首先，在防禦層面，AI 將大幅提升網路安全系統即時反應能力。透過機器學習與大數據分析，AI 可以在極短時間內處理龐大網路流量與系統日誌，快速辨識異常行為並進行威脅判斷。相較傳統資安系統需要人工分析與回應，AI 代理可在毫秒內自動採取防禦措施，例如封鎖惡意連線、修補漏洞或重新配置網路結構。這種「自主化防禦」能力將使國家能夠在大規模網路攻擊中維持系統穩定，並降低人力負擔與反應延遲。

惟 AI 影響同樣也將改變網路攻擊方式，用於自動化漏洞挖掘、惡意程式生成與社交工程攻擊，例如利用生成式 AI 製作高度逼真的釣魚郵件或深偽 (deepfake) 影音內容，以提升滲透成功率。此外，未來國家級網路部隊亦走向部署 AI 代理 (AI agents)，自動執行偵察、滲透與破壞任務，包括持續掃描目標系統漏洞、建立隱蔽後門或干擾關鍵基礎設施。當攻擊與防禦雙方皆採用 AI 系統時，網路衝突將逐漸演變為高度自動化的「演算法對抗」。

此一趨勢也將帶來攻防成本與能力分布重大變化。AI 工具能快速生成大量程式碼與惡意內容，使原本需要高度技術能力攻擊行動變得更加容易實施，從而降低網路攻擊的門檻，代表除大國外，更多中小型國家甚至非國家行為者亦可取得一定程度網路攻擊能力。同時，AI 驅動的攻擊速度遠超人類決策週期，使衝突升級與誤判風險增加，對既有網路危機管理機制帶來新的挑戰。此外，《戰略》亦

強調保護「AI 技術開發堆疊」(AI technology stack) 重要性，包括資料中心、訓練資料、演算法模型與算力基礎設施，凸顯未來國際競爭不僅發生在網路攻防層面，也將延伸至 AI 算力、資料資源與模型安全等關鍵領域。

對台灣與其他中小型國家而言，此一趨勢意味未來網路安全政策必須同時強化 AI 防禦能力與 AI 安全治理，例如發展 AI 資安監測系統、建立自動化防禦平台，以及推動 AI 攻防演練與人才培育。此外，AI 模型與訓練資料安全亦將成為新國安議題，一旦 AI 自主化或代理化系統遭滲透或操控，極可能導致整體網路防禦體系出現系統性風險。整體而言，AI 導入將徹底改變網路戰爭運作模式，使未來網路衝突更接近一場以演算法、算力與資料為核心科技競賽。

## 二、公私協力防禦體系：數位時代的國家安全治理新模式

由於數位時代的關鍵資源掌握在民間手中，網路防禦已不再是政府單方面的職責，而是一場全民參與的集體行動。當對手發動大規模攻擊時，單靠政府的公權力已不足以覆蓋廣大的數位疆域，必須仰賴私營企業提供技術支援與第一線防禦，因此《戰略》主張透過激勵機制與法規精簡，建立「公私部門新水平關係」，以確保在和平與戰爭時期均能發揮聯合作戰的效能。

在此架構下，美國未來將透過多種機制深化公私合作。首先是建立更即時與制度化的威脅情報共享機制，使政府與企業能迅速交換攻擊資訊與漏洞情資，以縮短威脅偵測與回應時間。其次，政府透過政策誘因鼓勵企業主動參與網路防禦，例如提供法律責任豁免、財政補助或研發資金，以提升企業在資安領域的投資動機。第三，科技公司與資安企業未來可以直接參與國家安全任務，例如協助開發網路監測工具、AI 資安系統與關鍵防禦技術，甚至在重大事

件中提供技術支援。長期而言，此種合作模式將逐漸形成一個「國家級數位防禦生態系」，其中大型科技公司、雲端服務商與資安企業將扮演類似國防承包商角色，成為國家網路安全體系重要支柱。

另《戰略》提出美國政府將減少負擔沉重且效率低的監管規定，改以較具彈性的「常識性監管」(common-sense regulation)取而代之，以提升產業創新速度，代表對現行網路治理模式進行調整，從過去以「官僚合規」為主監管方式，轉向更具彈性的「敏捷治理」。這種去管制化並非完全放任市場，而是希望透過更靈活政策環境，使私人企業，尤其是新興科技公司與新創企業，能更快速開發網路防禦工具與新技術。

在此政策思維下，美國未來可以逐步建立類似「網路工業複合體」合作模式。政府與科技產業之間將形成更緊密且長期戰略夥伴關係，不僅在和平時期共同強化防禦能力，在危機或衝突情境中也能迅速動員產業資源參與防禦與反制行動。此外，政府亦可以透過法律調整，重新界定企業在網路攻擊情境中的權責，例如放寬企業在追蹤攻擊來源或協助防禦行動時的法律限制，使民間力量能在一定程度上參與國家防禦體系。然公私協力模式深化也可能帶來新治理挑戰，例如企業在網路反制行動中權限界定、資料隱私與監控爭議，以及大型科技公司在國家安全決策中影響力等問題。對台灣而言，由於科技產業高度發達且民間企業掌握大量數位基礎設施，建立類似公私協力資安體系將具有重要意義。透過政府、科技企業與研究機構之間協同合作，不僅能提升整體網路防禦能力，也有助在全球科技與資安競爭中維持戰略優勢。



# 中共黨報在共軍腐敗事件中的宣傳模式

梁書瑗

中共政軍與作戰概念研究所

焦點類別：中共黨政

## 壹、前言

習近平延任後，開始推進軍隊反腐作為，但在共軍將領落馬的案件中，可靠的訊息並不多。然而，中共黨中央又需藉由向外界釋放部分訊息，一方面收取震懾官僚、軍隊之效；另一方面藉以證明中共黨國體制有自我更新之能，反過來鞏固社會對體制的支持。<sup>1</sup>最重要的是，必須在高度爭議事件中，統一全黨上下的政治立場與口徑。在相關訊息不多的限制下，堅守「黨性原則」的黨報如何透過黨報傳遞將領落馬的訊息，便深具觀察價值。

在社會主義國家中，新聞事業必須為無產階級專政服務，但如何完成這個目標？第一，執政黨必須掌握宣傳高地，發展黨報、黨刊，主動營造有利於自身的輿論環境；其次，黨報、黨刊的編輯方針必須遵守「黨性原則」，意即「無條件服從黨的領導」，正確地向受眾宣傳黨的路線、方針、政策。<sup>2</sup>

本文以中共二十屆中央軍委領導班子落馬的將領（李尚福、何衛東、苗華、張又俠、劉振立）為主要對象，運用黨報必須遵守「黨性原則」的特性，從黨報：一、傳遞案件訊息時採用何種消息來源與稿件類型；二、如何轉載擴散相關訊息；三、如何編排新聞版面等角度觀察，說明中共企圖對外釋放何種訊息。

---

<sup>1</sup> 黃信豪，〈解析習近平反腐作為下民眾的政治心理：貪腐認知的類型建構〉，《中國大陸研究》，第67卷第4期，2024年12月，頁1-34。

<sup>2</sup> 郝雨、王艷玲，《新聞學概論》（上海：上海大學出版社，2003年），頁197-199。

## 貳、安全意涵

### 一、中共使用不同的稿件搭配傳播將領落馬的訊息

中共二十大以來，據官方正式宣布落馬的軍委委員，依序為：李尚福（2024/6/27）；何衛東、苗華（2025/10/17）；張又俠、劉振立（2026/1/24）。黨中央對外首次宣布上述將領落馬的消息各有不同的管道與搭配的稿件類型，如表 1。

表 1、二十屆軍委成員落馬的消息來源與搭配的稿件類型<sup>3</sup>

案情見報的時間	落馬將領	消息來源	稿件類型
2024/6/28	李尚福	新華社	1、新華社通稿〈中央軍委原委員、原國務委員兼國防部長李尚福受到開除黨籍處分〉
2025/10/18	何衛東	國防部新聞發言人	1、2025/10/18〈就近期涉軍問題發布消息並答記者問〉 2、2025/10/18 解放軍報社論〈堅定不移把軍隊反腐敗鬥爭進行到底〉（頭版） 3、2025/10/24 解放軍報社論〈堅定捍衛人民軍隊政治本色〉（二版） 4、2025/10/28 解放軍報本報評論員文章〈持之以恆推進全面從嚴治黨—四談認真學習貫徹黨的二十屆四中全會精神〉（頭版）
2025/10/18	苗華		
2026/1/25	張又俠	國防部新聞發言人	1、〈就近期涉軍問題發布消息並答記者問〉 2、2026/1/25 解放軍報社論〈堅決打贏軍隊反腐敗鬥爭攻堅戰持久戰總體戰〉（頭版） 3、2026/1/31 解放軍報本報評論員文章〈堅定反腐必勝、強軍必成的信念信心〉（頭版） 4、2026/2/1 解放軍報本報評論員文章〈持續深化政治整訓 縱深推進正風反腐〉（頭版）
2026/1/25	劉振立		

<sup>3</sup> 本文所討論的新聞稿件（包含社論與本報評論員文章）均以內文提及落馬將領為主。

		5、2026/2/2 解放軍報本報評論員文章〈以強烈的使命擔當攻堅奮進〉（頭版）
--	--	--

資料來源：作者整理繪製。

## 二、黨報間轉載稿件的模式隨著落馬將領不同而有差異

中共從中央到地方、各類由中共直接控制的群、團、單位，均有各自主辦的機關報，亦是本文所稱的黨報。本文所指稱的「黨報」分為三類：（一）中共中央或中央部會所主辦的機關報；（二）全國性群團組織的機關報；（三）地方黨報，各省、直轄市、自治區的黨委機關報。<sup>4</sup>不同的黨報有各自有負責宣傳的群眾與議題，以此建立起一個由黨主導的宣傳網絡。

黨報在傳播關於軍委成員落馬的稿件類型如前表 1，主要分有：（一）李尚福（及魏鳳和）案：新華社通稿〈中央軍委原委員、原國務委員兼國防部長李尚福受到開除黨籍處分〉；（二）何衛東、苗華案及張又俠、劉振立案：國防部新聞發言人〈就近期涉軍問題發布消息並答記者問〉（以下簡稱〈近期涉軍問題發布消息〉）；（三）《解放軍報》針對何衛東、苗華與張又俠、劉振立案所發表的社論與本報評論員文章。

然而，不同的案件在黨報間轉載的模式：轉載範圍、轉載時所使用的稿源、稿件轉載後的版面位置等也不盡相同，如表 2 所示。此外，表 2 並不包含地方黨報，因地方黨報在各案件相關稿件轉載的狀況不一，但未轉載的黨報居多。

<sup>4</sup> 第一，中共中央或中央部會所主辦的機關報，如《人民日報》、《解放軍報》、《光明日報》、《經濟日報》、《人民政協報》、《中央紀檢監察報》、《法治日報》、《中國組織人事報》、《人民法院報》、《人民公安報》、《科技日報》、《中國社會工作報》、《農民日報》等；第二、全國性群團組織的機關報，如《中國青年報》、《工人日報》、《婦女日報》；第三，地方黨報，各省、直轄市、自治區的黨委機關報，如上海市委機關報《解放日報》、北京市委機關報《北京日報》、山東省委機關報《大眾日報》、江蘇省委機關報《新華日報》。關於中共主要的黨報可參見：〈黨報黨刊〉，《求是網》，<https://www.qstheory.cn/v9zhuanqu/resource/dbdk/index.htm>。

表 2、黨報轉載各案件的模式

案件	稿件	轉載範圍	轉載時所使用的稿源	稿件轉載版面位置
李尚福	新華社通稿	解放軍報、人民日報、光明日報、中國紀檢監察報	新華社通稿	未固定
何衛東 苗華	〈就近期涉軍問題發布消息並答記者問〉	解放軍報、人民日報	1、解放軍報採本報記者發稿的方式。 2、人民日報採用新華社通稿。	未固定
	解放軍報社論	無	--	--
	解放軍報本報評論員文章	無	--	--
張又俠 劉振立	1、〈就近期涉軍問題發布消息並答記者問〉	解放軍報、人民日報、光明日報、中國紀檢監察報、工人日報、中國青年報、法治日報、檢察日報	1、解放軍報採本報記者發稿的方式。 2、其他黨報採用新華社通稿。	未固定
	2、解放軍報社論	人民日報、光明日報、中國紀檢監察報、經濟日報、法治日報、工人日報、中國青年報	1、解放軍報社論全文（含標題）照登。	固定在頭版的左側下方位置。
	3、解放軍報本報評論員文章	無	--	--

資料來源：作者整理繪製。

## 參、趨勢研判

### 一、黨報的消息來源、稿件類型根據落馬將領的身分序列而有差異

根據表 1，李尚福（以及魏鳳和）因擔任國防部長，雖是軍委成員，但亦屬國務院的行政序列，因此黨中央在通報李尚福（與魏鳳和）落馬的訊息時，甚至是中央紀委、國家監委官網上的通報，一律採用新華社通稿的方式對外發布並說明案情。反觀何衛東、苗華；張又俠與劉振立雖亦為軍委成員，但卻因未任政府部門職務，則相關消息統一由國防部發言人的系統藉說明近期涉軍問題的方式對外公布，並搭配《解放軍報》社論與本報評論員的文章說明涉案情節。

### 二、黨報間轉載稿件的模式隨著案件嚴重性、政治敏感性而有變化

對黨的喉舌而言，「黨性原則」在實踐層面上，便如《人民日報版面備要》一書所言，處理好重大案件的報導，是一個政治問題，要聽中央的招呼，堅決按中央的部署辦事。<sup>5</sup>因此，本文認為，外界可從黨報針對將領落馬的宣傳模式獲知中央的立場、態度。

在二十屆中央軍委成員裡面，身為習近平盟友的張又俠為排名第一的軍委副主席，再加上排名第四的劉振立（聯合參謀部參謀長）分管聯合作戰，兩人被認定違紀違法，則對中共中央的衝擊性可見一斑。但外界僅能從涉案人的資歷、職務為憑據來論證。事實上，雖然黨報在傳播何、苗及張、劉這兩個案子時，不論是消息來源或所搭配的稿件看來，並無二致（如表 2），但卻在黨報間轉載的範圍與版面安排中看出差異。

首先，從黨報轉載的範圍來看，相較之下，張、劉一案比何、苗一案，不管是在〈近期涉軍問題發布消息〉或解放軍報的社論與

---

<sup>5</sup> 人民日報編輯部，《人民日報版面備要》（北京：人民日報出版社，1997年），頁 355。

本報評論員文章，其轉載範圍更加廣泛。解放軍報關於何、苗一案的社論甚至並未有任何黨報轉載。顯示，對中央而言，張、劉涉案更具衝擊性，需要透過廣泛的轉載傳遞相關訊息給黨內受眾。由於解放軍報為中央軍委機關報，所刊登的社論立場直接反映中央軍委的立場態度，從目前黨軍關係看來，解放軍報的社論映照的應該就是習近平的意志。解放軍報頭版刊登針對張、劉一案的社論〈堅決打贏軍隊反腐敗鬥爭攻堅戰持久戰總體戰〉，堪稱對此案的定性。

對中共而言，歷來事涉共軍腐敗的訊息，政治敏感程度都極高。〈堅決打贏軍隊反腐敗鬥爭攻堅戰持久戰總體戰〉一文應該在宣傳部門的管控下，受到《人民日報》、《光明日報》、《經濟日報》、《中國紀檢監察報》、《工人日報》、《中國青年報》、《法治日報》、《檢察日報》等 8 份黨報轉載。從下表 3 可知，除了《解放軍報》以外，其他三份受中共中央管理的黨報——《人民日報》、《光明日報》、《經濟日報》，均在頭版全文轉載。除了受到中共中央直接影響之下的黨報以外，中共最重要的群團組織——工會與共青團，以及紀檢、政法、檢察系統的機關報亦身負轉載該文的任務。

其次，張、劉一案的政治敏感性更高也可從轉載稿件在不同黨報間的版面位置可知。因為只要是轉載張、劉一案的社論文章〈堅決打贏軍隊反腐敗鬥爭攻堅戰持久戰總體戰〉的黨報，其文章版面安排亦受到管控，均置於頭版左下側的位置。顯示這個案子的傳播效果需要被管理，而不能任由黨報自己下判斷。若根據版面位置的重要程度來說，黨報版面左下側的位子除了頭條以外最重要的版面區塊，<sup>6</sup>顯示，〈堅決打贏軍隊反腐敗鬥爭攻堅戰持久戰總體戰〉

---

<sup>6</sup> 關於黨報版面重要性的討論可見：寇健文、梁書瑗，〈中共領導人的權力消長在黨報新聞照片上的呈現〉，《政治科學論叢》，第 38 期，2008 年 12 月，頁 51-52。

一文，是各家轉載黨報在當天除了在各自負責的傳播領域以外最重要的文章。

表 3、轉載落馬將領訊息的主要黨報

	主辦單位	宣傳任務或受眾類型
《人民日報》	中共中央委員會機關報	中共黨員
《解放軍報》	中共中央軍委機關報	軍隊
《光明日報》	中共中央直屬事業單位、中宣部代管	知識分子
《經濟日報》	中共中央直屬事業單位、中宣部代管	經濟工作的重要輿論陣地
《中國紀檢監察報》	中紀委、國家監察委員會主管	反腐倡廉的相關指導思想、政策與工作方針
《工人日報》	中華全國總工會主管	服務職工群體與宣傳工會新聞的輿論陣地
《中國青年報》	共青團中央機關報	以青少年讀者為主要受眾引領青少年思想的陣地
《法治日報》	中央政法委機關報	中共在政法戰線的喉舌也是中央全面依法治國委員會及其辦公室的主要宣傳平台
《檢察日報》	最高人民檢察院主管	中國檢察機關的宣傳平台與輿論陣地

資料來源：作者整理繪製自各黨報官方網站所載訊息。



# 歐盟造船戰略下低排放與數位孿生的結合

賀增原

網路安全與決策推演研究所

焦點類別：國際情勢、能源安全

## 壹、前言

歐盟委員會於 3 月 4 日宣布一項支持歐洲造船業和港口發展的產業戰略，目的在提升歐盟造船業在全球市場中的競爭力，並推動海事產業的綠色轉型。此舉是歐盟推動再工業化和強化「歐洲製造」(Made in Europe) 戰略的一部分。<sup>1</sup>儘管目前全球造船產業由中國處於龍頭地位，根據中國工信部發布的數據，指 2025 年中國造船業的完工量、新接訂單量、手持訂單量都高居全球第 1，且連續 16 年都保持世界之冠。<sup>2</sup>然而，世界各國皆朝向綠色智慧船舶的發展，使產業核心競爭力正經歷從「低碳排」(Low Carbon) 演進到「低排放」(Low Emission) 的關鍵轉變。歐盟於 2025 年 1 月 1 日正式施行的 FuelEU Maritime 強制令正式生效，要求航運企業在燃油效率和低碳推進上做出決策。<sup>3</sup>除了二氧化碳 (CO<sub>2</sub>) 外，國際海事組織 (IMO) 在《國際防止船舶造成污染公約》(MARPOL) 附錄 VI 限制以下船舶廢氣中所含空氣污染物的排放：一、硫氧化物 (SO<sub>x</sub>)；二、顆粒物和氮氧化物 (NO<sub>x</sub>)；三、臭氧消耗物質 (Ozone-Depleting Substances, ODS)；四、揮發性有機化合物 (VOC)。<sup>4</sup>在此

---

<sup>1</sup> 安娜，〈歐盟推出造船業發展戰略：應對亞洲競爭 提升歐洲海事產業競爭力〉，《法國廣播電台》，2026 年 3 月 4 日，<https://www.rfi.fr/tw/%E4%B8%AD%E5%9C%8B/20260304-歐盟推出造船業發展戰略-應對亞洲競爭-提升歐洲海事產業競爭力>。

<sup>2</sup> 邱國強、朱建陵〈中國 2025 年造船完工及訂單量 連續 16 年居全球之冠〉，《中央社》，2026 年 2 月 1 日，<https://www.cna.com.tw/news/acn/202602010139.aspx>。

<sup>3</sup> “FuelEU Maritime Regulation Enters into Force,” *The Maritime Executive*, January 1, 2025, <https://maritime-executive.com/article/fueleu-maritime-regulation-enters-into-force>.

<sup>4</sup> “Clean Air in Shipping,” *International Maritime Organization*, <https://www.imo.org/en/ourwork/environment/pages/clean%20air%20in%20shipping.aspx#:~>.

低排放發展的背景下導入數位孿生技術不僅能帶動數位升級，更能精準驗證減碳成效，成為綠色轉型的核心手段。

## 貳、安全意涵

### 一、能源轉型下的動力系統革新

全球航運業在倫敦於 2025 年簽訂「淨零框架」(Net-Zero Framework) 協議，將導入全球首套國際碳定價體系，希望減少航運界所產生大量的溫室氣體。這項協議將於 2028 年起對溫室氣體排放徵收費用，迫使商船必須轉用清潔燃料以規避高額罰款。此項徵收碳費的協議，對於碳定價設定兩個排放目標：一個相對容易達到的基準目標，以及另一個旨在鼓勵使用更清潔燃料的更具挑戰性的目標。所以未達基準目標的船舶將面臨每噸二氧化碳最高 380 美元的罰款；達到基準排放標準但未達到更高目標的船舶，每噸二氧化碳排放量將被處以 100 美元的較低罰款；這兩項標準每年都會調整。<sup>5</sup>

傳統船舶動力系統皆是以柴油主機或者是燃氣渦輪機為主，不僅會產生大量二氧化碳同時會產生各式污染物，因此目前的船舶動力潔淨燃料將逐漸轉向氫、氨、甲醇等液態（船舶儲存狀態，氫氣一般是以高壓氣態壓縮氫氣為主），藉由動力燃料的轉變，搭配動力系統全面革新，例如：使用氫氣為燃料的燃料電池系統，搭配大型鋰電池組來形成電力平衡負載；或者利用雙燃料內燃機，可以靈活使用液化天然氣（Liquefied Natural Gas, LNG）和柴油，以發揮生態友好性與廣泛的使用性；<sup>6</sup>日本引擎製造商 Japan Engine Corporation

---

<sup>5</sup> “Global Shipping Faces New Carbon Rules but Emissions May Keep Rising,” *rfi*, April 14, 2025, <https://www.rfi.fr/en/environment/20250414-global-shipping-faces-new-carbon-rules-but-emissions-may-keep-rising>; 〈全球航運碳排放新規上路！航運業準備好了嗎？〉，《TCCiP 電子報》，2025 年 5 月 12 日，[https://tccip.ncdr.nat.gov.tw/km\\_news\\_one.aspx?kid=20250512004946](https://tccip.ncdr.nat.gov.tw/km_news_one.aspx?kid=20250512004946)。

<sup>6</sup> 〈船用發動機與柴油和天然氣燃料結合使用，具有更清潔的排放和更大的動力〉，

(J-ENG) 於 2025 年正式發表全球首台商業化「零碳」氨燃料引擎，同時預劃於 2026 年正式讓氨燃料貨船啟航，其最大的優點在於氨的分子結構是  $\text{NH}_3$ ，僅含有氮與氫氣，不含碳元素，所以在燃燒的過程只會產生氮氣與水，不會排放二氧化碳。<sup>7</sup> 中國大陸在擁有強大造船產能與國際合作之際，透過收購瑞士溫特圖爾的「氨引擎」技術 (WinGD, WinGD X-DF-A) 以及「甲醇引擎」技術 (WinGD, WinGD X-DF-M)，現在已經是中國船舶旗下的公司，其甲醇雙燃料內燃機已經於 2025 年安裝在貨櫃船市場。<sup>8</sup>

## 二、數位孿生對海事數據的掌握

船舶的設計從早期製圖桌的線圖到電腦輔助設計 (Computer-Aided Design, CAD)，造船工程師使用 AutoCAD、Tribon 或 AVEVA 等軟體，將製圖桌上的紙本線圖轉化為電腦裡的 3D 模型，這些存在伺服器內靜態的線圖與船體、艙裝、機電、管線等資料，隨著物聯網 (Internet of Things, IoT) 感測器技術與高頻寬衛星通信的普及，在這些科技的帶領下以歐洲供應商瓦錫蘭 (Wärtsilä) 為代表，確實地實踐將船舶即時數據回饋至虛擬模型「數位孿生」(Digital Twin)。該公司致力於「智能海洋生態系統」(Smart Marine Ecosystem)，透過在引擎、推進器和其他設備上安裝感測器，收集航行數據 (如燃料消耗、引擎性能、船殼壓力、海洋環境因素) 並回饋至虛擬模型，在模型當中可以了解船舶在海洋中航行狀況，藉以掌握預測性維修 (Predictive Maintenance) 與營運效能最佳化。<sup>9</sup>

---

《YANMAR》，[https://www.yanmar.com/tw/about/technology/vision1/dual\\_fuel\\_engine/](https://www.yanmar.com/tw/about/technology/vision1/dual_fuel_engine/).

<sup>7</sup> Chris，〈不是氫氣，是「氨」：全球第一台氨燃料商用船引擎即將在日本下水〉，《INSIDE 電子報》，2025 年 9 月 2 日，<https://www.inside.com.tw/article/39464-not-hydrogen-but-ammonia-world-first-ammonia-fuel-commercial-ship-engine-to-launch-in-japan>。

<sup>8</sup> 〈全球首發！我國自主研製世界最大功率甲醇雙燃料發動機交付〉，《我的鋼鐵》，2025 年 2 月 26 日，<https://news.mysteel.com/a/25022614/18257726D53790CF.html>。

<sup>9</sup> 《瓦錫蘭公司》，<https://www.wartsila.com/insights/article/it-s-easy-to-tell-these-twins-apart>。

這意味著，數位孿生涉及大量的船舶運行數據與設計參數，在「低排放」的定義下，船舶不僅監控油耗，同時需要模擬以下的狀況：

(一) 選擇性催化還原系統 (Selective Catalytic Reduction, SCR)：模擬如何精確噴灑尿素以消除 NO<sub>x</sub>；<sup>10</sup> (二) 甲烷逃逸模擬：透過數位模型優化引擎燃燒室設計，將未燃盡的甲烷降至最低；<sup>11</sup> (三) 碳捕捉系統 (Carbon Capture and Storage, CCS)：在船上模擬化學吸收過程，對 CCS 系統的熱經濟性和環境性能進行分析；<sup>12</sup> (四) 歐盟透過擴大「排放」的定義（納入甲烷、黑碳等），實質上拉高進入歐洲港口的限制門檻。所以中國手持訂單中的船舶若是僅能滿足「低碳」技術而無法提升「全維度低排放」，這些資產在未來 10 年內仍然面臨巨大的法規風險。因此利用數位孿生可以建立海事網路安全標準，防止核心技術數據外洩，並確保歐盟在虛擬造船領域的數據主權與智慧財產權。

## 參、趨勢研判

### 一、從「硬體製造」轉向「數位效能的管理」

因此研判未來船廠的核心競爭力將不再侷限於鋼鐵焊接、管線組裝與艙裝設計，而是軟硬體整合的能力。數位孿生將使船舶從「交付即結束」轉變為「全壽期性能的監控」，預測後續維修與軟體升級將成為造船業的新獲利模式。

隨著「萬物皆可連網」技術的提升，先進的船舶透過各式的感

---

<sup>10</sup> “Prediction for SCR Systems Performance Using 3D CFD Simulation: Aiming at SCR Development for Various Layouts,” YANMAR, [https://www.yanmar.com/global/about/technology/technical\\_review/2017/1005\\_4.html](https://www.yanmar.com/global/about/technology/technical_review/2017/1005_4.html).

<sup>11</sup> “Reducing Power Plant Greenhouse Gasses Using AI and Digital Twins,” NVIDIA. DEVELOPER, <https://developer.nvidia.com/blog/reducing-power-plant-greenhouse-gasses-using-ai-and-digital-twins/>.

<sup>12</sup> Engin Guler, Selma Ergin, “Thermo-economic and Environmental Performance Analysis of Carbon Capture and Storage Systems for Different Types of Ships,” *International Journal of Greenhouse Gas Control*, <https://www.sciencedirect.com/science/article/abs/pii/S1750583625001136>.

測器，就有如人體的神經一般，將實體設備（例如：動力引擎、大軸、減速齒輪、螺葉與船舵）安裝感測器連接到遠端監控，不僅可以做為安全性自動預警，也可以利用 AI 運算來預測零件何時會損壞達到預防性維修，避免船舶於大海中發生故障。例如，達飛海運（CMA CGM）的「導航支援中心」（Fleet Navigation & Support Centre）是一個全天候運作的專業平台，其特色在於結合資深船員的經驗與數位化工具，提供船隊航行路徑規劃、即時監控、燃油效率最佳化與安全警示，以確保全球航線的可靠性與環保目標。<sup>13</sup> 瓦錫蘭（Wärtsilä）開發的「船隊營運解決方案」（Fleet Operations Solution, FOS）是一個總部位於丹麥的 UltraShip 公司，利用雲端技術的整合平台優化其 18 艘液化石油氣（LPG）油輪船隊部署，透過蒐集船舶的航行規劃、氣象導航、燃料管理、船隊績效和船岸通信整合至單一數位化系統中，利用人工智慧（AI）、機器學習和大數據分析，協助航運公司調整最佳化船舶航線和航速，提高船隊營運效率、安全性並降低碳排放。<sup>14</sup>

## 二、數位孿生驅動下的「海事生態圈」重組

歐盟透過 FuelEU Maritime 等法規，正利用「數位孿生」技術與精確排放數據，建立一套全球造船新標準。藉由船舶整個全壽期不同階段排放數據的監控，尤其該法規要求船舶在歐盟港口營運停泊時，必須逐年降低其能源的溫室氣體強度，此也導致如前所述新造船（如 WinGD 的 X-DF-A 氫引擎）會在雲端建立一個「數位孿生」的系統，即時在不同負載（不同數量的貨櫃）、不同的海況與氣

---

<sup>13</sup> 《達飛海運》，<https://www.cma-cgm.com/local/taiwan-agencies>。

<sup>14</sup> “Wärtsilä Fleet Operations Solution to Optimise Performance of UltraShip’s Entire Fleet,” *Wärtsilä*, January 11, 2021, <https://www.wartsila.com/media/news/11-01-2021-wartsila-fleet-operations-solution-to-optimise-performance-of-ultraship-s-entire-fleet-2843315>.

候下量測實際排放數據，如果數據偏離法規要求的「淨零曲線」的條件，數位系統將會提前預警並提供最佳化的建議，以確保船舶公司不會因為數據造假或效率不佳而面臨歐盟的罰款。

本文的數位孿生不單指船舶，甚至涵蓋能源與港口設施，例如歐盟要求自 2025 年 2 月 1 日起，電池製造商須公開電池的碳足跡數據，自 2027 年 2 月 1 日起，均須持有「數位電池護照」(Digital Battery Passport, DBP) 結合物聯網 (IoT) 感測器與雲端平台的數位檔案，記錄電池的完整生命週期資訊，確保電池在設計、生產、使用、回收過程中都能被追蹤、透明化並符合永續目標，<sup>15</sup>如此該船舶方能在歐盟航線上取得「綠色標籤」。

最後則是港口基礎設施優化，亦即是「即時到港優化」(Just-in-Time Arrival, JIT) 它是一種港口與船舶協同的調度方法，藉由安排精準抵達港口的時間，避免船舶長時間等待進港，顯著降低燃油消耗、減少碳排放並提升港口效率。鹿特丹港是歐洲最大的港口，其宣布要引進 IBM IoT 技術和雲端平臺，不論是陸地與水下都建置物聯網感測器，將會蒐集各式各樣的資料流 (data streams)，包括：潮汐與潮流的水氣濕度和天氣氣象資料、溫度、風速與風向、水位高度，以及泊位的可用性和能見度等，如此將可以提供港務人員更有效率的決策，顯著達到低排放的境界。<sup>16</sup>

簡言之，數位孿生的定義已超越單一船舶，擴展至電池供應鏈與港口基礎設施。這種全方位的「數位與綠色生態系」正促使傳統

---

<sup>15</sup> 〈[數位電池護照] 歐盟新規正式上路，電池產業新紀元〉，《台灣鈣鈦礦研發及產業聯盟》，2024 年 3 月 24 日，<https://www.tpria.org/post/20240324001>。

<sup>16</sup> 王若樸，〈鹿特丹港開始打造 IoT 智慧港，目標是 2025 實現港內航運連網全自動〉，《iThome》，2018 年 2 月 12 日，<https://www.ithome.com.tw/news/121307>。

造船產業蛻變為高科技整合服務業，並重塑全球海事市場的競爭規則。

發行人 / 霍守業

總編輯 / 柯承亨

主任編輯 / 蘇紫雲 執行主編 / 吳宗翰

助理編輯 / 黃政勛、陳宥芯、林均蓉、賴達文、李虹宜