敵明我暗：多領域軍事欺敵之道*

Leveraging Multi-Domain Military Deception to Expose the Enemy in 2035

取材：美國《軍事評論》雙月刊，2021 年 3－4 月號

Military Review, March-April 2021

作者：美國陸軍中校 **Stephen Pikner**

譯者：劉宗翰

The operational problem facing the Army in the year 2035 will fundamentally differ from problems it has previously confronted. The legacy challenge for which the Army’ s current platforms and doctrine are still optimized was a problem solved by breaking the Soviets’ second echelon of assault forces with precision long-range fires, fixed-wing air interdiction, and deep strikes by rotary-wing attack aviation. Today, and more so in 2035, the United States’ emerging great-power competitors pose an entirely different challenge. By threatening U.S. access into a theater and denying the assembly areas needed to stage for a decisive counterattack, U.S. adversaries have undercut America’ s preferred, expeditionary way of war. This anti-access/area denial （A2/AD） approach hinders the ability to effectively respond to rapid, limited aggression, which leaves allies and partners vulnerable to a wide range of coercive and subversive activities. Central to A2/AD is a well-defended, redundant, and largely hidden network of sensors and shooters that can locate, target, and strike friendly forces moving into and staging within a theater of operations.[2] To meet this challenge, the Army must adopt a novel approach to finding and fixing the critical components of an adversary’ s A2/AD complex to ensure freedom of action in 2035.

*屬於公開出版品，無版權限制；本文榮獲 2020 年威廉・杜普伊（William Depuy）上將徵文比賽佳作。

Foreword

前言

美國陸軍在 2035 年面臨的作戰問題將澈底不同於以往。**過往美陸軍武器載臺與準則面對的主要挑戰，是如何有效因應蘇聯第二梯隊突擊兵力所具備的精準長程火力、定翼機空中阻絕及旋翼機空中深度打擊等能力。時至今日，甚至展望 2035 年，美國將面對截然不同的挑戰：新崛起的大國競爭者。美軍會在敵情威脅下進入戰區，還會面臨敵人阻斷可以發動決定性反攻的集結區，這種作為將足以擾亂美軍以往慣用的遠征作戰模式。敵「反介入/區域拒止」可以阻止美方快速有效之應變能力、形成有限侵略態勢，從而讓美方盟國與作戰夥伴大量暴露於敵情威脅的環境下。[1]「反介入/區域拒止」本質屬於防守力強、大量隱藏分散的偵攻一體系統，可以定位、鎖定並打擊美方派赴作戰區馳援的我軍部隊。[2]為了因應此種挑戰，美陸軍須採取新方法來找出並打擊敵「反介入/區域拒止」的關鍵弱點，以確保未來（在 2035 年時）作戰行動之自由。

Finding the key nodes of an adversary’ s A2/AD network in 2035 requires an inversion of the traditional logic of reconnaissance. While cavalry squadrons and regiments can effectively fight for information on the disposition of advancing enemy echelons, finding the critical components of an integrated A2/AD complex is an altogether different issue. Rather than exposing vulnerable friendly forces as they methodically seek out a largely static and well-camouflaged adversary with fire and maneuver, future land forces can provoke an opponent into unmasking the long-range sensor and strike assets central to its A2/AD system by leveraging multi-domain military deception. In particular, this stimulation of an adversary’ s targeting and strike complex must consider how artificial intelligence （AI）-informed decisions will be made. In the near future, America’ s opponents will likely use such automated systems to fuse a wide range of information into targeting proposals for human decision-making. By triggering the premature activation

** 譯者註：2019 年美陸軍現代化戰略(Army Modernization Strategy)文件指出，陸軍多領域作戰所望目標是在 2028 年具備多領域作戰能力，在 2035 年完善多領域作戰能力。因此，本文才以 2035 年的時間點作為論述依據。

[1] Andrew J. Duncan, “New ‘Hybrid War’ or Old ‘Dirty Tricks’? The Gerasimov Debate and Russia’s R esponse to the Contemporary Operating Environment,” *Canadian Military Journal* 17, no. 3 (Summer 2017): 6–11.

[2] Wilson C. Blythe Jr. et al., *Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study* (Fort Leavenworth, KS: Army University Press, 2020), acc essed 20 October 2020, https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNG W-Unclassified-Summary-Report.pdf?ver=2020-03-25-122734-383.

and deployment of an adversary’ s high-value assets in its attempt to find, fix, and strike phantom American targets, multi-domain military deception can be central to an integrated effort to find and destroy the enemy on future battlefields.

未來在 2035 年時要找出敵「反介入/區域拒止」網絡的重要節點，所需的是不同於傳統偵察的邏輯思維。雖然騎兵中隊和團級部隊可以有效對抗敵前進梯隊，但找出整體「反介入/區域拒止」體系的關鍵弱點則又是另一回事。為了不讓我軍暴露弱點，必須想方設法找出火力與機動力兼具的蟄伏偽裝之敵；未來地面部隊應運用多領域軍事欺敵之道，以找出「反介入/區域拒止」體系中關鍵的長程偵測器與攻擊武器。值得注意的是，在模擬敵鎖定與打擊系統時，必須理解人工智慧如何輔助決策下達的過程。因為在短期的未來之內，美國敵人將會使用自動化系統來統整資訊，藉此提供特定提案來輔助指揮官下達決策。若美方飄忽不定的假目標能誘敵進行發現、修正及打擊等一連串行動，就能從中觀察敵這種未經熟慮的行為及高價值資產的部署位置，因此在未來戰場上軍事欺敵為找出並殲滅敵人至關重要的一項策略。

This argument for multi-domain military deception as central to finding U.S. adversaries on the battlefields of 2035 unfolds in three parts. First is a brief doctrinal background on military deception as it stands today. Second, and more comprehensively, is a discussion of the probable evolution of adversary A2/AD systems, with a focus on the strengths and potential weaknesses of AI support to targeting. Third is a series of recommendations the Army should consider to best employ multi-domain deception to find the enemy in 2035, with great-power oriented field armies as the integrator for these activities.

為了找出未來 2035 年美國在戰場上敵人的蹤跡，多領域軍事欺敵之道是關鍵解方。本文從三個部分加以探討：首先，概述軍事欺敵相關的準則背景，因為軍事欺敵之道至今仍屹立不搖；其次，更全面性探討敵「反介入/區域拒止」體系之可能演進過程，同時著重於人工智慧輔助武器鎖定系統的利弊；最後，提出一些建議事項讓美陸軍思考軍事欺敵的最佳運用之道，俾利找出未來 2035 年之敵要害，同時也說明為何大國軍隊下的各個野戰軍團是欺敵策略的最佳執行者。

Doctrinal Background on Military Deception

軍事欺敵相關的準則背景

The doctrinal and historical background for military deception is well

established. Broadly speaking, military deception activities "are planned and executed to cause adversaries to take actions or inactions that are favorable to the commander's objectives."3 In the specific context of stimulating an adversarial A2/AD system, this involves amplifying signatures of decoy units and continuously substituting the signatures of real units with simulated ones, thereby overloading an adversary with an overwhelming number of false positives.4 This approach of generating a large number of false positives—the impression of targets when in fact there are none—contrasts with the traditional notion of camouflage, which attempts to create a false negative of no target by masking the signatures of friendly forces. Central to the success of deception efforts is their multi-domain character; in an era of increasingly widespread, sophisticated, and varied sensors, spoofing only one type does little against an adversary capable of rapidly fusing multiple sources of information. "Multi-domain deception," as proposed by Christopher Rein, "requires close and careful coordination across the warfighting domains to ensure that lapses in one do not undo efforts in other areas."5

軍事欺敵準則與歷史案例已所在多有。大體而言，軍事欺敵活動之規劃與執行，「是為了使敵在落入我方指揮官所望目標後採取錯誤行動或不敢輕舉妄動。」[3]在特定時空背景下，為誘敵啟動「反介入/區域拒止」體系，除了必須強化誘餌信號外，還須持續用假信號來取代真實信號，如此才能製造大量「偽陽性」讓敵窮於應付。[4]這種製造大量「偽陽性」方法，就是讓敵偵察結果有，但實際上卻沒有目標物；至於傳統的偽裝法則是想辦法隱藏我軍單位信跡，企圖製造沒有目標物的「偽陰性」。欺敵作為的成功之道是善用多領域的特點；在眾多廣泛設置先進感測器的環境下，單一管道的欺敵作法，不足以應付能迅速整合各方資訊來源的敵人。誠如多領域軍事欺敵的提出者克里斯多福・雷所言，「多領域軍事欺敵策略需要各個作戰領域的密切配合，才能確保在某地方的小失誤不致於前功盡棄。」[5]

The Probable Evolution of Adversary A2/AD Systems

敵「反介入/區域拒止」體系之可能演進

Gaining an accurate understanding of an opponent's A2/AD

[3] Field Manual 3-13.4, *Army Support to Military Deception* (Washington, DC: U.S. Government Publishing Office, 2019), pp. 1-2.
[4] Ibid., pp. 1-8.
[5] Christopher M. Rein, ed., "Multi-Domain Deception," in *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations* (Fort Leavenworth, KS: Army University Press: 2018), p. 2.

architecture involves integrating information gathered through a variety of means. Overreliance on a single method, such as intercepted electronic communications or overhead imagery, can result in unbridgeable gaps in understanding. The United States has long been unmatched in its battlefield awareness, but its great-power competitors are rapidly gaining ground due to a pair of interrelated developments. First, the increased sophistication, fidelity, affordability, and variety of sensors have made gathering militarily relevant information easier and cheaper. Turning that information into understanding, however, requires a second step, and its impending automation may prove to be revolutionary. The promise of machine learning to fuse raw information rapidly and accurately into actionable targeting proposals will greatly complicate the tasks of hiding—and surviving—on the future battlefield.

為了正確理解敵「反介入/區域拒止」體系架構，必須透過各種手段統整各類資訊來源。過度依賴單一方法，如阻斷電子通信或空照影像，將陷入理解的認知缺陷。美國長期以來擁有優越的戰場覺知，但其實力匹敵者正不斷迎頭趕上。首先，感測器愈來愈進步、精準、多樣化及毋須花大錢取得，這讓軍事情蒐愈來愈容易。其次，即將來臨的自動化所帶來的革命性變革，可以將資訊轉為人能夠理解的部分。最後，由於機器學習可望將原始資訊快速準確轉變成特定的行動方案，這將使未來在戰場上的隱蔽與掩蔽更為困難，存活率也因此降低。

Widespread advances in low cost, off-the-shelf platforms and sensors such as drones and high-resolution cameras alongside near real-time, open-source information such as social media posts and commercially available satellite imagery have transformed both the scale and fidelity of information available and the number of international actors who have access to it. Previously only available to leading powers, such sensors have proliferated widely in the past decades. This trend shows no sign of abating; as the means of detection become cheaper, more reliable, and capable of gathering high-quality information, the information advantage enjoyed by the United States for the past several decades will erode further.[6]

各式感測器如無人機、高解析度相機等低成本、商規現貨載臺日益普及，另外像是社群媒體貼文、商業衛星影像等近及時、公開來源資訊之運用，這些除了大幅改變資訊的獲得規模與正確性外，也讓愈來愈多國際行為者得以接觸使用。感測器這類的裝置以往都是先進國家才有能力獲得，但在數十年演變下

已開始廣泛的普及化。這種趨勢顯而易見，偵測手段不再需要花大錢、也更為可靠及更能獲得高品質的資訊，而美國過去數十年所享有的這種資訊優勢也正逐漸消失。[6]

Increasing the diversity and quality of information gathering means solves one half of the challenge. The second half—fusing information from multiple sources to paint a comprehensive portrait of a target—is a more challenging task. Currently, this is a labor-intensive process involving cross-functional teams of analysts painstakingly poring over massive quantities of data captured by increasingly high-resolution sensors. By one estimate, it would take "eight million people just to analyze all of the imagery of the globe that will be generated in the next twenty years."[7] Advances in machine learning, however, may significantly improve and accelerate the fusion of gathered information. Machine-learning classifiers, which "take an input sample and identify it as one of several output classes," are particularly well suited to fusion and targeting.[8] In an AI support to A2/ AD targeting context, the input sample would be data gathered through a range of sensors, and the output classes would be a classification of the target. A properly trained machine-learning algorithm with access to a wide range of accurate data would be then able to find the proverbial needle in the haystack and accurately classify a target, greatly accelerating and improving the hitherto laborious information fusion process.[9]

資訊蒐集手段愈來愈多樣性與品質提升，雖然解決了問題的一半，但另問題的一半則是更富挑戰性－須統整多方資訊來源並研擬出針對目標的全般計畫。就當前狀況而言，這是種勞力密集的過程，因為各個跨職能領域的分析師必須不斷鑽研由高解析度感測器所產生的大量數據資料。一項預估指出，「全球未來二十年所產製的影像，將需要八百萬名人力。」[7]機器學習的進展可以大幅改善並加速資訊的統合，因為機器學習的分類器可以將各種單筆資訊進行歸類，尤其適合執行整合工作與特定事項。[8]在人工智慧輔助下的「反介入/區域拒止」體系，其輸入樣本是一系列感測器所蒐集的資料，但其產出資料部分能依

[6] Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International P olitics* (Princeton, NJ: Princeton University Press, 2010).
[7] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hatchette, 2020), p. 59.
[8] Patrick McDaniel, Nicolas Papernot, and Z. Berkay Celik, "Machine Learning in Adversarial Settings," *IEEE Security & Privacy* 14, no. 3 (May 2016): pp. 68-72.

據目標做歸類。機器學習演算法經適當訓練後，可以正確處理眾多的資料，甚至能夠大海撈針，準確地進行目標分類，大幅加速並改善現今運用人力處理資訊的過程。[9]

Much like its diminishing edge in sensors, the United States will not have a monopoly on these automated fusion techniques. By 2035, U.S. adversaries will likely have leveraged machine-learning techniques to fuse information gathered from a wide array of sensors to target their A2/AD weapons. This will present a novel set of challenges in how friendly forces conceal themselves. The wholesale collection of a wide range of signatures of friendly forces may nullify friendly efforts to camouflage in a monodimensional way. For example, minimizing electromagnetic emissions may have a negligible effect against an adversary that can still detect a unit’s thermal, civilian contracting, or social media signature. In more general terms, creating a cohesive false negative against a highly sensitive, multi-domain sensor system will be almost impossible—the adversary will detect something, and well-trained AI will be able to extrapolate an accurate picture of the target from what is detected.

美國未來將不再獨大這些自動化整合資訊的技術，情況類似於其在感測器上不斷消失的獨家優勢。到了 2035 年時，敵很可能會利用機器學習技術來整合從各式感測器所蒐集的資訊，藉此用來校準其「反介入/區域拒止」武器。這對美方部隊的隱蔽與掩蔽，將構成一系列新的挑戰。這種全面性的信號蒐集，將使我方部隊單一偽裝的作法不再有效。例如，減少電磁波傳送的功用微乎其微，因為敵人仍可以從事熱感應偵測、追蹤人的足跡或是社群媒體動態等工作。大體而言，創造一個集體的「偽陰性」假象來騙過高敏感度的多領域感測系統，這是不可能的事，因為敵人還會偵測其他事物，而且訓練有素的人工智慧可以從偵測的各項數據中正確找到目標所在位置。

While daunting, this potential revolution in U.S. adversary’s information-gathering and fusion techniques presents an opportunity for friendly forces to find the enemy in the battlefields of 2035. If done cohesively, novel multi-domain military deception can warp an adversary’s algorithms and exploit organizational and procedural tensions between machine-learning-produced proposals and human decision-makers. This

[9] Stephan Pikner, “Training the Machines: Incorporating AI into Land Combat Systems,” Landpower Es say Series (Washington, DC: Institute of Land Warfare, January 2019), accessed 20 October 2020, https://www.ausa.org/sites/default/files/publications/LPE-19-1-Training-the-Machines-Incorporating-AI-into-Land-Combat-Systems.pdf.

deception is not an end unto itself; to clarify the uncertain and contradictory targeting decision information, an adversary will be forced to expose its A2/AD architecture by using increasingly active means that emit unambiguous signatures. Deceiving an adversary into exposing critical nodes of its A2/AD architecture is central to finding well-hidden enemy forces in 2035.

儘管美國敵人可能會在資訊蒐集與統合技術上有所革新，但美方部隊仍有機會找出未來 2035 年的戰場之敵。只要美軍能齊心協力研擬新的多領域軍事欺敵之道，就可以打擊敵人的演算法，還可以在機器學習與敵決策者之間製造組織和程序上的緊張關係。這種欺敵法本身不是目的（而是手段）；為了釐清不確定性與目標鎖定決策資訊的矛盾情形，敵人將不得不主動傳送明確信號，從而暴露其「反介入/區域拒止」的體系架構。用欺敵手法使敵暴露其「反介入/區域拒止」體系架構的關鍵節點至關重要，如此才能找出未來 2035 年善於隱匿的敵軍。

Machine learning is not impervious to spoofing. Machine learning relies more heavily on readily quantifiable data as inputs than existing processes in which humans can place ambiguous evidence in context. Sensors narrowly focused on detecting specific, measurable electromagnetic, acoustic, thermal, gravitational, visual, vibrational, geotagged social media, or computer-aided text analysis data must feed cleanly into a machine-learning algorithm. This algorithm, in turn, is trained by forming correlations between similar signatures and known target characteristics.[10]Its accuracy hinges on the richness of its training dataset, where true positives and valid, associated covariates form a basis for the algorithm to be tuned and updated. In a military context, the true positives would be actual cases of the target, and the associated covariates would be the full range of measurable signatures across all domains. Currently, the fusion of multi-domain information happens through manpower-intensive cells on military staffs; machine learning offers the opportunity for this same process to happen rapidly, automatically, and through the recognition of patterns of correlations that may elude human cognition. Deliberately muddying the waters through military deception operations that obfuscate how a true target looks can undermine this learning process, tricking an AI-enabled A2/AD system to look in the wrong place for the wrong signatures. Or, as Edward Geist and Marjory Blumenthal put it, friendly forces can employ “fog

of war machines" to confuse adversarial sensors and the associated machine-learning processes.[11]

機器學習並非不可愚弄或欺騙，其極為仰賴可量化數據的持續輸入，與人工情報所蒐集的不明確性資料不同。感測器針對特定事物、電磁波、聲波、熱源、引力、圖片影像、震動、社群媒體地理標註或電腦輔助文本分析等進行偵測，而這些數據必須有條不紊輸入機器學習演算法；接著，演算法在將類似信號與所知目標特徵進行連結配對。[10]因此機器學習的演算法之準確性在於其資料集的豐富性，而演算法是否適時校正和更新將影響正確接受數、效度及相關共變數。就軍事而言，正確接受數是實際目標數，至於相關共變數則是跨所有領域一連串可測量到的信號。當前，多領域資訊的整合需要在人力密集的軍事單位；然機器學習則為同樣的處理程序帶來一個迅速、自動化完成的機會，而且透過關聯模式的認知方式就可以代替人的認知。軍事欺敵作為就像是把水弄得更混濁一樣，讓人搞不清楚真正目標在哪裡，從而破壞機器學習的處理程序，並愚弄由人工智慧輔助的「反介入/區域拒止」體系，使之迷失在錯誤方向下的錯誤目標。誠如愛德華・蓋斯特與馬喬里・布盧門撒爾兩位專家所言，我方部隊應部署能夠製造戰爭迷霧的機器，以混淆敵人的感測器及相關的機器學習處理程序。[11]

This increased reliance on quantifiable data streams to feed a machine-learning-driven targeting algorithm can also open a critical vulnerability within an adversary's organization: it comes at the expense of human expertise and intuition, making the entire system vulnerable to multi-domain deception. The halting, uneven development of AI over the past several decades is littered with examples of seemingly clever machines that, when posed with real-life challenges beyond the narrow scope of their training, are completely baffled.[12] In contrast to conventionally programmed systems, there is no team of engineers who can easily tweak the code to better support the human decision-makers in the system but rather a black box where outputs are generated by hidden layers of weighted links within a neural network formed by iterating through training data.[13] This lack of clarity as to how the machine learns may cause friction in an AI-enhanced human

[10] Gary Marcus, "Deep Learning, a Critical Appraisal" (paper, New York University, 2018), accessed 20 October 2020, https://arxiv.org/ftp/arxiv/papers/1801/1801.00631.pdf.

[11] Edward Geist and Marjory Blumenthal, "Military Deception: AI's Killer App?," War on the Rocks, 23 October 2019, accessed 20 October 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

decision-making system. Prior to a real-world failure, a machine-learning algorithm's assumed omniscience may diminish the relative value of human decision-making, creating the dilemma that when the machine-learning system is most needed it is least trusted, while the human-driven alternative to it has atrophied in status and capability.[14]

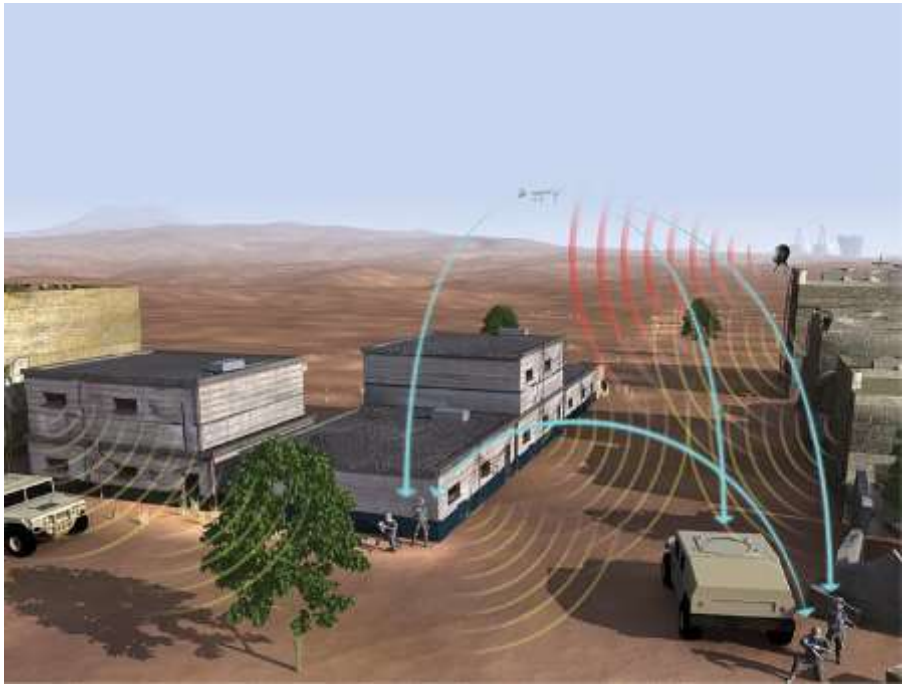
這種逐漸依賴可量化數據輸入至機器學習的目標鎖定演算法，將使敵人產生一個致命弱點：機器學習毋須靠人的專業知識與直覺，這讓多領域軍事欺敵找到一個切入點。過去數十年斷斷續續人工智慧發展的案例都顯示，機器所受的狹隘訓練當遇到真實生活中的各種挑戰時，往往出現許多狀況。[12]有別於傳統程式設計系統，沒有任何一個工程團隊可以輕易調整代碼，讓機器可以更有效率協助系統中的人類決策者，其作用原理反而是由一個黑盒子內的類神經網路（不斷更新訓練資料）中各個隱藏的權重連結層所產製的輸出指令。[13]這讓機器學習存在不明確性，導致在人工智慧輔助人類決策系統中產生摩擦。機器學習的演算法在真實世界的失敗是可以預知的，因為其無所不能的設定將削減人類決策者的相對重要性，同時也會形成一種困境：機器學習系統獲得愈來愈多的信任，反觀人工決策的信任感在地位與能力卻愈來愈萎縮。[14]

Deceiving an adversary's machine-learning-driven targeting system can trick the adversary into either activating high-signature sensors or striking at phantom targets. In future land conflict, this opens an important window of opportunity to deliver friendly joint counterbattery fires against the enemy's "kill chain" of sensors, command and control nodes, and weapons platforms.[15] What multi-domain military deception brings to future warfare is the potential to spoof the machine—to confuse an AI-augmented adversary's targeting chain—and through that deception, expose its reconnaissance and strike assets.

欺騙敵人的機器學習目標鎖定系統，可以讓敵啟動高信號的感測器或是向幽靈目標發動打擊。在未來的地面衝突中，有效欺敵作為將可為我軍開啟重要的機會之窗：發揚聯合反砲戰火力，以打擊如感測器、指管節點及武器系統等敵要害。[15]多領域軍事欺敵對未來戰場所帶來的效益是愚弄機器，也就是混淆由

[12] Marcus, "Deep Learning, a Critical Appraisal."
[13] McDaniel, Papernot, and Celik, "Machine Learning in Adversarial Settings."
[14] Peter Hickman, "The Future of Warfare Will Continue to Be Human," War on the Rocks, 12 May 2020, accessed 20 October 2020, https://warontherocks.com/2020/05/the-future-of-warfare-willcontinue-to-be-human/.
[15] Brose, *The Kill Chain.*

人工智慧輔助的敵目標鎖定鏈，同時還能使敵暴露其偵察工作與武器位置。



Source: Illustration courtesy of the Defense Advanced Research Projects Agency

New technologies will convert and integrate electromagnetic signals from multiple sources into digital data that can be processed at unprecedented speeds to enhance the warfighter's ability to see through enemy deception measures to identify and neutralize threats on the modern battlefield. Technological advancements will also dramatically upgrade the ability of friendly forces to deceive enemy intelligence collection efforts through improved electronic warfare measures.

新式科技可以整合各種不同來源的電磁信號並將之轉化成數位資料，而數位資料的快速處理程序，將使作戰人員能看穿敵人的欺敵戰術，進而辨識並殲滅現代化戰場上的威脅。至於各項科技的進步與電子戰措施的精進，同樣也會大幅提升我軍的欺敵策略。

Recommendations and Conclusions

建議與結論

Developing and fielding the organizations, doctrine, training, and equipment needed for effective employment of multi-domain military deception requires a deliberate and coordinated approach.[16] This section outlines four specific considerations for a force capable of leveraging multi-domain deception to find the enemy in 2035. First, the components of an integrated,

multi-domain deception posture must be flexible and adaptable to maintain a sustained deception effect against a learning adversary. Second, multi-domain full-spectrum deception cannot begin in a crisis but rather must be grounded in baseline conditions set during competition below the threshold of armed conflict. Third, as it is highly likely that land operations will involve allies and partners fighting alongside U.S. ground forces, multi-domain deception will be enhanced by including them into a theater-wide scheme. Lastly, multi-domain deception must not be viewed as an end unto itself but rather a means to prompt an adversary to "show its hand." By provoking an enemy's A2/AD kill chain to pursue phantom formations, multi-domain deception can stimulate—and therefore expose—critical components of its network to destruction.

為了有效部署軍事欺敵之道，必須適切發展並運用組織、準則、訓練及裝備等事項，同時也需要一個縝密的全盤計畫。[16]為了使部隊有效利用多領域欺敵以找出未來 2035 年之敵，本文提出四項特定思維：第一，一個整體多領域欺敵的態勢必須具有彈性及適應力，這樣才能針對不斷學習的敵人發揮維持欺敵的效果；第二，多領域全頻譜的欺敵不能在危機發生時才開始，其運用的情境設定應該是在未達武裝衝突程度；第三，未來的地面作戰情況極可能是美軍協同友軍部隊的盟軍作戰，因此多領域欺敵的研擬必須將友軍部隊納入戰區計畫之中；第四，多領域欺敵不應視為目的而是作為手段，意在使敵人暴露其部署弱點。軍事欺敵可以讓敵人「反介入/區域拒止」擊殺鏈對幽靈部隊發動攻擊，從而暴露自身網絡的關鍵節點而走向毀滅之路。關於上述四項思維的細節敘述如後：

The first consideration in developing multi-domain deception is the interactive, competitive, and evolutionary dynamic of military deception. Successful deception depends as much on an adversary's perceptions and interpretations of friendly signatures as it does on the emissions that formations generate. In addition to the technical dimensions of generating credible apparitions, there is a critical organizational element that is grounded in the U.S. adversary's military culture: what may fool Americans may not spoof an adversary, and methods that may be effective against one competitor

[16] Eric Wesley and Jon Bates, "To Change an Army—Winning Tomorrow," *Military Review* 100, no. 3 (May-June 2020): pp. 6-18.

may be discounted by another. Deception efforts must continuously adapt as adversary biases, capabilities, and doctrine evolve.

思維一：多領域欺敵之發展是交互式、競爭式及動態演進過程。成功欺敵之道重點在於敵對我方部隊產生信號的認知與理解。除了在技術層面製造令敵相信的幻影外，還需理解在敵軍事文化中的關鍵組織要素，也就是美國認為有效的愚弄方式並不見得對敵人有效，同樣道理，對這個敵人有效的方法，用在其他敵人身上可能就大打折扣。各項欺敵作為必須根據敵人的偏好、能力及準則演進等要素持續調整。

Second, successful deception in a crisis of conflict must be built on a foundation established in peacetime. Persistent competition below the threshold of armed conflict should include deliberate efforts to monitor, mask, and simulate the full spectrum of friendly land force signatures. The goal of this is twofold: first, to comprehensively “see ourselves” and second, to influence the training data sets that U.S. adversaries are building on friendly forces in peacetime to train their AI targeting systems. To achieve these goals, friendly formations operations in peacetime must be thoroughly monitored by teams tasked with building a comprehensive profile of a unit’s signatures and emissions. This profile will be the baseline of what can be detected and exploited by an adversary’s A2/AD sensors. These teams would monitor friendly forces in both simulated tactical engagements and during deployment to real-life forward locations. From this data, gathered in peacetime competition during rotational deployments and exercises, a thorough, all-spectrum picture of how land formations appear to the full range of an adversary’s sensors can be painted.

思維二：多領域欺敵在衝突危機的成功之道，是奠基在承平時期的基礎之下。因此在未達武裝衝突程度的持續競爭環境時，吾人應做好監視、偽裝，以及模擬我軍地面部隊的各式信號源等工作要項。這個目標是一體兩面：一面是要全盤看見我方部隊，另一面是要影響敵人在承平時期為訓練其人工智慧目標鎖定系統而對我軍所建立的訓練資料集。為了達成這些目標，我軍部隊在承平時期的行動必須由專責小組負責監控，完善建立單位訊號與足跡等全面性資料檔。這個資料檔可以讓我們理解敵「反介入/區域拒止」感測器之偵探情形。專責小組必須監控我方部隊不管是在模擬戰術交戰，或是在真實前進點的部署情形。無論是在承平時期的競爭環境，或是在定期部署與演習期間，將這些資料進行蒐集後，就能得到一個全般地面部隊圖像，這也是敵人感測器所描繪出的

圖像。

That comprehensive signature of friendly forces catalogued in peacetime can be used in two distinct ways. The first is to mask the footprint of true formations by minimizing their emissions. Contrary to the conventional wisdom of “train as you fight,” many of the steps that would be taken to mask a unit’s footprint should only be taken in a real-world crisis. Exercising them routinely during peacetime competition would allow an adversary to learn alternate “tells” of a unit’s location and disposition that are harder （or impossible） to mask during conflict. For example, minimizing a unit’s electromagnetic footprint during a rotational deployment may drive an adversary to search more closely for other, less easily concealable signatures as key indicators of friendly forces.

在承平時期如何運用我軍部隊所發出的各種信號，以下提出兩種獨特的方法：第一種，藉由避免洩漏聲、光、熱、氣等來偽裝真正部隊的足跡，有別於傳統思維是去訓練士兵如何作戰，工作的重點卻是不斷以各種方法偽裝單位足跡，以往這都是在真正危機來臨時才做。在承平競爭時期例行性進行上述演練，敵人就會為了尋找某單位的位置與部署情況而暴露其各種尋找方式，一旦衝突來臨時，敵人將難以隱匿其原本的偵察模式。舉例而言，欺敵的作法是在定期部署期間讓一個單位的電磁足跡最小化，敵人就會轉而搜尋另一個鄰近、信號較強的我軍單位，因為敵認為這個單位是找出我方部隊部署的重要指標。

In addition to informing how best to mask the true location of a friendly unit in crisis, the comprehensive signature of friendly forces can be replicated as a deception technique. This signature not only includes the military equipment of a friendly formation but also the social media and commercial contracting emissions that are produced by the deployment of such a force. Friendly deception units that can simulate the characteristics of full combat formations can act as “honey pots” that draw attention away from actual formations and fool the enemy into exposing critical components of its A2/AD kill chain.

第二種，在危機期間除了妥善隱匿某個我方單位外，複製我軍部隊的各種信號也能成為欺敵的技巧。這種信號可以是我軍部隊的裝備武器，也可以是部隊在部署時所產生的社群媒體訊息和承包商活動。我軍從事欺敵的單位可以偽造全戰鬥編隊，作為吸引敵人的陷阱，甚至愚弄敵人並使其暴露「反介入/區域

拒止」擊殺鏈的關鍵組成部分。

Third, future warfare in the land domain is almost guaranteed to take place in a coalition context. To maximize the tactical effectiveness of multi-domain military deception, the signatures of allied and partner land formations should be measured and mimicked in a manner similar to American ground forces. At the theater level, this includes military deception operations involving ports of debarkation, strategic force hubs, and other critical infrastructure that enables friendly forces to surge into an area of operations. As these facilities are often near population centers and typically have dual civilian and military functions, special consideration must be given to allied concerns about and constraints on military deception activities. Clear lines reinforcing the protected status of certain facilities and personnel （e.g., hospitals, religious sites, medical personnel） must be drawn and communicated with U.S. allies to avoid any perception that these efforts would violate the Law of Armed Conflict.[17]

思維三：未來的地面作戰幾乎可以確定是盟軍作戰型態。為使多領域軍事欺敵發揮最大戰術效果，盟國與作戰夥伴部隊信跡之檢測，都應比照美軍地面部隊的模式。在戰區層級，軍事欺敵行動涉及登陸港口、戰略力量中心及其他關鍵設施等，這些都是影響我軍部隊在作戰區集結的因素。某些設施往往位於人口稠密中心，通常還具有軍民兩種用途，我方盟軍部隊尤其需要注意關於軍事欺敵活動的各種限制因素。清楚劃分各設施的界線將有助於保護特定設施與人員（如醫院、宗教設施、醫療人員）的安全，美國必須向盟軍部隊做好溝通，避免做出錯誤決策而導致違反武裝衝突法。[17]

Finally, the overarching purpose of this multi-domain military deception effort is to find the enemy on the battlefields of the future. It is in presenting an irresistible, but false, target to the adversary where multi-domain military deception facilitates finding the enemy. Stimulating the enemy's integrated system of sensors and shooters by simulating the presence of lucrative, but phantom, targets can expose the high value, highly survivable assets in their kill chain. Effective deception can trigger a full range of adversary sensors—reconnaissance teams, electronic attack systems, satellites,

[17] "Geneva Convention (IV): Relative to the Protection of Civilian Persons, Part I," Infoplease, 12 August 1949, accessed 2 November 2020, https://www.infoplease.com/primary-sources/government/united-nations/convention-relative-protection-civilian-persons-time-war.

unmanned aerial vehicles, ground surveillance radars, and cyber assets to activate in search of a chimera. An enemy's A2/AD weapons such as theater ballistic missiles, long-range artillery, and special forces would similarly deploy from secure, camouflaged sites to strike what they believe are actual friendly concentrations. Anticipating this activation, friendly intelligence, surveillance, and reconnaissance systems, synchronized with the multi-domain military deception plan, can anticipate, sense, and exploit this overt and active enemy activity. Instead of an ineffective and costly search against hardened and camouflaged components of an A2/AD system, multi-domain military deception can trick our future adversaries into exposing themselves prematurely.

思維四：多領域軍事欺敵之整體目的是找出未來戰場之敵。多領域軍事欺敵是一種手段，主要是誘敵落入假象，進而讓敵人洩露蹤跡。藉由製造合適的幽靈目標，誘敵啟動偵打一體系統，從而暴露其擊殺鏈中高價值、高存活率的各種武器與設施。有效的欺敵之道可以讓敵誤以為有目標而啟動一系列感測器網絡，如偵察隊、電子攻擊系統、衛星、無人飛行載具、地面偵察雷達、網路設備等。敵「反介入/區域拒止」武器系統，如戰區彈道飛彈、長程火砲、特戰部隊，勢必也會進行隱蔽與掩蔽之部署，伺機而動打擊我軍部隊的集結地。為能預測敵活動，我軍的情監偵系統應與多領域軍事欺敵計畫相結合，如此才能預測、察覺及找出隱匿之敵的各種活動情形。有別於使用既無效又昂貴的搜尋方法來對付堅固隱匿的「反介入/區域拒止」系統，多領域軍事欺敵可以愚弄未來之敵，並使之不經意暴露自身蹤跡。

Implementing these recommendations requires detailed understanding of a great-power competitor, the proper level of friendly authorities and capabilities, and the posture during competition below the threshold of armed conflict to maintain and modulate an enduring deception campaign. In the Army's current structure, this task would most likely fall between the corps and the Army Service component command. As the Army adapts to great-power competition, the final recommendation of this article is that a field army, focused on competing against a specific adversary, should be the proponent for and integrator of multi-domain military deception operations. [18]Unburdened of the theater-wide responsibilities of the Army Service component command, and in contrast to a corps oriented on a specific adversary in peacetime

competition, a field army would be best positioned to design and prosecute an enduring, cohesive, and tailored military deception campaign. Through this deception, the Army can force its adversaries to strike out blindly against shadows, exposing the critical components of their A2/AD architecture to detection, destruction, and ultimately, defeat.

執行這些建議事項必須做到澈底理解大國競爭者（知敵）、強化我軍部隊能力，以及完成在未達武裝衝突程度的態勢部署，如此才能在不斷調整下遂行持久性的欺敵策略。在美陸軍現行架構下，將多領域軍事欺敵任務賦予軍級單位與各個陸軍部隊指揮部並不洽當。至於要如何因應大國競爭，最後提出的建議是各個野戰軍團應成為多領域軍事欺敵行動的支持者與整合者，因為其是對付特定大國軍隊的最佳人選。[18]不像各個美陸軍部隊指揮部有作戰責任區的劃分，以及軍級部隊主要任務是在承平競爭時期對付特定之敵，各個野戰軍團是最能夠設計並執行長期性、一致性及針對性軍事欺敵活動之不二人選。藉由欺敵之道，可以讓敵人盲目打擊假目標，從而暴露其「反介入/區域拒止」架構中的關鍵弱點，我方便得以進行偵測、打擊，最終達摧毀敵人之目標。

譯後語

美軍未來作戰所要克服的是敵「反介入/區域拒止」武器系統。雖然目前中共「反介入/區域拒止」能力限縮於第二島鏈以西，但假以時日不無可能涵蓋整個西太平洋。美軍認為中共「反介入/區域拒止」將限制其兵力投射能力，使之無法進入交戰區，甚至讓美軍行動限縮在特定的敵火力範圍內。為克服未來 2035 年的作戰困境，本文提出軍事欺敵策略，作法是誘敵產生特定行動，使其暴露「反介入/區域拒止」架構中的關鍵弱點，將「敵暗我明」的劣勢扭轉為「敵明我暗」的優勢，進而攻擊敵要害。

未來戰場的情監偵將會使用大量的感測器，同時輔以人工智慧自動處理所蒐集的龐大資料，進而提供指揮官可行的行動方案。因此，在未來戰場上只要能愚弄敵感測器，就能擾亂敵人決策及行動。欺敵作為可分為實體與非實體：實體即為人所知假的戰、甲、砲車或火砲，可能是充氣式、木造式或是塑料製成，藉此消耗敵彈藥或保全真正武器載臺；非實體則是利用假的信號源讓感測器認為是武器所在位置，進而回報錯誤資訊，擾亂敵決策系統。在未來戰場環境中，非實體的欺敵作為比重將大為增加，正所謂制敵機先，勝利公算不外乎

[18] Amos C. Fox, “Getting Multi-Domain Operations Right: Two Critical Flaws in the U.S. Army’s Multi-Domain Operations Concept,” Land Warfare Paper 133 (Washington, DC: Association of the United States Army, June 2020), accessed 20 October 2020, https://www.ausa.org/sites/default/files/publications/LWP-133-Getting-Multi-Domain-Operations-Right-Two-Critical-Flaws-in-the-US-Armys-Multi-Domain-Operations-Concept.pdf.

儘早完成整備。

中共「反介入/區域拒止」武器系統也會對我國造成安全威脅，因此國軍應及早準備多領域軍事欺敵的相關事項，只有混淆並擾亂敵決策系統，才能有效達戰力保存，發起爾後之攻擊。值此國軍組織變革之際，繼成立「聯合兵種營」後，又著手將原本的澎湖防衛指揮部、花東防衛指揮部及第六、第八、第十軍團，分別改成第一、二、三、四、五作戰區。作戰區層級將是欺敵策略最佳執行者，未來各作戰區指揮官在做兵力規劃部署時，應將多領域軍事欺敵之道納入考量，才能獲得最大的勝利公算。

在砲兵作為方面，除了持續強化砲陣地轉移戰鬥訓練外，也應建置各項砲兵的偽裝欺敵設施，實體假象與非實體假信號兩者應同時並進，因為在感測器與情監偵科技的進步下，將能夠識破實體假象的偽裝，如能在實體假象設施中加入非實體假信號，才能讓敵人誤以為是攻擊目標，在敵下達錯誤決策之際，我方才能趁隙攻擊敵關鍵弱點，達成奇襲之效。

作者簡介

Lt. Col. Stephan Pikner, PhD, U.S. Army, is an Army strategist （FA59）and a graduate of the Advanced Strategic Policy and Planning Program. He holds a BS from the U.S. Military Academy, an MPA from the Harvard Kennedy School of Government, and a PhD from Georgetown University.

美陸軍中校史蒂芬‧平克納（Stephen Pikner）係陸軍戰略研究家（具 FA59 校級軍官專長），曾受高級戰略規劃與政策學程（ASP3）；西點軍校畢業，哈佛甘迺迪政府學院公共行政碩士，喬治城大學博士。

譯者簡介

劉宗翰陸軍中校，國防大學管理學院 93 年班、政治大學外交系戰略所碩士，現服務於國防部政務辦公室史政編譯處，曾任《國防譯粹》月刊主編。