

對美軍聯戰準則 —《作戰安全》之研究

A Study on U.S. Military Operations Security (OPSEC) Doctrines

雷仲州 中校、簡睿宇 上校

提 要：

- 一、「作戰安全」係確保軍事行動成功並維持決策優勢的作戰能力。美國自「越戰」的「紫龍行動」研究起，即透過聯戰準則與國家政策，逐步建構完整制度，並落實作戰安全觀念，俾確保任務均能順利達成。相較國軍內部雖存在保密、反情報等既有程序，但缺乏對「作戰安全」系統化之探討，故瞭解美軍作法確實有其必要性。
- 二、2025年6月21日，美軍對伊朗實施「午夜之錘行動」，任務全程透過保密與欺敵作為，致伊朗防空與預警系統能力，均未能順利發現並應處，周邊國家亦無法發現異常，讓美軍順利對伊朗地下核設施進行打擊，凸顯「作戰安全」在任務成功中的關鍵角色。
- 三、臺海局勢持續嚴峻，國軍若仍偏重被動「訊跡管理」與行政保密，整體行動遭敵現代情監偵科技掌握機率將大增，亦不利任務執行；故透過對「作戰安全」流程之研究，能協助國軍在計畫階段主動識別關鍵資訊與弱點，採取反制措施，降低或混淆敵對我作戰意圖感知外，亦能強化決策優勢，提升防衛作戰能量。

關鍵詞：作戰安全、關鍵資訊、紫龍行動

Abstract

1. “Operations Security” (OPSEC) is a critical capability ensuring mission success and decision superiority. While the U.S. military has established a comprehensive framework through joint doctrine and national policy since “Operation Purple Dragon” during the “Vietnam War”, Taiwan’s Armed Forces still lack a systematic approach, necessitating an in-depth study of U.S. “OPSEC” mechanisms.
2. On June 21, 2025, the U.S. military executed “Operation Midnight Hammer” against Iran. Rigorous secrecy and military deception effectively denied Iranian air defense and early-warning systems, achieving total tactical surprise against underground nuclear facilities without alerting

neighboring nations. This underscores the decisive role of “OPSEC” in mission success.

3. Amid an escalating cross-strait threat environment, Taiwan’s current measures rely heavily on passive signature management and administrative secrecy, leaving military indicators vulnerable to modern enemy ISR detection. Researching the U.S. “OPSEC” process will enable Taiwan to proactively identify critical information and vulnerabilities during planning, implement countermeasures to deny or confuse enemy perception, protect decision superiority, and enhance overall defense capabilities.

Keywords: Operations Security (OPSEC); Critical Information; Purple Dragon

壹、前言

美軍強調的「作戰安全」(Operations Security, 以下稱OPSEC), 並非單純的行政管制或保密措施, 而是透過系統化的循環運作流程, 識別並管制關鍵資訊, 同時分析我方行動可被對手察覺之可觀測指標, 加上適當反制措施, 將能降低敵方利用已方弱點之可能, 進而達成任務。¹「OPSEC」的核心目的在維持指揮官決策循環之完整性, 並確保任務成功; 然在國軍內部實務認知中, 「作戰安全」泰半被認為僅單純之保密或反情報作為, 較缺乏對流程與聯合作戰準則體系之探討; 如由作戰效能面向觀察, 「作戰安全」強調識別並保護影響任務成敗之關鍵資訊, 防止敵方透過情報蒐集與分析掌握我方作戰意圖與行動時機。²再者, 由於現代戰場透明

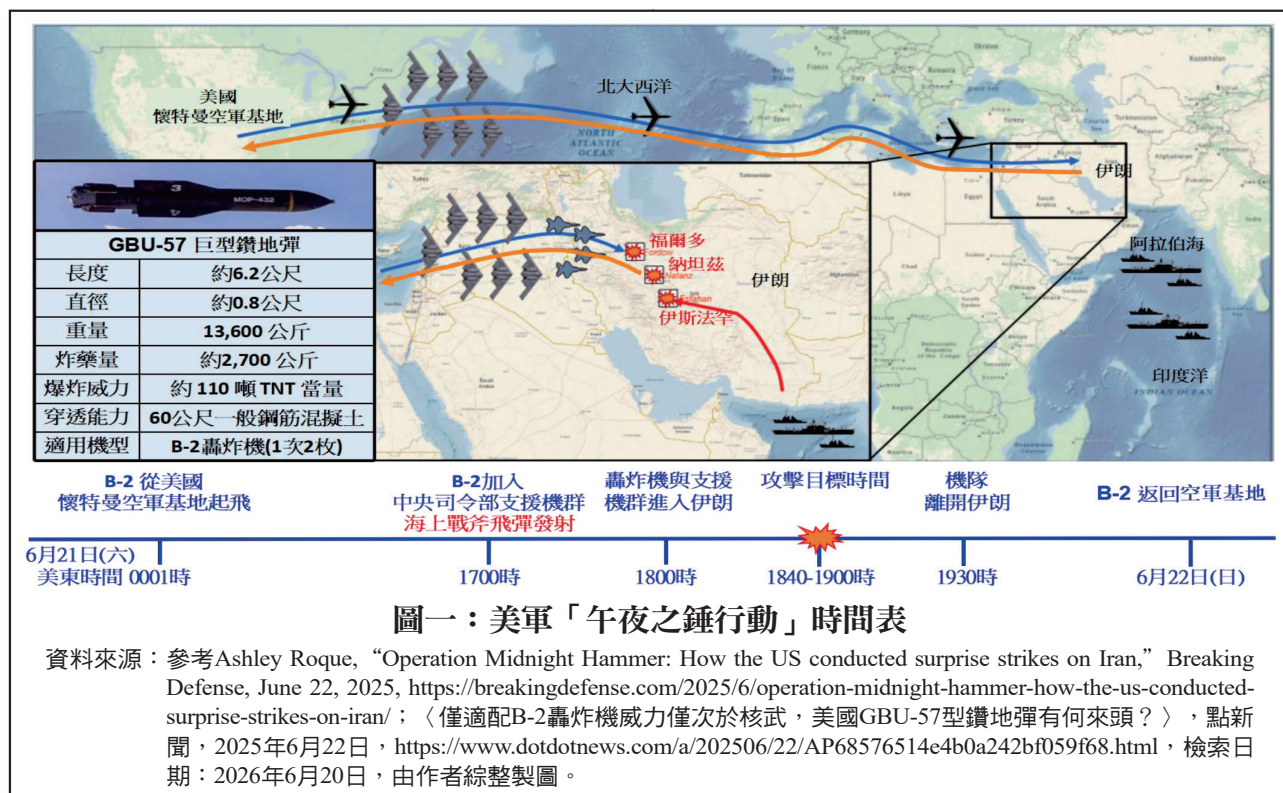
度大幅提升, 過往保密作為實不足以因應瞬息萬變之戰場環境; 故國軍必須從動態「訊跡管理」與混淆敵方著手, 方能透過散布戰場迷霧, 增加敵方誤判,³順利達成「作戰安全」之目的。

以2025年6月21日美軍對伊朗地下核設施實施「午夜之錘行動」(Operation Midnight Hammer)為例, 美軍在極度保密與欺敵作為下, 動員逾125架軍機、數十架加油機及攻擊潛艦, 使用約75枚精確制導彈藥對伊國3處核設施發動突襲。行動之初, 停泊於「阿拉伯海」(Arabian sea)之潛艦先對伊國伊斯法罕核設施發射約30枚「戰斧」(Tomahawk)巡弋飛彈; 隨後, 7架「B-2」隱形轟炸機對另2處核設施(福爾多與納坦茲)投擲14枚「GBU-57巨型鑽地彈」(以下稱GBU-57或鑽地彈), 美軍在僅25分鐘的攻擊窗口內, 精準命中所

註1: U.S. Joint Chiefs of Staff, “Operations Security,” Joint Publication 3-13.3, January 6, 2016, p.9。

註2: 同註1, 頁15。

註3: 沈育德, 〈淺談「訊跡管理」對軍事作戰之重要性〉, 《海軍學術雙月刊》(臺北市), 第58卷, 第5期, 2024年10月1日, 頁18~19。



有目標並成功撤離，全程未遭伊軍攔截與反制(如圖一)。⁴正是因為美軍成功管控攻擊行動時機的關鍵資訊，並透過欺敵、反制措施，使周邊各國情報機構事前皆未掌握相關跡象；伊朗甚至是在美軍完成攻擊後才驚覺行動已經結束，足見「作戰安全」在現代戰爭中占有的定位與份量。

任何軍事行動若無嚴謹之「作戰安全」作為，一旦行動徵候外洩，對手便可能轉移關鍵設施或強化防護措施，致而嚴重削弱行動，甚至面臨失敗風險。鑑於「作

戰安全」在任務行動中的關鍵地位，特別是美軍如何從經驗教訓、制度與準則層面構建此項能力，更值得深入探討。因此，本文從美軍在「越戰」期間對「OPSEC」的概念起源與發展著手，逐步釐清聯戰準則-《作戰安全》(JP 3-13.3 Operations Security, 以下稱JP 3-13.3)，⁵如何從傳統保密作為，轉變為主動的資訊安全與風險管控，並納入國家政策之歷程。其次，探討「作戰安全」在軍事領域的推展，分析其從建立訓練制度到準則體系發展，以

註4：“Secretary Hegseth And Gen.Caine Discuss Operation Midnight Hammer With Media,” Marianas Business Journal, June 23, 2025, <https://mbjguam.com/secretary-hegseth-and-gen-caine-discuss-operation-midnight-hammer-media>, visited date: 2026/6/20。

註5：《作戰安全》(JP 3-13.3)準則於2006年，調整至《資訊作戰》(JP 3-13 Information Operations, JP 3-13)準則體系之下，並將「作戰安全」納為資訊作戰的核心能力。同註1，頁4。

及如何進一步擴大至國防相關產業鏈。期許國軍官兵建立安全觀念、重視「作戰安全」作為，並延伸至相關國防事項上，共同提升任務成功機率，確保國家安全，這也是撰文主要目的。

貳、「作戰安全」概念之起源與發展

「作戰安全」(OPSEC)是一套動態的分析流程，其思維邏輯可以用一個因果鏈來說明，一方若無法有效管控「指標」，便會形成敵方可利用的「弱點」，最終導致「關鍵資訊」遭到外洩，進而影響任務成功。⁶有關美軍「OPSEC」由概念起源到發展成為國家政策過程，臚列說明如后：

一、「紫龍行動」緣起

「作戰安全」概念起源可追溯至「越戰」期間，當時美軍高層為釐清轟炸行動為何屢遭北越軍隊掌握，導致戰機損失，故由「參謀首長聯席會議」(Joint Chiefs of Staff，以下稱JCS)於1966年間啟動「紫龍行動」(Purple Dragon)，它是一項安全性評估與調查研究，並以敵方視角來檢視自身行動，並對資訊外洩問題進行分析；同步發覺敵方是如何在行動的計畫、準

備和執行過程中，透過各種管道獲取敏感資訊，之後再將分析結論，逐步發展成為完整「OPSEC」概念與程序。「越戰」後期，由於採取連串反制措施後，讓美方軍事行動逐漸展現成效，JCS遂將此方法全面推行至美軍各層級。⁷詳細說明如后：

(一)對「弧光行動」之檢討

1.1993年，「國家安全局」(National Security Agency，以下稱NSA)於《紫龍行動：美國作戰安全計畫的起源與發展》(Purple Dragon: The Origin and Development of the United States OPSEC Program)報告中指出，北越軍隊對美軍行動的預先掌握，非源於機密資訊外洩，而是透過多種情報來源與可觀測活動，再對美軍偵察行動與盟軍活動模式進行綜合分析，據以辨識特定作戰徵候，進而預測即將採取的軍事行動。例如美軍空襲前循特定模式，包括先進行空中偵察、之後空中活動增加，再由戰鬥機或轟炸機執行攻擊；隨著行動持續，北越軍逐漸能依據活動模式，推測某處將成為「弧光行動」(Operation Arc Light，指「B-52」轟炸機任務)轟炸的重要目標，從而提前分散部隊或轉移重要物資，降低損失。⁸

註6：M.Kubilay Akman, "OPSEC Model and Applications," Security Dimensions, No.25, 2018, p.7。

註7：DCMA Information Security, "OPSEC history: From ancient origins to modern challenges," U.S. Air Force Nuclear Weapons Center(AFNWC), January 5, 2023, <https://www.afnwc.af.mil/News/Article-Display/Article/3269169/opsec-history-from-ancient-origins-to-modern-challenges/>, visited date:2026/6/20。

註8：U.S.National Security Agency(NSA), "Purple Dragon: The Origin and Development of the United States OPSEC Program," February 6, 2008, p.78。

2. 除航空動態外，北越軍亦透過訊號情報蒐集，掌握部分盟軍作戰資訊，如截收美軍未加密的通信，包括火力支援、醫療後送需求等無線電發射，並從中推測部隊位置與可能的行動。另方面，某些重型火炮或空襲預警通信，甚至會在轟炸前數分鐘即被截收，使其能在有限時間內迅速採取躲避措施。⁹分析這些資訊多屬可被截收或觀測之訊號，而非純粹來自機密文件或內部洩密，這也凸顯「作戰安全」的重要性。

(二) 精進作法

1. 依「國家安全局」(NSA)報告內容，北越軍對美軍行動的預先掌握，僅係透過觀察軍事行動中可觀測指標與通信訊號，做為情報來源，並經由分析加以拼湊推導；因此，軍方有必要透過系統化機制識別並管制這些指標，避免敵方據以推斷關鍵資訊。此一概念遂成為美軍「作戰安全」理論發展的重要基礎。¹⁰

2. 美軍針對「OPSEC」之體認與實踐，不僅具備理論意義，更在戰場上展現出驚人的實戰效果。統計1966年12月美軍執行轟炸任務初期，北越的空襲預警平均時間約8小時，正確率約百分之三十四；當採取「作戰安全」反制措施後，至1967年

4月，北越軍對美軍空襲預警正確率已下降至約百分之五，預警時間更縮短至30分鐘以內。¹¹此一變化證實，透過對「作戰安全」的流程管控，能有效干擾敵方預判，不僅提升任務成功機率，更減少人員傷亡風險。

二、「作戰安全」納入國家政策

「越戰」結束後，「作戰安全」概念被美軍各級部隊廣泛採納與運用，且基於其對國家安全的重要性；1988年1月22日，時任美國雷根總統(Ronald W. Reagan)簽署《第298號國家安全決策指令》(National Security Decision Directive-298，以下稱NSDD-298)，明定凡執行或涉及國家安全任務，且包含機密或敏感活動的政府部門與機構，均須建立「作戰安全計畫」(OPSEC Program)，¹²有關「OPSEC」由軍事領域延伸至政府機關的具體推展作為，分述如后：

(一) 編組與執行機構調整

1. 美國為解決各行政部門因組織文化、業務屬性與保密習性不同，而導致標準不一與跨部會協調溝通管道不足等問題，1985年，成立「國家作戰安全諮詢委員會」(National OPSEC Advisory Committee，NOAC)，負責「作戰安全」議題，在《

註9：同註8，頁76。

註10：同註8，頁76~78。

註11：同註8，頁33。

註12：U.S. The White House, "National Operations Security Program," National Security Decision Directive Number 298, January 22, 1988, p.2。

NSDD-298》指令頒布前，整合跨部會意見、擬定《NSDD-298》草案、發展訓練標準與建立協調機制的過渡性安排。¹³

2. 考量各部會與情報機關均能確實貫徹「OPSEC」政策，1989年2月，美國正式編組「跨部會作戰安全支援署」(Interagency OPSEC Support Staff, 以下稱IOSS)，由「國家安全局」負管理指導，並由國安與情報相關部門派遣各領域專家進駐。透過舉辦「國家作戰安全會議」(National OPSEC Conference)等大型論壇，統籌協助各聯邦行政機關研擬「作戰安全計畫」，¹⁴成為美國將「OPSEC」自軍事領域延伸至國家安全韌性的重要樞紐。

(二)「冷戰」後的轉型發展

1996年4月，《作戰安全情報威脅手冊》(Operations Security Intelligence Threat Handbook)出版，揭示美國於「冷戰」(Cold War)結束後，將「作戰安全」由傳統軍事對抗，轉向政治、軍事、經濟、專利技術、智慧財產權與資訊科技等國家安全威脅，當時估計有超過100個國家正在對美國進行情報活動，進而開始重視公開資訊、開源情報、訊號情報與人員情

報結合，所可能形成之新型態風險。¹⁵手冊也提醒各機關在制定安全計畫時，須考量新型態的情報蒐集威脅，包含外國情報機構能力、內部滲透、系統遭駭等可能性外，亦須注意公共領域是否已出現導致關鍵資訊洩露之指標。¹⁶同時為因應科技所帶來的威脅與挑戰，遂將作戰安全觀念由各行政機關執行，逐步擴展為跨部會協調下的風險辨識與防護機制，並為後續整體風險管理奠定基礎。

(三)建立各部門「作戰安全」能力

隨著安全環境與威脅型態的演變，2021年，華府進一步將「作戰安全」納入跨行政部門間的國家安全機制，除發布《國家安全總統備忘錄第28號》(National Security Presidential Memorandum-28, 以下稱NSPM-28)，並建立「國家作戰安全計畫」(National Operations Security Program)。該備忘錄要求各行政部門建立「OPSEC」能力，以識別並保護關鍵資產、降低組織與系統弱點；並在風險管理過程中，納入對外國敵對勢力威脅評估，¹⁷以建構行政部門面對新威脅的安全韌性。

(四)「作戰安全」防護之擴展

註13：同註8，頁96~97。

註14：「跨部會作戰安全支援署」(Interagency OPSEC Support Staff, IOSS)，由中央情報局(CIA)、國防部(DOD)、能源部(DOE)、聯邦調查局(FBI)、聯邦總務署(GSA)及特勤局(USSS)等部門派員組成。參考U.S. Central Intelligence Agency(CIA), "First National OPSEC Conference," Document No.OS 89-8016, November 29, 1989, p.1。

註15：Interagency OPSEC Support Staff(IOSS), "Operations Security Intelligence Threat Handbook," April, 1996, <https://irp.fas.org/nsa/ioss/threat96/part02.htm>, visited date:2026/6/20。

註16：同註15。

註17：U.S. Office of the Director of National Intelligence, "National Operations Security Program," NSPM-28, October 22, 2021, p.1。

2021年，美國「國家反情報與安全中心」(National Counterintelligence and Security Center)依據《NSPM-28》授權，負責統一指導各行政部門發展「作戰安全」計畫外，同時亦提供計畫開發、教育與宣導教材。¹⁸若稱《NSDD-298》象徵美國建立國家級「OPSEC」制度的重要里程碑；則《NSPM-28》代表在此安全環境下，將其進一步整合至政府風險管理與反情報體系之中。此一政策不僅強化政府機構對敏感行動之保護能力，也擴展至關鍵基礎設施與供應鏈領域安全。

參、美軍「作戰安全」制度推展

「作戰安全」除在國家政策層面做出規範，其實踐核心仍在軍事領域，美軍不僅策頒「OPSEC」相關準則外，為落實平時執行的實務，更逐步建立系統化的教育訓練機制。以下針對其制度推展概況，分述如后：

一、制度建立與課程規劃

(一)早在1982年12月，「參謀首長聯席會議」即協調「國家安全局」(NSA)建立並維持一套「作戰安全」訓練課程，供軍、文職人員施訓；NSA亦據此研訂

「國家作戰安全課程」(National OPSEC Course)，並於1983年11月在「國家密碼學院」(National Cryptologic School，NCS)授課，¹⁹為專業化「作戰安全」訓練奠定重要基礎。

(二)「作戰安全」訓練採專人專責模式，並區分基礎與軍種專業訓練兩層，其中除「國防反情報與安全局」(Defense Counterintelligence and Security Agency，DCSA)提供「作戰安全意識」(OPSEC Awareness)線上基礎訓練外，²⁰各軍種與聯合單位亦設置專責機構並發展進階課程，如「國防大學」(National Defense University)所屬「聯合資訊學校」(Joint Information School)，就發展結合網路空間、社群媒體及資訊作戰的進階專業課程；²¹並透過專責單位實施系統化訓練，以確保官兵在複雜資訊環境中，具備識別並保護影響任務成敗之關鍵資訊的能力。

(三)美軍對「作戰安全」(OPSEC)之發展與重視，反映軍事思維從傳統保密朝向爭取資訊優勢的戰略轉型；整體制度演進亦由概念、制度、聯戰準則與納入資訊作戰，並由各軍種發布指令落實執行，這

註18：同註17，頁1。

註19：同註8，頁96。

註20：U.S.Center for Development of Security Excellence, “OPSEC Awareness for Military Members, DOD Employees and Contractors GS130.16,” <https://www.cdse.edu/Training/eLearning/GS130/>, visited date:2026/6/20。

註21：美國國防大學所屬聯合資訊學校，負責基礎課程；海軍由資訊部隊所屬之作戰安全支援小組任專責機構實施認證訓練；陸軍由資訊作戰主管單位施訓。



也逐步形成完整的「OPSEC」運作體系(如圖二)。

透過設立專責單位、編排獨立訓期與專業證照之教育模式，顯示美軍已將「OPSEC」視為一門需長期專業培養之能力，同時凸顯對其重視程度。

二、聯戰體系之初步整合

(一)聯戰準則-《作戰安全》之發展，最早可追溯至1973年發布之《作戰安全準則》(JCS Pub 18 Doctrine for Operation Security, 以下稱JCS Pub 18)，²²1980年代中期進入制度化。1984年起，三軍及海軍陸戰隊相繼發布軍種指令，將「OPSEC」概念轉化為部隊執行之作業程序；²³1991年「參謀首長聯席會議」(JSC)發布《聯合作戰安全準則》(JP 3-54 Joint Doctrine for Operations Security, 以下稱JP 3-54)，將其納入聯合作

戰功能內；1993年更頒布《聯合作戰安全指令》(CJCSI 3213.01 Joint Operations Security)，律定聯合軍事行動、軍種作戰行動、計畫、訓練、演習等軍事活動，均應將安全概念納入規劃與執行之政策指導文件。²⁴

(二)隨著科技發展與新型威脅(如電子戰及網路空間作戰)變化快速，美軍也逐步調整「作戰安全」定位。2006年撤銷《JP 3-54》，改納入《資訊作戰》(JP 3-13 Information Operations, 以下稱JP 3-13)準則體系下，並發布功能性分支準則《作戰安全》(JP 3-13.3)。此項改變顯示美軍對「OPSEC」領域之認知，已由單純的安全管理，轉變為資訊作戰下之運作機制。有關準則定位與修訂概要，摘述如后：

1. 美軍正式將「作戰安全」定位為

註22：該準則屬機密準則。同註8，頁107。

註23：空軍、陸軍均稱《作戰安全》(分別為AF 10-701, 1984、AR 530-1, 1985)；海軍為《作戰安全計畫》(OPNAVINST 3432.1A, 1985)；海軍陸戰隊為《海軍陸戰隊作戰安全計畫》(MCO 3070.2A, 1986)。

註24：《聯合作戰安全指令》從1993年頒布後，分於1997、2003、2008及2012年修頒，最新版本為《CJCSI 3213.01D》。參考U.S. Joint Chiefs of Staff, “Joint Operations Security,” CJCSI 3213.01D, May 7, 2012, p.7。

表一：美軍聯戰準則《作戰安全》修訂與相關演進概況表

年份	策頒準則名稱	內 容 概 要
1973	作戰安全準則 (JCS Pub 18)	首本「作戰安全」準則，建立基本概念與架構。
1991	聯合作戰安全 (JP 3-54)	◎納入聯合作戰「指揮與管制作戰」(C2W)架構。 ◎1994年，建立支援聯合作戰之「OPSEC」規劃程序。
1993	--	頒布《聯合作戰安全指令》，律定聯合軍事行動、軍種作戰行動、計畫、訓練、演習等，均應將安全概念納入。
2006	作戰安全 (JP 3-13.3)	◎納入資訊作戰架構；2012年，強化跨政府與跨組織規劃、提升資訊暴露風險意識。 ◎2016年，將軍事欺敵列為反制措施、納入「紅軍」支援規劃與評估。

資料來源：參考“Purple Dragon:The Origin and Development of the United States OPSEC Program,” U.S.National Security Agency,February 6, 2008, p.107; “Joint Operations Security,” U.S. Joint Chiefs of Staff,CJCSI 3213.01D, May 7, 2012, p.7; “JP 3-13.3 Operations Security,” U.S. Joint Chiefs of Staff,January 6, 2016, p.4; “JP 3-54 Joint Doctrine for Operations Security,” https://irp.fas.org/doddir/dod/jp3-54/3-54c_c1.htm, visited date:2026/6/20，由作者集整製表。

「資訊相關能力」(Information-Related Capability)，²⁵其核心不再僅限於傳統的保密或安全管理措施，而是將其納入資訊作戰整體架構，透過「資訊作戰小組」(Information Operations Cell)之協調整合，成為影響敵方決策與認知、塑造資訊環境，並維持我方決策優勢之關鍵工具。

2. 由該準則發展過程，已明確反映出「OPSEC」從獨立準則轉型為「資訊作戰功能性準則」的修訂與演進過程(如表一)；美軍在《聯合作戰》(JP 3-0 Joint Operations)準則中強調，「作戰安全」為支撐聯合作戰效能之關鍵因素，並與「軍事欺敵」(Military Deception)相互配合，為塑造戰場態勢、主動爭取決策優勢之重要機制。²⁶

三、「OPSEC」的擴大應用

(一)為強化整體國防體系之防護能量

，「國防部」(現已改名為戰爭部)於1999年11月29日發布〈第5205.02號國防部指令〉(DoD Directive 5205.2)，要求所屬機關、組織及承包商(含分包商)，在執行所有國防任務、功能、計畫與活動時，均須透過「作戰安全計畫」保護關鍵資訊。²⁷此舉將「OPSEC」制度由軍事作戰層面，進一步擴展至整體國防體系與相關承包商等產業鏈。

(二)美軍「作戰安全」制度係在戰場經驗、政策指導與組織運作的長期發展下逐步形成，並建立制度化的系統；其在訓練方面，已將概念轉化為標準化教育課程，由專責單位施訓，使官兵具備識別「OPSEC」指標、關鍵資訊與風險管理之能力。

整體而言，「作戰安全」觀念藉聯合作戰準則頒布，建立「由上而下」的制度

註25：同註1，頁10。

註26：U.S. Joint Chiefs of Staff, “Joint Operations,” Joint Publication 3-0, October 22, 2018, pp.178~179。

註27：U.S. Department of Defense, “Operations Security (OPSEC) Program,” DOD Directive 5205.02, March 6, 2006, pp.1~3。

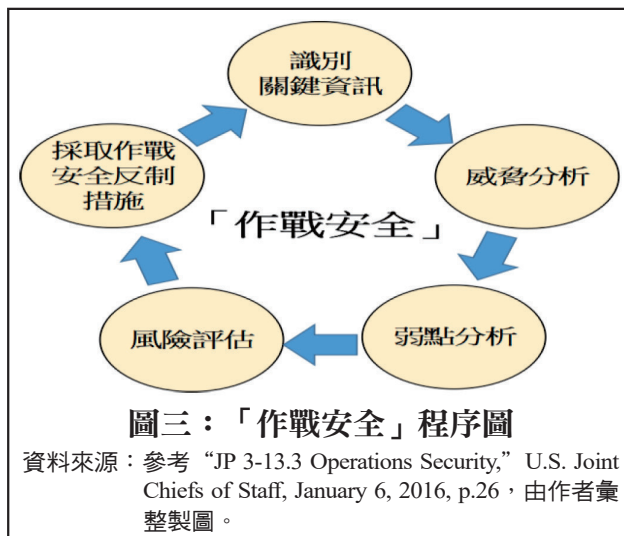
架構，引導各軍種形成一致作業標準；更在防護範疇上，延伸至「戰爭部」所屬機關與民間承包商，期透過整合概念、訓練與準則，使其成為美軍維持資訊優勢、確保任務成功的重要能力。

肆、美軍「作戰安全」程序分析

《孫子兵法》〈虛實篇〉提及「吾所與戰之地不可知，不可知，則敵所備者多；敵所備者多，則吾所與戰者，寡矣。」²⁸意指讓敵方無從知曉我方計畫與敵交戰的時間與地點，敵人將不分主次、處處設防，此即「備多力分」。此與美軍「作戰安全」之核心及準則規範應用高度契合；再結合反制措施、管控行動徵候與關鍵資訊，將使敵無法掌握我方真實意圖與主攻方向，並被迫採取全面防範，進而分散其情蒐能量與戰力，致有利我方於關鍵處，以相對優勢達成任務。由於「作戰安全」係一項系統化且循環的程序，步驟包含識別關鍵資訊等五項(如圖三)，²⁹摘陳說明如后：

一、識別關鍵資訊(Identify Critical Information)

(一)作戰安全首要在識別關鍵資訊，



同時隱藏我方意圖、能力與行動，不僅要識別重要資訊，亦需聚焦在重點防護；畢竟關鍵訊息若遭敵方掌握，將有助對手策劃並執行有效行動，危及我方安全。³⁰故透過各聯參與「OPSEC」人員協助，結合任務分析與作戰規劃，並識別有用資訊彙整成「關鍵資訊清單」(Critical Information List)，同時依美軍《作戰安全手冊》(Operations Security Program Manual)內容，按敵我雙方的重要性，評估其價值與等級(如高、中高、中、中低、低)，而非將所有資訊全面保密。³¹

(二)此清單並非一僵化不變的項目，隨著作戰階段與戰場環境變化，人員須持續檢視並動態做出內容修正，³²以確保其

註28：司馬志，《孫子兵法全書》(臺北市：華志文化事業有限公司)，2016年10月，頁129。

註29：同註1，頁26。

註30：同註1，頁25。

註31：U.S. Department of Defense, “Operations Security (OPSEC) Program Manual,” DoD Manual 5205.02-M, October 29, 2020, pp.22~24。

註32：同註1，頁24。

表二：美軍「午夜之錘行動」關鍵資訊與風險評估表

關鍵資訊清單	關鍵資訊價值	威脅值	我方弱點	目前風險
官方政治意圖	中高	中	中	中高
「GBU-57鑽地彈」	中高	中	中	中高
「B-2」動態	高	高	高	高
加油機動態	高	中高	高	高
護航戰機協同	中	低	中低	中

資料來源：參考「Operations Security (OPSEC) Program Manual,」 U.S. Department of Defense, DoD Manual 5205.02-M, October 29, 2020, pp.29~30，由作者彙整製表。

能反映當前作戰最具影響性的資訊。以美軍「午夜之錘行動」為例，依公開情資與戰果蒐整分析顯示，其從運用「B-2」機搭載「GBU-57鑽地彈」跨越北大西洋，攻擊約11,000公里外的伊朗核設施全程，摘整出包含官方政治意圖、鑽地彈整備、轟炸機、加油機動態(指「廣播式自動監視回報」【Automatic Dependent Surveillance-Broadcast，以下稱ADS-B】)³³以及護航戰機協同等5項(如表二)，並依任務階段區分不同等級，持續動態調整清單內容。

二、威脅分析(Threat Analysis)

(一)作戰行動需要情報體系支援，如「聯合情報準備」(Joint Intelligence Preparation of the Operational Environment，以下稱JIPOE)，實施情報、反情報與開源情報等資料彙整，並納入反情報人員組成「紅軍」(Red Team)，主動從敵方角度思考，發現我方及友軍忽視的洩

密管道；另結合關鍵資訊清單，研判敵方對各項資訊之蒐集能力與意圖強度，據以判定威脅程度。

(二)依《作戰安全》(JP 3-13.3)準則，此步驟需由作戰規劃人員與情報、反情報幕僚協同作業，並在「作戰安全規劃官」(OPSEC Planners)協助下，研析相關威脅問題。檢視美軍此次對伊朗核設施的攻擊行動，威脅項目包含伊國防空系統、伊朗意圖目標、持續發展核武建立區域性威懾、敵方協力者包含伊拉克什葉派武裝團體等(如表三)；進而再研判伊朗是否已掌握哪些關鍵資訊與目前掌握程度等，並分析其最可能與最危險行動方案，俾列入後續反制措施研擬之參考。

三、弱點分析(Vulnerability Analysis)

(一)分析前應先釐清「作戰安全指標」(OPSEC indicators)，亦即我方可能被敵偵知之行動或公開資訊、有可能讓敵方

註33：依美國「聯邦航空總署」(FAA)及「歐盟航空安全局」(EASA)規定，大型飛機必須開啟「廣播式自動回報監視」(Automatic Dependent Surveillance-Broadcast，ADS-B)訊號，透過內建的「全球衛星導航系統」(GNSS)傳輸飛機動態，提供地面站台及周邊航空器接收。參考蔡元鴻，〈ADS-B智慧化空中監視技術的演進與挑戰〉，《台灣好報》，2025年7月4日，<https://newstaiwan.net/2025/07/04/333843>，檢索日期：2026年6月20日。

表三：美軍「午夜之錘行動」威脅分析表

威脅問題	威脅評估分析
對手是誰？他的決策過程？	伊朗防空系統與防空部隊。
對手的目標？	伊朗持續透過核武計畫建立區域性威懾。
對手最可能和最危險的行動方案？	轉移核材料、威脅退出不擴散核武條約。
對手已經掌握了哪些關鍵資訊？	美軍加油機群異常調動、政治決策意圖。
對手的情報蒐集能力如何？	伊朗情報與安全部與聖城軍情報機構。
敵方之協力者為何？是否會分享資訊？其資訊傳遞管道為何？	國家有俄羅斯、中共、北韓、敘利亞等；組織如葉門胡塞武裝與黎巴嫩真主黨等。

資料來源：參考“JP 3-13.3 Operations Security,” U.S. Joint Chiefs of Staff, January 6, 2016, pp.26~28；UK Intelligence and Security Committee of Parliament, “Iran,” HC 1116, July 10, 2025, pp.15~17；Michele Gaietta, “Iran’s Nuclear Programme after the 12-Day War:Options and Challenges,” Istituto Affari Internazionali(IAI), July 15, 2025, pp.6~13，由作者彙整製表。

得以解讀或拼湊內容，進而可能讓對手推導出我方關鍵資訊；而我方行動中所暴露之「作戰安全指標」，讓敵方得以於有效時間內獲取並評估，據以支援其決策，形成對我方任務之威脅，此即「作戰安全弱點」(OPSEC vulnerability)。³⁴「弱點分析」的重點在反向檢視我方行動，依不同情報蒐集途徑進行檢視，例如人員、訊號、量測與特徵情報、地理空間與開源情報等，³⁵並辨識可被敵方蒐集、正確解讀利用之行為或作業。

(二)在空襲行動中，從關鍵資訊清單、伊朗情報蒐集視角，推導出極易暴露且會被伊方列為偵蒐重點的可觀測指標，包含政府公開對話、重型載具調度、轟炸機、大型機群之「ADS-B」訊號與異常通信流量等5項(如表四)。進一步對比伊朗情報蒐集能力，如空中加油機航跡可於公開

平台即時追蹤，形成顯著後勤指標；若伊朗藉此推斷美軍運用「B-2」機採取軍事行動企圖，勢必影響任務成效。

四、風險評估(Risk Assessment)

(一)由指揮官與參謀共同評估各項反制措施對作戰之影響(如時間、資源、兵力、人員負荷或對其他作戰活動之干擾)與成本，並與敵方成功利用該弱點，將對任務造成之損害進行比較；加上整合情報蒐集資訊與預期損失程度，以判定風險等級，都能做為後續反制措施之依據。換言之，風險評估並非消除風險，而是支援指揮官進行取舍，部分風險可能因任務需要必須承受；因此，指揮官須在效益與風險間做出判斷，並核定相應之反制措施。³⁶

(二)依《作戰安全手冊》內容，風險不是隨機產生的，而是價值、威脅與弱點三者交織的結果；故風險等於關鍵資訊價

註34：同註1，頁25。
註35：同註31，頁20。
註36：同註1，頁29。

表四：美軍「午夜之錘行動」弱點分析表

作戰安全指標	作戰安全弱點評估
政府公開對話決策層級言論	國家元首之對外言論、政府官方對外談話、外交立場等，可成為伊朗推論美軍採取行動之線索。
重型載具調度與彈藥掛載特徵	鑽地彈體積龐大且吊裝程序特殊，其後勤調度無法完全實施物理遮蔽，即可能成為作戰安全指標。
「B-2」機動態	「B-2」數量稀少、基地固定，任何異常調動或活動，可由開源情報、航空迷社群或商業影像掌握，以及基地人車異常進出。
大型機群飛航訊號	加油機於跨區域飛行時依法需開啟「ADS-B」訊號，使其航向與集結區域可被公開平台即時追蹤。
指管與無線電通信異常流量	轟炸機隊須仰賴大批戰機支援，多種整合之指管與通信衍生通信流量異常特徵，有助伊朗分析行動規模。

資料來源：參考Joseph Rodgers, “What Operation Midnight Hammer Means for the Future of Iran’s Nuclear Ambitions,” Center for Strategic and International Studies(CSIS), June 23, 2025, <https://www.csis.org/analysis/what-operation-midnight-hammer-means-future-irans-nuclear-ambitions>; David Vergun, “Defense Agency Contributed Toward Operation Midnight Hammer Success,” DOD News, July 10, 2025, <https://www.war.gov/News/News-Stories/Article/Article/4240876/defense-agency-contributed-toward-operation-midnight-hammer-success>, visited date:2026/6/20，由作者彙整製表。

值、敵方威脅與我方弱點三者加乘而得的「邏輯公式」。³⁷透過此公式評估美軍行動風險屬「高」的關鍵資訊，包含「B-2」機與空中加油機動態等2項(同表二)。

五、採取「作戰安全」反制措施(Apply Operations Security Countermeasures)

(一)採取反制措施是「OPSEC」的核心，透過具體行動阻止敵方情報蒐集，或藉由欺騙手段使敵方對關鍵資訊與作戰指標產生錯誤判讀；亦可選擇承受風險不做反制。反制措施之決策邏輯係依據前述風險評估，進行成本與損害效益比較，如選擇反制所需付出之代價高於敵方利用該弱點可能造成之損害，則該措施不具成本效益；若不反制，則等同需承擔敵方可能利

用該弱點所帶來之風險。故準則內容強調相關反制措施須經指揮官核定，以降低任務風險；另若發現風險無法降低，可能需要投入更高成本之反制措施，或者是調整原計畫。³⁸

(二)從決策過程顯示，「OPSEC」並非單純之保密機制，而是一種結合風險承擔、資源配置與作戰目標之動態管理能力。為有助瞭解反制措施之決策過程，經參考《作戰安全手冊》風險評估流程範例，³⁹推斷美軍行動所擬之反制措施與達成效益，以及行動如何影響伊朗對相關資訊之判讀(如表五)。例如針對初始風險「高」的轟炸機與加油機動態，美軍透過編組佯動誘餌與對開源情報網餵養假資訊等反制措施，順利將剩餘風險降至「中低」，也

註37：同註31，頁29~30。

註38：同註31，頁30。

註39：同註31，頁29~30。

表五：美軍「午夜之錘行動」反制措施一覽表

關鍵資訊	威脅分析	初始風險	反制措施	剩餘風險	達成效益
官方政治意圖	開源情報人員情報	中高	0619日白宮宣布「2週內決定是否打擊」，用斡旋掩蓋突襲。	低	誘導外界美方無行動意圖。
GBU-57鑽地彈	地理空間情報	中高	將彈藥移出與掛載作業，集中於夜深人靜時段執行。	低	阻斷基地周邊人員觀測。
B-2機動態	訊號情報	高	派6架編組佯動誘餌飛往關島，主攻7架利用夜間發航。	中低	誤導及引誘情報資源錯置。
空中加油機動態	訊號情報 開源情報	高	行動前6日派出逾20架加油機東飛，餵養假資訊。	中低	以虛掩實。
護航戰機整合	量測與特徵情報	中	運用低軌衛星提供通信與精準定位導航數據。	中低	阻斷伊朗訊號偵測。

資料來源：參考“Operations Security (OPSEC) Program Manual,” U.S. Department of Defense, DoD Manual 5205.02-M, October 29, 2020, pp.29~30；蔡元鴻，〈戰場迷霧：B-2關島佯動與「午夜之錘」剖析〉，蕃薯藤新聞，2025年6月25日，<https://n.yam.com/Article/202506252478771>；Mikayla Easley, “EXCLUSIVE: Space Force’ s role in Iran, Venezuela raids fueling push for more resources,” February 22, 2026, <https://defensescoop.com/2026/02/22/space-force-role-iran-venezuela-raids-fueling-push-for-more-resources>，檢索日期：2026年6月20日，由作者彙整製表。

成功主導伊朗迫使其在真假難辨的訊號中，錯失防禦先機，讓美軍得以無預警成功地對伊朗核設施實施突襲。

美軍「午夜之錘行動」成功的主因，係不斷檢視「OPSEC」行動的程序，並打破傳統靜態、被動之行政保密框架，轉化為動態的作戰機能，據以提供決策層級實施風險取舍與反制；加上並非消極地全面封鎖資訊，而是主動管理並引導敵方所能觀測的訊跡，此種因故意暴露而轉化成對敵的戰術迷霧，反而形塑戰場有利態勢，並為最終軍事行動成功提供重要助力。

伍、國軍強化「作戰安全」之建議

「作戰安全」並非靜態與被動的行政保密；而是一項攸關軍事行動成功與否的主動機制。當前中共成立的「信息支援部隊」，即是運用科技裝備來蒐集我方各類訊跡；這也凸顯敵方的情報蒐集觸角已延伸至我國社會網絡、民間組織及社群媒體等非軍事領域，致使官兵日常的數位足跡暴露，極易遭敵有系統地蒐集、拼湊與大數據解讀，形成軍隊的「作戰安全弱點」。⁴⁰故「國家安全局」揭示中共滲透的「四大手法」與「五大管道」，⁴¹確實值得國人警覺留意。

再者，國軍現行之保密機制，若仍停留在傳統防堵洩密與靜態公文書管制，恐難以有效應對新型態的科技偵蒐與訊跡暴

註40：〈中共網軍？「信息支援部隊成立」 習近平：全新戰略性兵種〉，《自由時報》，2024年4月19日，<https://news.ltn.com.tw/news/world/breakingnews/4646934>，檢索日期：2026年6月20日。

註41：「四大手法」為透由退役拉攏現役、網路勾聯、金錢利誘與債務脅迫；「五大管道」為利用黑道幫派、地下錢莊、掩護公司、宮廟團體及民間社團。李育材，〈軍人成共謀比例上升 國安局曝中共滲透4大手法、5大管道〉，《鏡週刊》（臺北市），2025年1月12日，<https://www.mirrormedia.mg/story/20250112soc012>，檢索日期：2026年6月20日。

露；且我方在作戰規劃過程中，泰半關注偽裝與隱(掩)蔽，鮮少將欺敵的「OPSEC」反制措施納入作戰方案中，確實亟待升級強化。謹以研究心得提出強化建議，期能做為提升國軍「作戰安全」觀念之參考，說明如后：

一、行動納入主動欺敵戰術

「OPSEC」的最高境界，絕非消極的躲藏，而是主動形塑有利戰場態勢、誘導敵人犯錯的戰術工具。美軍在「午夜之錘行動」中，透過空中加油機提前東進大西洋釋放模糊航跡；加上調動部分「B-2」轟炸機向西佯動、配合官方社群平台上的資訊操作，成功誘導伊朗情報機構錯置其偵蒐資源，才能順利達成零預警打擊任務。⁴²再以「二戰」末期在法國的「諾曼第登陸」(Normandy Landings)行動為例，盟軍於登陸前夕，透過「堅忍行動」(Operation Fortitude)虛設「美軍第一集團軍群」(First United States Army Group)與空降師等主動欺敵作為，成功誤導德軍研判主要登陸點位於挪威與法國加萊，致德方錯置防禦資源，讓盟軍順利登陸並奪取戰術主動。⁴³因此，國軍可增加「以真似假」的演訓規劃，說明如后：

(一)編組佯動部隊與欺敵假陣地

鑒於國軍重要軍事目標、指管節點與戰術營區周邊，極易潛藏敵特工、在地協力者或開源情報刺蒐網，常態性監控我軍任務動態。故於防衛作戰各階段，各級指揮官可編組戰術佯動部隊，透過異時、異地、多線之不規則機動，並規劃多組由營區至臨戰陣地之主、次要預備路線，破壞敵方情報鏈之觀測週期，使其無法掌握主戰兵力真實位置與動態；或借鑑「俄烏戰爭」中之誘敵武器，運用主戰裝備模型、充氣載具與無人機誘餌等手段欺騙共軍，以消耗敵彈藥與資源。⁴⁴

(二)多重戰力保存節點

單位應規劃多處備用陣地，由指揮官依當前情勢，臨機選特定地點設置欺敵的戰力保存節點，派遣非必要之運輸車輛，運載仿實資材(如空彈藥箱)進行高調的兵力調度，或於欺敵陣地常態性實施電磁輻射發放與開設偽裝設施，或透過物理與技術訊跡之人工調製，誘導敵方情報系統與潛伏人員回報錯誤情資，混淆、誤導敵之鑑別與辨識，除掩蓋我方主要戰力部署動態，並誘使敵方指揮官基於錯誤情資做出誤判，俾達成主動欺敵效果。

註42：章倩萍，〈兵不厭詐/美國多重欺敵戰術奏效 伊朗與全世界都未監測到〉，客新聞，2025年6月23日，<https://hakanews.tw/2025/06/23/207356>，檢索日期：2026年6月20日。

註43：李振林，〈由諾曼第登陸嚴格保密防護-論強化國軍保密防諜作為〉，《步兵季刊》(高雄市)，第292期，2024年5月，頁28。

註44：維塔利·舍甫琴科(Vitaly Shevchenko)，〈充氣坦克與 裝火炮：烏克蘭戰爭中的誘敵武器揭秘〉，yahoo!新聞，2025年9月7日，<https://tw.news.yahoo.com/充氣坦克與 裝火炮-烏克蘭戰爭中的誘敵武器揭秘-062557474.html>，檢索日期：2026年6月20日。

二、建構完備「作戰安全」訓測機制

(一)美軍將「作戰安全」定位為資訊相關能力之一，並在各軍種和聯合單位編設專責機構實施系統化培訓；反觀國軍目前多由政戰官科或保防幹部兼任涉密安全審查，較缺乏從作戰規劃角度出發的專業參謀。故可參考美軍設置專責「作戰安全規劃官」(OPSEC Planners)，並於進修教育與深造教育中規劃納入「作戰安全意識」基礎課程，選定訓練機構增設獨立「OPSEC」進階班隊或併入與作戰訓練有關之專業班隊施訓，培養具備戰術與情報整合能力的專職人員，以利後續納入各聯合作戰指揮體系的規劃架構中。

(二)此外，可將「資通電軍」與「軍事情報局」等專業單位聯合編組納入演訓「紅軍」，模擬敵方於地理空間情報與訊號情報情蒐手段，在無預警狀態下對國軍各演訓區域、飛彈陣地與雷達站等進行逆向偵測，透過實地的訊跡捕捉，發覺部隊在掩蔽、偽裝與發射管制上的真實弱點，進而改善並精進補強。

三、落實數位覺察文化

(一)2026年6月9日，俄羅斯國防部掌管火炮與飛彈彈藥的高階幹部突遭汽車炸彈暗殺。經調查，其行踪遭精準鎖定之原

因，竟是其子在社群平台上分享與父親車輛的合影，導致車牌與地緣關係等關鍵資訊外洩所致；⁴⁵此案例，充分顯示當前「訊跡管理」的範疇已不再侷限於傳統營區內。加上中共近年全面性運用大數據與人工智慧(AI)，讓國軍官兵日常暴露之數位足跡與部隊可觀測指標(如社群媒體發布單位活動照片等)，均可能遭敵利用人臉辨識系統，搜尋資訊進行拼湊或滲透行動。此外，國軍當前持續加強營區內的資安管控，但官兵使用的智慧手機、穿戴式裝置及社群媒體，在無意間產生大量的非機密數據，已成為敵方無風險刺探部隊動態的核心管道；故應教育官兵使用時應以「不揭露、不標示」為原則，方能建構「由內而外」的訊跡防護機制。

(二)「美國空軍指揮與參謀學院」(Air Command and Staff College)研究指出，在21世紀多元感測器滲透的資訊環境下，倘若「作戰安全」的反制防護僅侷限於職務或公務環境，將完全無法有效遏止資訊外洩；故防護網必須向外延伸至官兵之私人領域。⁴⁶因此，國軍應建立常態化之數位覺察教育機制，使基層官兵深刻體會個人私領域不應成為國軍整體任務安全之危害，營外的團體休閒活動紀實，更應

註45：吳宜錡，〈俄羅斯高階軍官開車一半遭炸死！全場疑被兒子1張照片出賣〉，鏡報，2025年6月11日，<https://today.line.me/tw/v3/article/vXanqJ3>，檢索日期：2026年6月20日。

註46：Adanto A.D' Amore, Major, "Air Force Operations Security in the Twenty-first Century: An Unaddressed Vulnerability," Wright Flyer Paper, No.87, August, 2022, pp.9~13。

避免於社群媒體公開後，成為數位足跡，演變為大數據的資料庫。此外，亦應教育官兵嚴格管控演訓期間之地理位置，防止敵方利用開源數據拼湊出部隊戰力保存位置、重要陣地輪廓與人員進出規律，俾杜絕任何的私領域數位足跡外洩。

陸、結語

美軍之所以能在戰略、戰役、戰術與技術層面持續落實「作戰安全」，關鍵在於其長期制度化與法制化所建構之完整體系，並已建立涵蓋國家、作戰區、軍種及部隊等不同層級之制度與訓練體系，使「OPSEC」不僅具備制度化的持續性與一致性，亦能因應不同作戰環境需求靈活調整。透過系統化之程序，得以有效識別關鍵資訊、評估敵情威脅、弱點分析、風險評估並採取適切反制措施，顯示「作戰安全」確已成為指揮官軍事行動規劃與執行中，不可或缺之作戰能力。

當前臺海局勢日趨嚴峻，中共持續藉由新興科技建構情監偵網絡，致使我防衛戰場呈現前所未有之高透明度。我軍在武器裝備硬體上，雖戮力籌建「不對稱」反制能力；倘若在資訊環境中無防範作為，將使私人領域數位足跡與部隊可觀測指標，遭敵方進行拼湊與大數據解讀，反而影響戰力發揮與部隊安全。換言之，國軍作戰任務的保密思維應由靜態保密，轉型為

主動風險管控與反制，以提升保密效能與作戰韌性。

國軍亦應借鏡美軍任務經驗，將「OPSEC」理念由保密管理層次，提升至作戰規劃與任務執行環節。除持續深化反情報教育、落實「訊跡管理」與人員保密等基礎作為外；更應自作戰計畫研擬階段，即循其程序識別各作戰階段的關鍵資訊，同時結合情報與反情報幕僚，持續進行威脅分析。另方面，各單位同步檢視我方可能暴露之「作戰安全弱點」，透過風險評估提出可行之反制措施，以降低我方作戰意圖與行動之可預測性，提升整體聯合作戰行動之隱蔽與安全。對政府及國防事務單位而言，亦應參考此等作法，審慎評估作業細節，將「作戰安全」管控納入與我國國防自主中相關產業鏈合約支援協定規範中，俾將關鍵資訊防護思維與國軍建構「不對稱」戰力進行鏈結，不僅強化決策優勢，同時提升防衛作戰能量。 

作者簡介：

雷仲州中校，陸軍軍官學校97年班，國防大學陸軍指揮參謀學院109年班，國防大學戰爭學院115年班。曾任連長、營長、憲兵指揮部計畫處副處長，現服務於憲兵指揮部。

簡睿宇上校，空軍軍官學校93年班，美國空軍指揮參謀學院106年班，美國國家戰爭學院114年班。曾任作戰官、訓練官、駐外空軍副武官、空軍第34反潛作戰中隊中隊長，現服務於國防大學戰爭學院。