



● 作者/Will McGee ● 譯者/周敦彥 ● 審者/丁勇仁

強化網路安全

Improve Cybersecurity for Information System Defense

取材/2021年8月美國海軍學會月刊(*Proceedings*, August/2021)

中共之先進駭客技術，已造成許多資訊安全防禦系統不堪一擊，若軍事系統亦遭受攻擊，後果則不堪設想。故設計和運用能夠防止遭受侵入的資訊系統，以及不會被駭客攻擊的武器系統，對於建軍備戰而言至關重要。

在2015年，中共駭客從美國人事管理局(Office of Personnel Management, OPM)資料庫中竊取了數百萬份人事檔案和安全許可紀錄。該局鬆散的安全防護，尤其是未能採取業界標準的安全措施，如「二因子鑑別」(Two-factor Authentication)，使得中共安全部門駭客得以輕易取得敏感的寶貴資料。

這並非單一事件。在過去十年，發布重要數據洩露的頭條新聞已經是司空見慣。小型公司、《財星》500大企業，以及州與地方政府都受到攻擊。就連軍方在內的聯邦政府都無法倖免，網路駭客還不斷刺探並試圖侵入整體國家安全資訊架構。這些攻擊往往奏效：檢視中共殲-31戰機，就會發現其和美國F-35戰機非常相似，而中共近岸作戰艦，看起來幾乎是美海軍獨立級近岸作戰艦的複製品。¹ 資訊戰在未來衝突中，將扮演前所未有之角色。

勃克級飛彈驅逐艦約翰保羅瓊斯號(USS *John Paul Jones*)在實彈測試期間發射標準六型飛彈。未來的武器系統在撥發使用前應該進行僅針對網路安全的測試。



防止技術資訊洩露是國家安全議題，因為一旦敵人取得這些資訊，將會削弱用來保護國家安全的工具。這不僅是戰略議題，在戰術層面，保護作戰部隊之計畫文件和情報成果至關重要，因為能夠進入友方資訊系統的對手，將會察覺部隊作戰企圖。例如，敵人如果得知友軍針對特定前進軸線進行地形研究，將會沿此路線完成抵抗整備，而使友軍奇襲的效果盡失。

美國國防部正在打一場資訊戰，而勝利端賴其網路和裝備系統的安全性。設計並且運用能夠防止遭受侵入的資訊系統，以及不會被駭客攻擊的武器系統，就是在資訊環境中建立防禦能力——在資訊環境中很難剝奪對手的優勢。

然而，國防部，特別是採購部門，在執行網路安全管制方面效果不彰。2018年政府問責署(Government Accountability Office, GAO)的一份報告中，標題直言不諱，明定為「武器系統網路安全：國防部才剛開始解決大問題漏洞」，報告指出在2012至2017年間，國防部測試人員經常發現，研發中的武器系統存在重大網路安全缺陷。在測試期間，假想敵團隊人員運用之「初、中級工具和技術」，能夠輕易破壞(侵入)進而接管武器系統，其肇因自安全管制不足或配置不當。報告中所揭露最嚴重的問題是，在系統測試期間發現許多網路安全缺陷，卻仍未獲得解決。²

軍事採購部門早就跟不上技術變革的速度，只能勉力加快各種系統設計和投入運用的速度。因此，現今武器採購最主要的重點為速度——快速研發、生產和運用，以確保盡快讓戰士可以獲得最新的技術。強調快速可能會增加整體的成本，

而這可能是政府問責署所發現導致網路安全問題的成因之一。

美國國防部如何使裝備系統安全與快速裝備研發相配合，同時盡可能降低軍種成本並提升部隊戰力？以下個案研究概述了近期網路安全測試活動之最佳作法和經驗教訓，應有助於回答此問題，並作為未來網路安全測試之參據。

測試新圖像系統的網路安全性

「美陸戰隊地理空間情報-分散式共同地面/水面系統」(Distributed Common Ground/Surface System-Marine Corps Geospatial Intelligence, DCGS-MC GeoInt，以下稱DCGS-MC GeoInt系統)是最近加入美陸戰隊情報單位裝備架構的系統。電腦藉由提供更強大的分析能力使各個情報系統現代化，同時減少各種設備的體積和重量。作為地理空間情報系統，很可能成為敵方網路駭客的優先目標，藉以刺探有關友軍作戰企圖之徵候。

由於部署該能力迫在眉睫，DCGS-MC GeoInt系統專案辦公室自專案任務賦予到系統解繳全面投入艦隊陸戰隊(Fleet Marine Force)止，耗時不到30個月。該系統的敏感性導致其被指定為「採購分類IV(含測試與評估)」(Acquisition Category IV[T])，在撥發運用前應完成作戰測試。筆者曾受命擔任作戰測試計畫官並負責測試事宜。

基於DCGS-MC GeoInt系統須迅速撥交給各部隊，以及資訊科技裝備之獨特性，我的工作團隊認定一般作戰測試程序並不適用該系統。例如，沒有必要依循往例在全作戰測試項目中確認系統

的可靠性、可取得性，以及可維護性，因為操作單位能夠以最低成本，輕易更換系統中的大部分元件。

然而，確定該系統在網路競爭環境中，針對指定任務所能發揮之效能至關重要。因此，我們決定放棄評估該系統的適用性與有效性，轉而專注其存活力。DCGS-MC GeoInt系統是第一個接受僅針對網路安全(Cybersecurity-only)進行作戰測試的美陸戰隊裝備系統。作為系統設計流程的一部分，專案辦公室必須測試網路安全管制，而且DCGS-MC GeoInt系統的網路安全管制，在作戰測試開始前要經過嚴格檢查。然而，政府問責署指出，以前發現的安全問題並不表示已經解決。僅針對網路安全的作戰測試對戰士而言很有價值，因為在裝備撥交部隊前，獨立單位會評估安全狀態。

僅針對網路安全的作戰測試程序包含三個主要項目：合作漏洞侵入分析(Cooperative Vulnerability Penetration Analysis, CVPA)、網路安全圖上兵推，以及對抗性評估。每個測試項目

都有不同目的，而且相互關聯，所以較晚執行的項目會得到整個過程中蒐集而來的數據。

合作漏洞侵入分析會檢查系統，以確定系統是否因為配置不當而存在重大漏洞。³就DCGS-MC GeoInt系統而言，由於該裝備系統位於猶他州洛根(Logan)的開發商工廠正進行可靠性測試，而作戰測試團隊身處維吉尼亞州匡堤科(Quantico)，因此我們決定將猶他州的系統與維吉尼亞州北部的測試人員進行邏輯連接，來執行合作漏洞侵入分析。這節省了時間和金錢，無須將設備運送

至新地點後重新組裝。合作漏洞侵入分析的測試結果在完成記錄與分析後，將送交專案辦公室。

網路安全桌上兵推召集系統操作人員、專案辦公室工程專家、作戰測試團隊，以及假想敵團隊成員，共同執行對抗性評估。運用合作漏洞侵入分析的結果，配合系統圖示，在此圖進行兵推可以推斷對系統產生影響所需要之時間。此項目耗時一週，獲得的結果可提供對抗性評估之分析模型所用。

對抗性評估是網路安全評估過程中最重要的項目。假想



中共殲-31隱形戰機在「中國國際航空航天博覽會」期間進行飛行展示測試。令人擔憂的美國網路安全可能讓中共取得重要的隱形技術資訊，應用於其自身的武器研發。



美陸戰隊的新型聯合輕型戰術輪車。雖然裝備發生工程上的缺陷需要經過駐地或廠級維修方能再度使用，但是在網路安全評估中所發現的漏洞可以在系統撥發後進行修補。(Source: Oshikosh Defense)

敵團隊會嘗試在美陸戰隊操作人員使用該系統時，侵入並且影響系統。假想敵團隊之諸般手段會被記錄下來，如此測試團隊就可以判定實力相當的對手，需要多長時間方能突破系統。在分析所蒐集的數據後，將作為決定系統能否撥發運用之依據，截至本文撰寫時，該系統已運往部隊。

DCGS-MC GeoInt系統的對抗

性評估與標準評估方式有兩個重大差異。首先，情報系統是透過「保密網路協定路由器網路」(Secret Internet Protocol Router Network, SIPRNet)運作，測試團隊在專案辦公室的支持下，決定對抗性評估也應該使用該網路。這似乎是常識，但標準作法是在獨立網路上進行作戰測試，以防止假想敵團隊的網路攻擊，進而影響其他網路運作的

可能性。雖然其他系統在連接保密網路協定路由器的網路時已經完成測試，但是情報系統的狀況不同，因為該系統的正常運作需要與僅內建在保密網路協定路由器網路內的資料庫和伺服器進行互動，所以連接該網路是一個重要功能組成，而不只是輔助功能。

此測試的第二個不同之處是系統複雜度。DCGS-MC GeoInt

系統是專門為資料處理與分析而設計的電腦，因此該系統執行網路安全作戰測試之複雜程度，遠高於戰術車輛的資訊科技系統，或美陸戰隊之其他裝備。

為了進行評估，美陸戰隊情報處(Marine Corps Intelligence Activity, MCIA)以及美陸戰隊網路安全指揮部(Marine Corps Forces Cybersecurity Command, MarForCyber)派遣人員支援測試團隊。前述單位派遣兩名合格的圖像和地理空間情報分析人員，在他們為美陸戰隊情報處產製情資時，美陸戰隊網路安全指揮部的假想敵團隊試圖侵入系統。參與一般作戰測試的操作人員，通常是在人為構建的場景中作業，且測試成果棄之不用，然而在本次測試規劃中，操作人員構建實際成果，因此兩名訓練有素的操作人員節省了超過160小時的工作時間。

DCGS-MC GeoInt系統對抗性評估開創新局面，破天荒在實際的保密網路上對美陸戰隊的情報系統進行了作戰測試，是首次由操作人員產製實際情報成果來執行系統作戰測試，也是迄今為止最複雜的美陸戰隊系統網路安全測試。⁴

未來測試的考量因素

下一場戰爭將是一場系統戰爭：網路和設備安全將和以往傳統戰爭中的自然地形一樣重要。美國政府現行系統並沒有準備好在這種環境下克敵制勝。

美國國防部的採購部門在這場角力中扮演了極重要的角色。藉由在系統開發期間，找出和修正網路安全問題，採購部門可以防止系統漏洞造成

部隊操作人員的風險。

由於情報系統資訊非常敏感，情報部隊的每一項資訊科技專案，都必須經過包括作戰測試的全面網路安全評估。正如DCGS-MC GeoInt系統測試所證明，藉由識別實際解決方案間細微差別之方式，以及願意僅針對相關特性進行有彈性的測試，作戰測試權責單位可以提升專案辦公室的重要性，並盡量降低評估的財務和時間成本，同時強化系統的品質和安全性以供部隊使用。

目前軍事採購模式要求以作戰測試結果來決定能否將裝備系統撥交部隊使用。但是就僅針對網路安全的測試而言，此要求可以放寬，以便在系統交運前後持續進行測試。由於合作漏洞侵入分析應該確認設備的安全配置，假設可滿足所有其他程式設計的需求，系統將會撥交部隊，然後在人員使用裝備時進行評估。

網路安全作戰測試與標準測試不同，因為即使發現漏洞也很少需要構改系統進行裝備實體的設計諸元。雖然設備發生工程上的缺陷需要經過駐地(Garrison)或廠級(Depot-level)維修後才能再度使用，但是在網路安全評估中所發現的漏洞，可在撥發系統後，藉定期軟體更新來進行修補。採用這種方法將節省時間，並可加快裝備系統的發展。

雖然DCGS-MC GeoInt系統為配合部署期程而提早撥交，該系統的對抗性評估和數據評估仍耗時兩個多月。在系統撥交部隊後再進行作戰測試，則對部隊和納稅人都有很大的好處。

正如DCGS-MC GeoInt系統在進行合作漏洞侵入分析期間所驗證，只要系統連接到網路，位於



不同設施的假想敵團隊人員就可以從遠端刺探。日本地區部隊所使用的系統，可由維吉尼亞州連接網路的操作人員執行評估，並透過軟體修補程序，遠端修復所發現的系統漏洞。這種方法不適用於沒有連接網路的系統，但是對於可以進行遠端評估的系統，將縮短系統開發兩個月的時間，加速武器籌獲的過程。

作戰測試必須在「準作戰」環境中進行，這通常代表在大型演習或離散測試(Discrete Test)項目時實施。對作戰部隊單位的系統進行測試時，測試團隊將建立更精確的項目(真正的作戰環境，而非準作戰環境)，採取適切的防干擾措施，以避免影響實際行動，其中操作人員是處理實際的情報，而不是產製測試項目結束後即丟棄的資料。此舉提高了測試的價值，同時將對支援作戰部隊單位的影響以及專案辦公室的成本減到最低。DCGS-MC GeoInt系統對抗性評估證明此法可行。

在系統撥交後執行網路安全評估，可以滿足重複測試的需要。政府問責署的報告指出，主要武器系統存在漏洞，在測試期間被發現卻未修復。如果在作戰測試期間發現重大漏洞，作戰測試權責單位在系統投入使用後，也可以編組進行第二次測試，以確認漏洞獲得因應。

在作戰環境中進行測試，也可以激勵各專案辦公室，讓他們參與將部隊中的武器系統上線。通常，系統在撥交部隊使用後，由單位使用者負責完成系統設定，以符合權責長官的操作需求，文件會概述系統在網路上的運作方式。對於美陸戰隊而言，這意味著四個獨立節點(三個美陸戰

隊遠征軍和美陸戰隊情報處)的人員，除了執行日常任務外，都必須獨立維持系統運作。DCGS-MC GeoInt系統的對抗性評估是在實際的保密網路協定路由器網路上進行，因此專案辦公室必須在測試項目開始前，協調完成系統連線並開始運作，而不是在系統撥交部隊使用後，由操作人員自行負責。

將此要求標準化，可減輕部隊的負擔。每當新資訊系統撥交部隊時，最具經驗之專案辦公室可藉前述簡化之流程，代表作戰部隊完成協調任務。

作者簡介

美陸戰隊Will McGee上尉畢業於美國海軍官校。在維吉尼亞州匡堤科的美陸戰隊作戰測評處擔任情報部門的作戰測試官。

Reprint from *Proceedings* with permission.

註釋

1. Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, 21 April 2020; www.wsj.com/articles/SB124027491029837401.
2. James C. Bussert, "Coastal Catamarans Serve Chinese Littoral Needs," *Signal*, 1 June 2015; www.afcea.org/content/Article-coastal-catamarans-serve-chinese-littoral-needs.
3. Government Accountability Office, *Weapon System Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC: October 2018); www.gao.gov/assets/700/694913.pdf.
4. Director Operational Test and Evaluation, "Cybersecurity OT&E—Guidance," Washington, DC, undated.