● 作者/Don Gomez ● 譯者/李育慈 ● 審者/馬浩翔

因應資訊泥巴戰

Canceled[1] in Combat: Get Ready for Smear War

取材/2021年6月美國海軍學會月刊(*Proceedings*, June/2021)

今日個資取得相對容易，資訊泥巴戰難以避免，加上敵人網路能力日益增強，未來戰場更形兇險。唯有指揮鏈上下信任，方可使官兵備便因應數位化抹黑攻擊。

(Source: DVIDS& USN/ Kelsey Hockenberger)

過去一年來，伊朗海軍革命衛隊(Revolutionary Guard Corps Navy)與美國及其盟友間以牙還牙的小規模衝突日益白熱化。伊朗砲艇例行挑釁美軍聯合巡邏，猖狂穿越編隊，險象環生，幾乎相互碰撞，試圖煽動具攻擊性的回應。聯軍自制避免災難發生，但此種情況顯示有可能衝突。

試作此想定：在重大衝突升高之際，一艘黎明前在波斯灣巡邏的美軍驅逐艦遭到一批小型無人機接連攻擊。當太陽在波斯灣升起，這艘驅逐艦甲板上冒出濃濃黑煙往天空竄升的景象出現在伊朗國家電視臺上，繼而充斥在美國社群媒體與有線電視節目中。驅逐艦艦長瓊斯(Harvey Jones)中校趁著努力消滅火勢之際錄製一段聲明，讚揚麾下士兵的韌性，矢言會追究這場攻擊。這支短片由美國第5艦隊公共事務小組發布，旋即被大量瘋傳，瓊斯中校一夕之間成為媒體焦點。

在這場攻擊事件後，第5艦隊開始採取行動，試圖透過文攻武嚇來逼迫伊朗自制。一支規模龐大的聯軍艦隊刻意在鎂光燈下開始緩慢進逼伊朗岸邊軍事設施。領導高層受到媒體新寵瓊斯中校所激勵，將他當作這場行動的「門面」。媒體詳細報導受損的驅逐艦，將其視為美海軍的主要回應，而瓊斯中校更接受許多媒體訪談，讚揚區域夥伴，以及其他們在面對卑劣攻擊時所展現的韌性。[2]

該行動緊接著被區域與國際媒體臆測為聯軍可能發動反擊。以受損驅逐艦作為前景，遙遠的伊朗海岸線作為背景，強大意象在媒體上廣泛傳播，還有好戰評論家激動呼籲有仇必報。瓊斯在有線新聞網上被稱為「貨真價實」的英雄，他的尖銳言論被當作「迷因」而廣泛傳播。瓊斯雖然對受矚目感到不自在，卻也深知他的公眾角色

是為了更遠大的目的。

翌日早晨在艦艇上，瓊斯中校開始查看他的電郵。他快速瀏覽道賀與支持訊息，忽略來自反美人士的死亡威脅。在匆匆一瞥中，他的目光盯住一封郵件主旨，寫著來自五角大廈一位海軍官校同袍的「警告」──哈維，不確定你是否看到，但現在風潮開始轉向了。

軍事欺敵、深偽與駭客

為瞭解當前與未來資訊戰威脅，有必要辨明可用之特定戰術，以及其近來如何被運用。假電郵螢幕截圖是軍事欺敵方式之一。聯合準則將軍事欺敵定義為「蓄意誤導敵方軍事、準軍事或暴力極端組織決策者的行動，從而促使敵方採取有助我方達成任務的特定行動(或不作為)」。[3] 在瓊斯中校的小故事中，欺敵行動的目標對象有權限將瓊斯逐出指揮圈的領導高層，目的是剷除公眾關鍵影響人物。

儘管捏造電郵並在網路上傳播在技術上並非難事，未來軍事欺敵卻可能複雜得多。我們現正處於「深偽」時代，就連門外漢都有能力製造幾乎難以辨明真偽的偽影音。[4] 歷史殷鑑，證明偽音訊或偽公告的效力(參見偽造信在「肉餡行動」[Operation Mincemeat]中的角色)。[5] 瀏覽欺敵信件或電郵是一回事，但若在影音資料中出現海軍指揮官作出污衊麾下官兵或上級機關的言論呢？人們總是相信所見，而這些深偽作法係利用社會對影像的偏見，尤其是透過影音。深偽技術已存在，認為其不會被用在未來衝突上未免顯得過於天真。

典型的駭客行動雖不常被視

兩棲船塢運輸艦的指揮官在巴布亞紐幾內亞的莫爾茲比港接受當地媒體採訪時；說明「深偽」時代可能會在幾分鐘內提升到國際重要性，要求高級軍事領導人立即做出反應。(Source: USN/ Anaid Banuelos Rodriguez)

為資訊戰，卻可輕易加以武器化。每個人，包括資深軍事領導人，都容易遭駭。過去十年來，不計其數的個人與組織駭客已使敏感資料公諸於世。2014年索尼(Sony)影業遭駭事件或許是最著名的例子。當時索尼影業的私密資料遭竊取並公諸於世，真實世界中導致的後果包括在據稱有北韓駭客要發動武裝威脅後，索尼決定取消《名嘴出任務》(*The Interview*)電影在戲院放映。[6]

一名美軍眷屬展示她收到來自自稱伊斯蘭國支持者但實則為俄羅斯間諜恐嚇訊息的螢幕截圖。美國的敵人將目標放在傳統戰士以外的人。

國家與非國家敵人有能力聯手駭入關鍵節點，且其製造逼真深偽影音的能力提升，在在使瓊斯中校的想定恐怕成真。美國敵人已採取欺敵與網路戰爭。在美國與伊斯蘭國衝突最烈期間，所謂的「網路哈里發」(Cyber Caliphate)組織整理並且公開美軍與眷屬名單及其個資，包括電話號碼、電郵與住家地址。這些據稱是伊斯蘭國行動者亦在社群媒體上威脅軍眷。在發生這些威脅時，網路上也在流傳伊斯蘭國在中東及各地暴行的影片，嚇唬軍人家屬。直到近幾年美國才得知，這些威脅實則來自假扮成伊斯蘭國駭客的俄羅斯特務。[7]

俄羅斯亦在烏克蘭採行類似的資訊戰戰術，以簡訊通知軍人家屬該名軍人已遇難，以蒐集電子簽章。[8] 美國的敵人對於遂行層層欺敵作為以達目的毫無歉疚之意，並經證實將傳統定義上的平民當作攻擊目標。

內部威脅

儘管美國的敵人從外部施壓，美軍本身面臨之內部壓力卻削弱有效因應欺敵性攻擊個人的能力。首先，美國是個開放社會，重視言論自由，因而增加其暴露在外來欺敵與操弄的危險性。其次，當涉及社群媒體與公共關係時，軍事領導人傾向採取謹慎而不願承擔風險的作法。在媒體或網路報導上過度謹慎的軍事領導高層，可能被指責為自私自利。最後，各級指揮官可能被迫基於當前資訊環境，或回應上級單位期待而迅速做出決策。總而言之，這些都是敵人可用來取得戰略優勢的特性。

言論自由是美國社會偉大的因素之一；即使政府應不遺餘力防止外國勢力滲透，自由社會仍應維護言論自由。然而，過去軍事領導人一直無須對付如此

美國國防部在回應重要議題時，均統由國防部發言人對外回應，以減少議題延燒的風險。2021年12月20日，美國國防部發言人柯比(John Kirby)在例行記者會，回應「反極端主義活動的工作小組報告」相關議題。
(Source: US DoD/ Chad McNeeley)

鋪天蓋地且充滿政治色彩的資訊環境。無論喜歡與否，許多人(包括軍人)自身都是媒體平臺。有問題的言論或訊息會在幾分鐘中內取得，並升級成具有國際重要性，而須軍事領導高層立即回應。此外，儘管陷阱重重，不願與媒體或公眾交涉的軍方所栽培出來的領導幹部如今受鼓勵要經常與媒體打交道。[9]

總之，軍方擁抱推特、部落格與播客等新媒體是正面之舉，且似乎無可避免要一改過去單位政令與照本宣科的媒體訪談。儘管如此，除在作戰安全方面的顧慮外，仍極少有關此現象的二階或三階段效應討論。敵人已從這些社群媒體取得美軍個資，倘若認為對方不會將之武器化以遂行軍事和政治目的，實是愚蠢至極。

領導高層可能會覺得因應新興危機極具壓力，尤其被誤會在質疑部屬品格。敵人企圖毀謗現役指揮官後，將緊接著促使民眾、專家及政治領導人要求回應。若敵人成功透過欺敵、深偽或以駭客方式發布貶斥訊息，則各階層領導人將被迫採取行動滅火，在此想定中可能意味著在關鍵時刻某位指揮官或人員得調離要職。

軍方優勢──信任

抵禦抹黑戰的贏面在於信任，信任夥伴、體系以及國家。未來衝突在個人層面的艱險程度前所未見。海軍應準備因應的想定是，低階官兵與高階指揮官皆可能在集合欺敵、深偽技術與駭客的資訊環境中遭到毀謗中傷。海軍領導人應體認到這場賭注極大，且競爭場域無所不在。可預期的是，敵人會利用每項可供利用之工具來破壞美國作為，即便是最底層亦復如此。唯有指揮鏈上下信任，才可讓官兵準備因應數位抹黑攻擊。

即便是最心存良善的領導人都會在這件事情上犯錯。他們可能會發現處在特定情境下，似乎真有針對美國重要領導人採取顛覆資訊戰。透明至上。美國民眾必須信任軍方會對真正違法者負起責任。基於這層信任，軍事領導人便能在敵人說謊並且試圖欺瞞之際承擔更多風險。

泥巴戰山雨欲來。今日取得個資相對容易，使泥巴戰無可避免，加上敵人日益增強的網路能力，以及展現涉入欺敵戰的意願，使得未來戰場變得更為兇險。美軍領導人應毫不猶豫接受敵人會為遂其目的而殘害官兵弟兄姊妹。毫不令人意外，他們會加以抹黑殘害。

未來美軍全體官兵皆可能遭毀謗中傷，因此，應透過平時生活、部隊訓練及作戰任務，建立彼此的信任感。

(Source: US DoD/ Tabitha Castellano)

註釋

1. 「解職」(Canceled)意指由於確實犯錯或被認定犯錯而被突然終止工作或職位，通常發生在此類過錯被加強檢視的階段中。
2. 沒有任何有關「敘事」的共通定義。筆者將敘事定義爲特定時刻的主導想法。這是引起社會集體注意與想像的整合資訊。近期有關主導敘事的案例是#MeToo運動與#BlackLivesMatter運動。主導敘事中所發生的事件，可能會透過該敘事的濾鏡加以處理。
3. Department of Defense, DOD Dictionary of Military and Associated Terms (January 2021).
4. Joe Littell, "Don't Believe Your Eyes (or Ears): The Weaponization of Artificial Intelligence, Machine Learning, and Deepfakes," *War on the Rocks*, 7 October 2019.
5. 「肉餡行動」是第二次世界大戰期間英國成功遂行的欺敵行動，其利用僞造文件誤導軸心國對同盟國於1943年施行「地中海入侵計畫」的判斷。
6. Andrea Peterson, "The Sony Pictures Hack, Explained," *The Washington Post*, 18 December 2014.
7. Raphael, Satter, "Russian Hackers Posed as IS to Threaten Military Wives," *The Associated Press*, 8 May 2018.
8. Lucas Scarasso, "Text Messages from Hell: Restraining and Information Warfare," *War on the Rocks*, 21 April 2020.
9. Robert Abrams, "Social Media: Senior Leaders Need to Get on the Bus," *From the Green Notebook*, 8 October 2019; Patrick Donahue, Mick Ryan, and Tammy Smith, "Why We Tweet: General Officer Use of Social Media to Engage, Influence, and Lead," *The Strategy Bridge*, 7 September 2020.