● 作者/Jonathan Hayes ● 譯者/張彥元 ● 審者/劉宗翰

主動網路防禦新論

A New Way to View Active Cyber Defense

取材/2019年2月美國海軍學會月刊(*Proceedings*, February/2019)

各項網路能力發展與世界互聯程度愈來愈高，圍繞著網路防禦的問題也應運而生，主動網路防禦就是重點之一，本文運用巡邏基地模式類比於主動網路防禦的作爲，可爲瞭解主動網路防禦提供另一個視角。

網路世界已經不再僅是科技達人的競技場。由於網路空間與日常的種種活動息息相關，因此每個人對各種網路相關概念至少也要有基本的理解。主動網路防禦(Active Cyber Defense, ACD)就是這些概念之一。

在陸、海、空及太空等領域，主動防禦的界定相對較為容易，但在網路領域卻未盡如此。何謂主動網路防禦目前仍未有一致的看法。然而，大多數定義均納入採取行動的概念。許多防禦措施與攻勢作為僅有意圖上的差別。巡邏基地作業的軍事準則，可為瞭解主動網路防禦提供一個模式。

以巡邏基地作業為類比

首先，主動防禦不能取代被動防禦。巡邏基地位置的選取，須以隱密與防護為考量，其建置須儘量不為人知。基地周邊必須構建堅實的防禦，用偽裝作戰陣地與交叉火網覆蓋基地外圍。巡邏基地防禦手段與許多被動網路防禦概念相同，例如執行進出管制、網路衛生作為(cyber hygiene practice)，以及建立防火牆等。[1]

至於主動網路防禦則與巡邏更為密切相關。

巡邏的型態主要有兩種：偵察巡邏與戰鬥巡邏。偵察巡邏係針對利害區所採取之周密行動。網路上的偵察巡邏是主動網路防禦的關鍵要素，且可能是預防或覺察攻擊的主要手段之一。然而，此手段常引發合法性顧慮與當局關切。[2] 網路偵察與網路間諜活動主要的差異在於意圖，而意圖則往往難以檢驗。

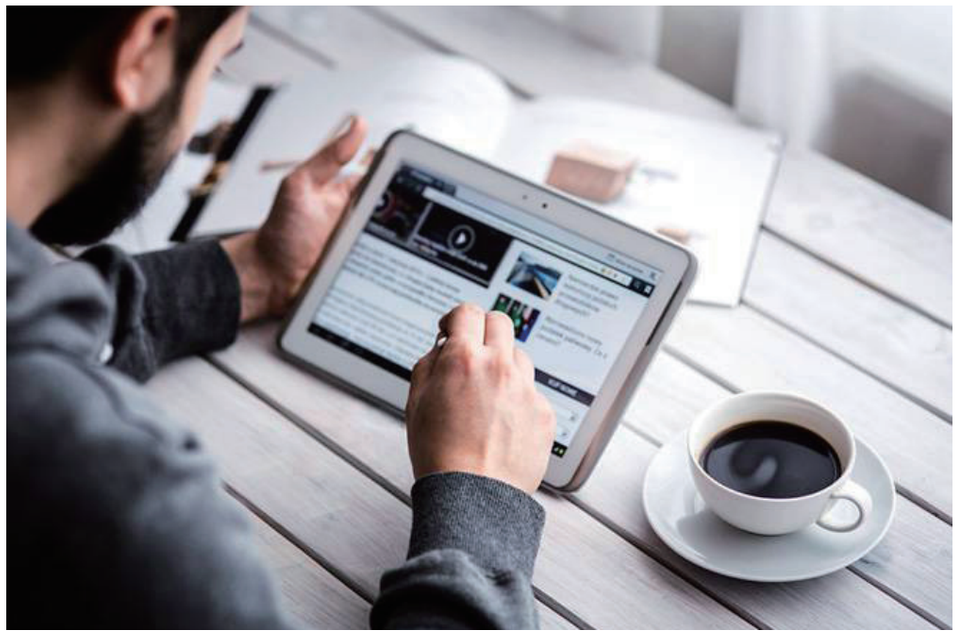
戰鬥巡邏一般可區分為四種型態：安全巡邏、伏擊巡邏、連絡巡邏、突襲巡邏。安全巡邏係執行巡邏基地周邊地區之搜索，並與所發現之敵接戰，相當於網路的入侵偵測/預防系統，負責巡查受防護系統，以找尋遭危害的跡證。安全巡邏係由指揮部單位策劃發起，但執行階段則由各單位獨立執行任務。入侵偵測/預防系統亦可以採行類似的方式：經系統管理員啟用後，入侵偵測/預防系統可找出整個系統中任何可疑的活動並進行自動封鎖。入侵偵測/預防系統亦可識別任何

(Source: USMC/Samantha Schwoch)

與系統管理員的聯絡(類似安全巡邏向指揮部回報)，並由人員在回報體系中決定是否須採取進一步的作為。

伏擊巡邏相當於「蜜罐誘捕系統」(honeypot)，埋伏在敵可能活動之區域，有時更設下誘餌，倘若敵出現則遂行接戰。[3]網路伏擊顯然設置於受防護系統之內部，以攻擊者希望獲取之資訊為誘餌，且一旦設置後就能自動反應。無辜者亦有遭誘入的危險，但可能性甚低。「蜜罐誘捕系統」設計可能不會使隨機搜索用戶在系統內停留，只有具不良意圖之行為者才會陷入其中。

連絡巡邏係於巡邏基地(受防護之系統)較外圍之區域活動，可用以發現敵軍或保持接敵。連絡巡邏的網路版係利用所謂白蟲(white worms)或其他手段「還擊」而保持接敵狀態。[4]然而，攻擊者可採取如「網際網路協定位址欺騙」和「斷點」等許多方法，隱藏其真實位置，因此反擊效果依其型態而有所不同，自動化反制措施也有可能影響已遭危害但卻是無辜的系統。



由於網路空間與日常種種活動息息相關，因此人人對於網路相關概念也應該要有基本理解。(Source: Wiki)

自動回溯追蹤攻擊來源的網路防禦，對每個單位或是一般民眾，均為適合的手段。然而，具較高「破壞性」的反制措施，諸如傳回資料或對攻擊的系統造成永久性破壞等，執行前應先行向權責主管之政府單位提出申請並獲核准。反擊強度需視損失可能造成的衝擊而定。例如，主管單位可能僅同意影片串流公司網飛(Netflix)可對攻擊系統進行回溯追蹤，以及以有限的搜索來瞭解系統屬性；然而，主管單位亦可預先核准全面的自動逆襲，以免可能發生停電而造成嚴重影響。這相當於在制定不同強度之接敵計畫並造成不同程度之可能周邊損害時，核准給予連絡巡邏不同形式的火力支援。

最後一種形式為突襲巡邏。一般認為，除非能辨識攻擊者身分並有機會取回或銷毀因遭受攻擊而失竊的資料，或是為了防止/化解攻擊，網路版的突襲乃屬攻勢作為。突襲執行係經縝密的規劃、高度協調、特定任務的有限目標巡邏，以及

撤退計畫。突襲巡邏有高度的資訊需求，民間公司若未進行詳細的偵察，不太可能獲得此類資訊，而這種偵察作業必須獲得政府核准。同樣地，任何對外國系統進行入侵或造成永久性改變作為，無論是由政府或民間單位進行，均必須獲得權責政府單位核准，因為這事實上是一種攻擊。

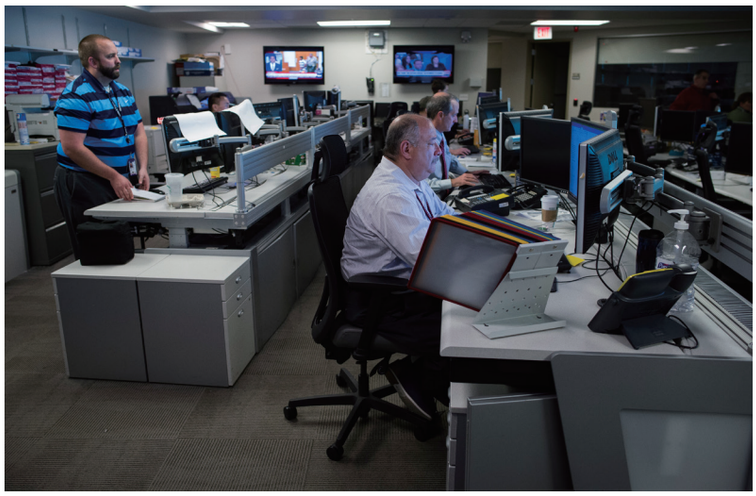
巡邏基地的啟發

隨著各項網路能力發展和世界互聯程度愈來愈高，環繞著網路防禦而生的各種問題，其增加速度可能比提供因應之道的速度來得更快。巡邏基地的模式是將一個累積多年經驗的作法跟一個相對較新且變化快速的領域做比擬，因此仍有不完美之處。但是，它為主動網路防禦提供了另一個視角，希望透過將眾所周知與較鮮為人知的兩個領域加以類比，可對吾人有所啟發。

作者簡介

Jonathan Hayes中校係美陸戰隊特種作戰司令部戰略特種作戰計畫官。他曾歷練步兵排排長、副連長、連長、副營長，並曾擔任陸戰隊特戰小組組長、副連長，以及連級分遣隊指揮官。

Reprint from *Proceedings* with permission.



隨著網路發展與全球網路互聯程度愈來愈高，網路防禦能力日益重要。圖為負責監控美國聯邦政府網路狀態的美國國土安全局網路安全與通訊整合中心。(Source: AP/達志)

註釋

1. Robert S. Dewar, “The ‘Triptych of Cyber Security’: A Classification of Active Cyber Defence,” in *2014 6th International Conference on Cyber Conflict,* ed. P. Brangetto, M. Maybaum, and J. Stinissen (Tallinn, Estonia: NATO CCD COE Publications, 2014); Irving Lachow, “Active Cyber Defense: A Framework for Policymakers,” Center for a New American Security, February 2013, www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.
2. Center for Strategic and International Studies, “CSIS/DOJ Active Cyber Defense Experts Roundtable,” 10 March 2015, http://csis.org/publication/csisdoj-active-cyber-defense-experts-roundtable; Lachow, “Active Cyber Defense”; James A. Lewis, “Cyberwar Thresholds and Effects,” *IEEE Security & Privacy* (September/October 2011): 23–29; Pierluigi Paganini, “The Offensive Approach to Cyber Security in Government and Private Industry,” INFOSEC Institute, 18 July 2013
3. 維基百科，「蜜罐專指用以偵測、抵禦或以某種方式反制未經授權操作資訊系統的陷阱。」
4. Wenlian Lu, Shouhuai Xu, and Xinlei Yi, “Optimizing Active Cyber Defense,” in *Decision and Game Theory for Security: 4th International Conference, GameSec 2013, Fort Worth, TX, 11–12 November 2013, Proceedings,* ed. Sajal K. Das, Cristina Nita-Rotaru, and Mura Kantarcioglu (Switzerland: Springer International Publishing, 2013), 206.