

● 作者/Eric P. Seligman ● 譯者/黃坤銘 ● 審者/馬浩翔

瞭解網路戰本質

There is No Cyber Bullet

取材/2022年7月美國海軍學會月刊(*Proceedings*, July/2022)

網路戰場經緯萬端，各級指揮官在運用網路武器時，應跳脫以武器性能為考量之窠臼，從戰略層面全盤評估其作戰效益與外溢風險，並責成戰略執行單位提早遂行作戰準備，以達成作戰目標。

自 有戰爭以來，戰士的實力一直與其如何有效地發揮當時的武器劃上等號。戰士花費數年磨練戰技，所運用的武器載臺即為其拳腳之延伸。這些武器可能是劍、弓、毛瑟槍、M16步槍或F-35戰機，但終其職涯，所用武器形式鮮少改變。然而，對網路戰士來說卻並非如此。他們的武器不具特定外型且不同以往，而這也就是大家熟知的「網路武器」(Cy-



ber Weapons)。

美國國防部《軍語辭典》(Dictionary of Military and Associated Terms)對「武器」(Weapon)一詞並無明確定義，但該詞卻被引用超過150次，用來解釋其他專有名詞。其中一個例子，就是眾所皆知的「火力」(Fires)：「運用武器系統或其他軍事行動，對目標產生致命或非致命效果」。¹ 這個詞彙受到某種程度青睞，因為「網路

火力」(Cyber Fires) 特別當論及攻勢網路作戰與相關軍事行動時，更受廣泛運用。²

倘若武器系統目的是投射火力，那麼這些火力的效果就必須能夠精準且為人所知。舉例來說，在目標區50呎外引爆500磅的MK 82炸彈，就能形成17個大氣壓的超壓狀態。炸彈破片可穿透厚達32公釐的裝甲鋼板，而在相同距離下，手無寸鐵的血肉之軀遭受波及則必

死無疑。³ 而且，此類型炸藥對CKS131猛士二代及GAZ Tiger猛虎車帶來同等殺傷效果(兩者皆為裝甲高機動多用途輪型車輛[High Mobility Multipurpose Wheeled Vehicle, HMMWV])。如果單發MK 82無法成功摧毀目標，接續射擊的MK 82必定能夠成功殲滅之。

物理定律亙久不變：當轉移到特定物體的能量超出其分子鏈結強度時，就會產生必然結

果。這就是動能打擊的世界，也就是炸彈和彈藥的世界。然而，網路作戰的世界卻非如此。

不過，海上、空中及地面作戰指揮官須親眼目睹網路武器所帶來的實質作戰效果。指揮官也該心知肚明，即便自己不諳網路作戰運作方式，或者無法掌握全盤狀況，網路武器也應產生特定作戰效果。第五作戰領域——網路——迥異於其他領域，完全是人為建構。這個領域的「定律」可說不斷改變。作戰人員運用的戰術或工具可能僅能適用在當下，一旦換個場景時就可能完全行不通。

那麼，如此虛幻的網路武器該何去何從？我們該如何讓它變得和MK 82一樣，具備同等的殺傷力和可靠度？

建置有效網路武器

MK 82與類似彈藥的研發、測試、製造及部署都有其明確作業流程。那麼網路武器又是如何？



網路武器錯綜複雜，指揮官務必瞭解，網路武器部署先期整備作業須耗時數週，即便投入心力整備，仍可能會產生意想不到的後果。

(Source: USN/Arthur Rosen)

假設有人告訴指揮官，武器的作戰效益完全取決在諸多變數上：部分可預測、大部分無法預測，而部分變數仍屬未知。這就是目前美海軍在試圖發展和部署網路武器時所面臨到的窘境。

試想在設計網路武器時存在的一個潛在變數：目標所處作業系統。雖然這似乎不難理解，因為微軟在過去15年也開發出14種不同版本的主要作業系統。⁴ 接著，再將32位元與64位元處理器這兩項變數納入考量，所要考慮的變數就會瞬間翻倍。不論目標物型態或製造商為何，MK 82皆可將目標摧毀。然而，網路武器卻並非如此，不同版本的作業系統，須運用不同網路武器方可有效加以反制。此外，上述變數仍未將自定義結構(Custom Configuration)、修補程式等級(Patch Level)、安全軟體(Security Product)或其他應用程式等納入考量，而這些都是會影響網路武器作戰效益的因素。

在部署網路武器時，須將多達數千項變數納入考量。當然，在評估武器性能時，只會把已知變數納入考量。若要考量未知變數(諸如網路連線或系統記憶體狀況)所導致的可能性，就必須把過往評估特定作戰效益的簡單常態評估流程，轉換為不確定機率演算。

換言之，最佳狀況就是網路武器「可能」發揮作戰效益，但最糟糕的情況是——「無法鎖定特定目標」。引發第三級、甚至

第四級的外溢效應，超出武器使用者最初的作戰意圖，這種狀況即便駭人聽聞，然而卻時常發生。

隱蔽網路行動之必要

假若研發與測試網路武器等諸多因素均已納入考量，該武器最終也量產部署。《美國法典》第10編與第50編明定多數網路作戰執行作法。⁵ 對不熟悉的人而言，上述權責區分一目了然：第10編明定攻勢網路軍事行動範疇；第50編授權「隱蔽行動」(Covert Activities)，更精確來說，就是情報蒐集。然而，就如網路作戰圈大多數人所熟知的現況，這在實務上很難明確劃分。⁶

上述爭議的重點在於，大多數第10編所提及的攻勢網路軍事行動，都必須透過「類似第50編」的相關作為來達成目標。這樣一來，美國比照傳統模式(如南海自由航行作戰)，試圖在網路環境遂行兵力展示時，就會產生爭議。此種軍事行動意圖，即在向敵方展示，美國有能力、也有意願嚇阻任何侵害其自身利益的舉措。

問題是，在網路環境中光明正大使用武器，而且還毫不避諱展示武器性能，很可能會是該武器最後一次發揮效能的機會。每次使用MK 82時，都會釋放出一股動力，然而網路武器卻非如此，每次使用都會產生特定簽章(Signature)。隨著使用次數逐漸增加，該項網路攻擊將變得難以遁形、更不易達到所望效果。⁷

一旦敵方發覺目標弱點，我方就會更難入侵，情況也就變得雪上加霜。雖然我方可以修改簽章，然而目標弱點有限，也不易發覺。兵力展示作為或任何刻意為之的類似舉措，都會導致武器性能失效或無法駭入目標系統的雙重後果。網路攻擊若要持續發揮效用，最好的方式就是一盡其所能地隱蔽進行且不留痕跡——只有在必要情況下才將其公諸於世。

存取能力與戰術作戰

倘若從作戰之初，網路武器均未遭敵偵獲，並且持續發揮效能，那美海軍與陸戰隊指揮官在海上與陸上坐鎮指揮時，如何讓其發揮應具備之作戰

效益？多數情況下，攻勢網路作戰必須駭入目標系統才能達到所望戰果，而預先部署的網路武器，無法透過兵力投射方式以支援遠方作戰部隊。

在網路作戰領域中，「存取能力等同作戰勝利」。而在多數成功作戰中，並非只要花費一小時或一天就可以成功存取目標。一般來說，耗時長達數週、數月，甚至是數年的先期準備都算是家常便飯。更進一步來看，即便花上數個月準備，費盡千辛萬苦才駭進特定網路，卻可能在轉瞬間就被踢出門外。⁸ 就算發現新目標，下手前也要經過萬全準備，等到時機成熟方可執行攻擊行動，而無法貿然行事。如此一來，戰術與作戰層級指揮官在目標偵獲初期，幾乎無法即時運用網路武器，而須回到戰略層面才能發動網路作戰。

戰術層級的網路攻擊概念實屬可遇不可求，因此，過去在戰術層級以網路武器攻擊未知目標的案例可說是少之又少。在網路作戰領域，這種「頭獎目標」屈指可數、難得可見。

網路武器的真理

綜上所述，如果使用者無法確切瞭解網路武器性能，而其作戰效果又隨著使用次數指數降低，又必須先行存取目標系統才能發揮效用，這樣一來，它還稱得上是一種武器嗎？這個問題完全問到網路作戰的痛處：沒有網路彈藥，沒有網路炸彈，事實上，更沒有網路武器存在。

現實情況是一塊無限延伸的拼圖，是由眾多類似網路形式連接而成的工具與技巧所拼湊而成，與其說它具有戰士般的能力，還不如說像是一位鎖匠、竊賊或破壞狂，擁有各式各樣技能。網路工具通過疊代式研發流程與快速測試，只求滿足基本功能。這樣一來，才能跟上網路領域稍縱即逝、快速變換的步調。

與MK 82的研發人員或工程師不同，網路工具開發商沒有幾十年的光陰讓他們精雕細琢、深入研究。他們也無法仰賴亙古不變的自然律和物理定律來設定假想事項，網路定律每天、每小時都不斷在改寫。



飛行員能夠熟練駕駛F-35C型戰機，不只知道如何操作飛機，也瞭解機上掛載武器的性能諸元。網路武器不斷改變，也讓操作人員難以掌握其所具備的特定作戰效果。(Source: USN/Haydn N. Smith)

未來展望

既然網路作戰錯綜複雜，那麼，指揮官如果發現網路作戰的潛在效益，卻又不知道如何整合、如何部署，該怎麼辦？逐一檢視下列要點，即可詳實評估網路效益運用時機與部署方式：

- **瞭解複雜性：**指揮官必須瞭解，命令愈複雜，就要花費更長時間、投入更多資源執行。網路作戰環境的變數族繁不及備載，因此，下令遂行網路戰即為一道繁瑣的命令。
- **備便戰場：**表面上看似簡單的一紙命令，可能須花費數週以上進行整備。過去可能

只須花幾秒鐘、發起一波動能打擊，即可將一個防空飛彈連全數殲滅。但是，如果場景轉換至網路作戰，可能要花上好幾個月，網路作戰單位須突穿重層網路與防火牆，才能夠在適當時機發起攻擊。舉例來說，網路指揮部在支援戰術單位時，務必確保作戰區先行完成備便，才能夠支援戰術層級的網路作戰行動。

- **著重作戰效益，而非特定能力：**船艦上與其他戰術層級的指揮官不可能具備網路領域專業知識，因而無法依照當前情況，直接選定特定網路戰工具。相對地，當其

與戰略與作戰指揮層級的網路戰單位並肩作戰時，反而應要求相關單位運用適切武器、發揮特定作戰效益，以支援所望作戰目標。

- **瞭解風險：**網路效益總是會產生意想不到的後果。兵力展示舉措無疑會喪失特定能力。同時，在針對快速癱瘓與殲滅目標作戰效果，則應秉持節約兵力的原則，謹慎運用，因為他們容易遭敵反制而無用武之地。作戰效益愈顯著、愈常投入戰場的網路戰工具，愈有可能喪失其能力。欺敵或低階效益有限的手段反而有較佳戰場存活率。

最後，如果美海軍希望在二十一世紀有效遂行作戰，各級指揮官就須具備部署與運用各式網路工具的能力。然而，海軍與陸戰隊能夠一如既往，仿效常規武器的武獲流程，以進行網路武器的設計、測試與部署——此種謬論也該適可而止。為能達到有效遂行現代化作戰，領導者必須改變思維，調整網路武器運用概念，並以作戰效益選擇武器。

遵循此戰略的指揮官，必能在戰時成功發揮網路能力與所望效益，而將網路戰的潛力發揮到極致。

作者簡介

Eric P. Seligman為美海軍後備役部隊少校，目前編配於第3艦隊情報暨資訊作戰處(Intelligence and Information Operations, N2/N39)擔任後備役處長。

Reprint from *Proceedings* with permission.

註釋

1. U.S. Department of Defense, *Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, March 2017).
2. MIDN 3/C Edwin Lopez, USN, “Call of Duty: A Prediction of Future Wars?” *USNI Blog*, 22 April 2021; Amber Corrin, “Air Force Calls for Hybrid Approach to Cyber Warfare,” *Defense Systems*, 22 October 2010; and Alexander Kott, “Overview of Cyber Science and Technology Programs at the U.S. Army Research Laboratory,” *Journal of Cyber Security and Information Systems* 5, no. 1 (December 2016).
3. Ordtech Industries, “Mk82 500 Lbs Aircraft Bomb,” www.ordtech-industries.com/2products/Bomb_General/Mk82/Mk82.html; R. Karl Zipf Jr. and Kenneth L. Cashdollar, “Explosions and Refuge Chambers: Effect of Blast Pressure on Structures and the Human Body,” Centers for Disease Control, National Institute for Occupational Safety & Health, www.cdc.gov/niosh/docket/archive/pdfs/NIO_SH-125/125-ExplosionsandRefugeChambers.pdf.
4. Microsoft, “Operation System Version,” Windows App Development, 5 November 2021, docs.microsoft.com/en-us/windows/win32/sysinfo/operating-system-version.
5. VADM Kevin D. Scott, USN, Joint Publication 3-12: *Cyberspace Operations* (Washington, DC: Joint Chief of Staff, 5 February 2013).
6. Andru E. Wall, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Cover Action,” *Harvard National Security Journal* 3, no. 1 (2011): 85-141.
7. Kimberly K. Watson, “Deploying Indicators of Compromise (IOCs) for Network Defense,” *Cybersecurity Automation and Threat Intelligence Sharing Best Practices* (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, February 2021).
8. David E. Sanger, “A Botnet Is Taken Down in an Operation by Microsoft, Not the Government,” *The New York Times*, 10 March 2020.