主動式防禦——前進滲透部署

詹祥威

網路安全與決策推演研究所

壹、前言

自 2000 年後期，隨著網路攻防技術的快速迭代與數位經濟的蓬勃發展，網路戰（Cyber Warfare）的複雜性與破壞力顯著提升，攻防雙方的「不對稱性」日益凸顯。傳統的「被動式防禦（Passive Cyber Defense, PCD）」手段，如「防火牆」、「入侵檢測系統」與「靜態修補程式」，已難以有效應對「進階持續性威脅（Advanced Persistent Threat, APT）」，及利用新興科技進行的高級攻擊手法。尤以後疫情時期，全球數位轉型加速，企業與政府機構對自動化技術，及雲端基礎設施的依賴加深，進一步擴大網路攻擊的潛在破壞面。攻擊者不僅運用人工智慧（Artificial Intelligence, AI）、機器學習（Machine Learning, ML）與大規模自動化工具，實現「精準化」與「持續性」的漏洞搜尋與攻擊，更藉供應鏈漏洞與零日漏洞（Zero-Day Exploits）滲透關鍵系統，挑戰既有防禦極限。

在此背景下，「主動式防禦」（Active Cyber Defense, ACD）作為一種「積極預防」、「動態應對」與「由情報驅動」為核心的網路安全策略，受到產官學研界的廣泛關注。相較於被動防禦的亡羊補牢模式，「主動式防禦」強調在威脅萌芽之初甚至發生前，透過「預測性分析」、「動態適應」與「主動反制」，封堵攻擊路徑、中和潛在風險並縮小影響範圍。這種策略不僅適用於企業層面的網路安全管理，更在國家安全層次展現出戰略價值，成為網路戰中實現情報優勢與嚇阻效果的關鍵手段。例如，美國自 2017 年起推動「主動式防禦」概念，透過《網路安全成熟度模型認證

（Cybersecurity Maturity Model Certification, CMMC）》與「前進防禦（Defend Forward）」政策，將其融入國防工業與軍事作戰框架，以應對來自中國、俄羅斯等國家的網路威脅。

本文以網路戰為分析框架，聚焦「主動式防禦」在國家安全層次的發展與應用，特別深入探討「前進滲透部署」的操作機制、技術基礎、規範與限制等，並藉實際案例與新興技術趨勢，探討「主動式防禦」如何重塑網路戰格局，並為政策制定者與安全從業人員提供實務參考。

貳、主動式防禦樣態

隨著 AI、量子計算與生成式攻擊技術的演進，「主動式防禦」的未來發展不僅影響網路安全生態，更將深刻塑造全球安全格局。過去面對網路攻擊的「防禦性」手段，大多為「檢測入侵程式碼」、「清洗受影響的系統」、「建立安全修補程式以阻止特定攻擊」，以及「在整個網路範圍內使用修補程式進行修護」等。相較於「被動防禦性」，「主動式防禦」通常聚焦於「預防性」與「動態的」網路安全作為，強調在威脅發生前，或在危機的初期即採取主動措施，以減輕、阻止潛在攻擊所造成的影響，並限定影響範圍。[1]

在「網路戰」的脈絡下，「主動式防禦」的範疇顯然涵蓋部分更具「進攻性」的操作，例如「前進滲透部署（Forward Penetration Deployment, FPD）」與「攻擊性網路行動（Offensive Cyber Operations, OCO）」。「前進滲透部署」主要係在敵方或目標網路中，主動建立隱秘立足點，作為情報收集、系統操控或破壞行動的跳板，著名的典型案例包括 2010 年的「震網病毒 Stuxnet 攻擊」與

[1] "ACD: Active Cyber Defense," *Information Innovation Office*, https://shorturl.at/Pn5ea. 關於被動防禦性手段，請參閱本特刊專文。

2022 年俄烏衝突中的網路戰。然而，這些行動因涉及跨境滲透與主權爭議，在《塔林手冊》（Tallinn Manual）等國際法框架下引發法律與道德爭議，其合法性與風險有待慎評估。

一、定義與演進

如前述，「主動式防禦」是一種以預防性、動態性與自動化為核心的網路安全理念，旨在主動識別、追蹤與中和威脅，降低攻擊的影響範圍。2021 年，Sven Herpig 博士的報告將其定義為：「由單一國家，或政府實體，集體實施或授權的一項、或多項技術措施，目的是消除和/或減輕特定正在進行的惡意網路操作或活動，和/或在技術上歸因於該活動，所造成的影響。」[2]

自 2017 年美國首次提出主動式防禦概念以來，其應用範圍已從企業安全擴展至國家安全層次。例如，美國國防部的《網路安全成熟度模型認證》框架，將「主動式防禦」融入「事件回應準備（Incident Response Preparedness, IRP）」、「持續監控（Continuous Monitoring）」與「定期風險管理（Regular Security Management）」等要求，強調快速回應與動態適應。

根據該框架，使用者必須建立「快速回應機制」，包括即時威脅情報共享，與事件緩解計畫，以確保在安全威脅樣態發生下可以依據事前計畫快速且有效的回應，並且進行相關通報計畫；此外，使用者必須以「零信任」為核心，持續性不間斷的實施網路監控，識別異常行為或未授權存取，並透過定期評估與更新安全控制措施，確保當前系統足以抵禦、防範已知與新興威脅。

根據較新的「主動防禦」作為，定期性的風險管理可藉由人工

[2] Sven Herpig, "Active Cyber Defense Operations - Assessment and Safeguards," *Policy Brief of Stiftung Neue Verantwortung*, November 2021, https://shorturl.at/7S56y.

智慧（AI）、機器學習（ML）與行為分析等科技，預測潛在的網路攻擊路徑，並在攻擊發生前預測及封堵漏洞，並且定期將最新威脅情資與既有資訊做整合；而在持續性的動態防禦部分，則逐漸強調藉由開發「即時適應威脅」的系統，例如自我修復網路、動態配置資源或改變系統架構以迷惑攻擊者。而事件回應準備則包含使用者運用「自動化應對」，亦即透過自動化工具快速識別與回應威脅，減少人為干預的延遲，並且快速識別和分析潛在的威脅。[3]

二、核心技術與實踐

（一）持續監控與威脅抓捕

「持續監控」是「主動式防禦」的核心，仰賴「安全資訊與事件管理（Security Information and Event Management, SIEM）」系統「實時」分析、紀錄網路流量、日誌與用戶行為，快速識別異常活動或未授權存取。人工智慧（AI）與機器學習（ML）技術進一步提升威脅抓捕（Threats Hunting）的精準度，通過行為分析與模式識別，預測潛在攻擊路徑並提前封堵漏洞。例如，AI 驅動的異常檢測系統可在毫秒內辨識釣魚攻擊的早期跡象，有效減少反應與作動的時間差。此外，生成式 AI 的應用正改變威脅抓捕的模式，甚至可藉由「模擬攻擊場景」生成虛假資料，誘導攻擊者或提早暴露意圖。

（二）動態防禦系統

動態防禦系統強調適應性與迷惑性，旨在降低攻擊者的成功率並增加其行動成本。核心技術包括「自我修復網路」、「動態資源配置」與「誘捕技術（如蜜罐與蜜網，Honeypots/Honeynets）」。例如，美國國防高等研究計劃署

[3]〈什麼是 MDR？MDR 服務對企業的好處是什麼？〉，《TeamT5 Media Center》，2023 年 7 月 17 日，https://shorturl.at/iii59。

（Defense Advanced Research Projects Agency, DARPA）的「任務導向可恢復網路」（Mission-Oriented Resilient Clouds）計畫，開發了能夠「動態重新配置」的雲端架構，在檢測到攻擊時自動隔離受損節點並重新分配資源。[4]「誘捕技術」則藉由部署假系統或資料，誘導攻擊者誤入陷阱，同時收集其手法與來源資訊，進而強化、改善整體既有防禦策略。

（三）自動化回應

「自動化回應」技術利用 AI 與自動化工具，實現對威脅的快速識別與處置，顯著減少人為干預的延遲。例如，AI 驅動的威脅回應系統可在檢測到惡意程式後，於毫秒內隔離受感染節點、阻斷惡意流量並啟動修復流程。這種能力在應對大規模分散式阻斷服務（DDoS）攻擊或勒索軟體時尤為關鍵；自動化回應可同時與威脅情資平台整合，根據實時情報動態調整防禦措施，確保系統對新興威脅的適應性。

（四）威脅情資共享

「威脅情資共享」是主動式防禦中「集體防禦」概念的重要機制，藉政府、產業、國際組織等跨領域、部門的合作，共享即時威脅情報與攻擊模式。例如，企業可透過如「美國國防工業基地網路 DIBNet」、「NATO 任務網路 FMN」等，獲取最新的「零日漏洞」資訊，並依據情資提前修補系統弱點；另一方面企業亦時常針對 APT 攻擊發布公開報告，揭露最新手法與觀察重點等。國際層面的情報共享則在網路戰中尤為重要，例如 2022 年俄烏衝突期間，烏克蘭與西方國家共享俄羅斯網路攻擊的情報，成功減緩了多起針對關鍵基礎設施的攻擊。

---

[4] "MRC: Mission-Oriented Resilient Clouds," *Information Innovation Office, DARPA*, https://shorturl.at/vSwLJ.

前述諸點在企業間業已廣泛適用，例如金融機構利用SIEM與誘捕技術防範釣魚攻擊，製造業則透過自動化回應保護供應鏈安全。然而，在網路戰的國安層次，主動式防禦進一步融入更具進攻性與爭議性的策略，特別是「前進滲透部署」與「攻擊性網路行動」，以實現情報優勢與戰略嚇阻。

參、 前進滲透部署

「前進滲透部署」指在敵方或目標網路中主動建立隱秘立足點（Foothold），作為情報收集、破壞或操控的跳板。這種概念實際源自軍事上的「前緣防禦（Defend Forward）」，由於對手國在正統軍事上無法撼動美國，因此經常面臨以各種手段滲透、攻擊，而此種滲透攻擊未達傳統軍事程度，故無法以正式軍事行動回擊。過去幾年著名案例如藉網路輿論控制干預 2016 年大選、2017 年的WannaCry和NotPetya攻擊等；由於往往面臨回應時間過晚、回應手段不足的窘境，美國國防部開始思考以「前緣防禦」進行「前進滲透部署」。

一、邏輯與流程

「前進滲透部署」概念的主要目標在於，使對手的攻擊成本加劇、使對手的攻擊面臨高度危險，以及使對手的攻擊無效化。[5] 甚至在軍事層面上，藉由「前進滲透部署」可探知攻擊者的內部網路架構，釐清指揮鏈路，甚至藉此獲取、破壞高價值目標，依此取得情報優勢、實現在敵方網路中的「持久存在（Persistent Presence）」，及在必要時執行進一步「戰略行動」。整體而言，實際的操作流程通常包括：

（一）情報收集：結合使用公開來源情報（OSINT）與主動掃

[5] Steve Benton, “Defend Forward - A Proactive Model for Cyber Deterrence,” *The Cyber Defenders Council*, https://shorturl.at/BYbJk, p. 12.

描，如 Network Mapper、Shodan 等搜尋工具，藉此完成目標網路繪製並搜尋漏洞。

（二）**初始滲透**：透過釣魚郵件、零日漏洞或供應鏈攻擊進入目標系統。例如，2020 年的 SolarWinds 攻擊利用供應鏈漏洞滲透多個美國機構。

（三）**立足點建立**：植入後門程式（Backdoors）或遠端存取木馬（RATs），確保長期存取並規避檢測。

（四）**橫向移動**：提升權限並探索內部網路，鎖定高價值目標（如指揮控制系統）。

（五）**行動執行**：竊取資料、癱瘓系統或影響決策。

（六）**撤離與掩蓋**：透過加密通道外傳資料並清除日誌，隱藏入侵痕跡。

簡言之，「前進滲透部署」基本核心在於，相較於傳統防禦，不再僅僅等待攻擊發生後才做出反應，而是主動出擊，將防禦縱深延伸至前方或潛伏於敵方的網路空間。此外，最終目標不僅是阻止或減輕攻擊程度，更重要的是藉此增加對手的攻擊成本、提高攻擊風險以及降低攻擊成功可能性，從而「重塑對手行為」，使其不願或無法發動攻擊，因此是一種更具「威懾性」的策略。而前述之「持久存在」是「前進滲透部署」的關鍵要素；它強調在對手網路中建立長期、隱秘的立足點，以便持續監控、收集情報，並在必要時採取主動行動，這種「持久存在」並非被動地潛伏，而是為了更有效地執行情報收集、威懾和干預等任務。

二、案例及法規

當前的網路行為經常存在「攻守一體」的特性，防禦端為達成「前進滲透部署」目標，基本依賴技術包含「惡意軟體」、「AI 與自動化」、「誘捕技術」、「加密與匿名化」等。所謂「惡意軟

體」，是指包括了木馬程式、清除器（Wiper Malware）與蠕蟲等；「AI與自動化」，則是依據AI驅動滲透工具，藉此大量、快速自動「掃描漏洞」，乃至於依據使用者特性與邏輯，生成具說服力的釣魚郵件以提升攻擊效率。「誘捕技術」則是部署蜜罐或假資料，誘導攻擊者在錯誤時間、地點暴露意圖，同時收集敵手之手法與來源資訊。「加密與匿名化」則利用如洋蔥路由（The Onion Router）隱藏使用者真實位址、避免網路監控及流量分析，或 DNS 隧道或偽裝流量等，確保行動隱秘性。[6]

2010 年，美國與以色列聯合以「Stuxnet 震網」病毒，透過前進滲透部署植入惡意程式，藉零日漏洞長期潛伏於伊朗核設施工控網路內，隨以長期隱蔽、蠶食模式精準破壞離心機，展現了高隱秘性與難以追蹤、監控的高破壞力。2022 年，在俄烏戰爭中俄羅斯則利用前進滲透部署，在烏克蘭政府與基礎設施網路中潛伏，結合DDoS攻擊與清除器，試圖癱瘓通訊系統。[7]

此外，中國解放軍 61398 部隊在 2013 年被公開揭露，長期針對美國及其他國家的企業和政府機構進行網路間諜活動，竊取商業機密和敏感資訊；其行動中必然包含在目標網路中建立長期立足點，以便持續收集情報。雖整體而言，對其具體滲透和存取方法的揭露細節不多，但符合「前進滲透部署」中情報收集、初始滲透和立足點建立的階段之模式。[8]

另一方面與俄羅斯政府密切關聯的，Fancy Bear 與 Cozy Bear 的 APT 組織，被指控參與包括美國總統大選干預、針對各國政府機構和智庫的網路攻擊等行動；這些行動同樣需要長時間潛伏在目標網

[6] "Browse Privately. Explore Freely," *TorProject*, torproject.org/.
[7] Ben Buchanan 著，《駭客與國家-網路攻擊與地緣政治新常態》（台北：國防部譯印, 2022），頁 124-134。
[8] Dan Mcwhorter, "Mandiant Exposes APT1 – One of China's Cyber Espionage Units – and Releases 3,000 Indicators," *Mandiant*, February 19, 2013, https://shorturl.at/J8sNd.

路中，進行情報收集和伺機行動，亦符合「前進滲透部署」的特徵。[9] 2020 年的 SolarWinds 供應鏈攻擊案例，據信與俄羅斯情報部門有關的攻擊者成功滲透到 SolarWinds 的「軟體更新系統」中，並藉此在數萬個客戶的網路中植入後門。這使得攻擊者能夠在受害者的網路中建立廣泛且深入的「前進滲透部署」，以便進行後續的情報收集和潛在的破壞活動。[10]

主動式防禦與前進滲透部署，在既有國際法框架下具高度爭議性。《塔林手冊》作為網路戰的非約束性規範，在「主權原則」、「自衛權」、「反制措施」及「國際人道法」等面相有其規範與建議；西伐利亞體系強調國家主權，未經許可在「他國網路」中進行滲透，如植入後門等，即使未造成實質物理損害，仍被視為構成對國家主權之侵害。倘網路攻擊最終構成「武裝攻擊」，亦即造成物理性破壞，主權受侵害之國家則可能採行物理性反制。

網路戰的反制措施相關規範，基本允許對違法網路活動採取「非武力反制」，但涉及「跨境回擊（Hack-Back）」則可能違反當前國際法；而在「國際人道」的相關規範中，在武裝衝突中網路行動亦被規範不得針對平民或民用基礎設施，但顯然此點在前述俄烏戰爭中已被違反，且戰爭行為中要有效解除敵方反擊力量，國家基礎設施自然是重要攻擊目標之一。簡言，「前進滲透部署」的合法性具有爭議，如美國的「前進防禦」（Defend Forward）策略允許在敵方網路中主動監控與中和威脅，但俄羅斯與中國認為這違反主權。

肆、 挑戰與未來展望

[9] Ran Levi, “Malicious Life Podcast: Fancy Bear, Cozy Bear,” *Malicious Life Cybereason*, https://shorturl.at/Js3bg.

[10] Saheed Oladimeji, Sean Michael Kerner, “SolarWinds Hack Explained: Everything You Need to Know,” *TechTarget*, November 3, 2023, https://shorturl.at/kMrKp.

如本文前述，當前由於 AI、ML 及大語言模型 LLM 的誕生與快速發展，一方面為防禦者提供更好、更精準的工具，但同時也為攻擊者提供良好的武器。在攻守一體的網路戰環境當中，端視使用者如何運用工具追求其定義的「國家安全」與「國家利益」；業此自視防守之一方，恐相較更須遵循相關法規與道德規範，且滿足背後的政治目標與動機，才能區別與攻擊者的差異。

而就整體的發展而言，當前可能面臨技術、法律、創新、演化等面向之挑戰。在技術複雜性層面，由 AI、量子運算等驅動的防禦與滲透技術普遍需高昂成本，除大型跨國企業足以承擔與支付，其餘大多由國家作為支持者。且複雜技術開發往往耗時，而攻擊者的不對稱手法日新月異，是否會陷入傳統軍事對抗中的消耗概念，值得進一步評估與思索。量子計算與生成式 AI 的發展，使攻擊手法更難預測，不斷挑戰現有防禦能力。此外，在法律與道德風險方面，如前述前進滲透部署與攻擊性網路行動可能誤傷「無辜第三方」，例如藉由跳板、繞道進入敵方網路中，可能進一步引發道德與國際法乃至主權爭端。

美國 DARPA 主持的「AI 網路挑戰（AIxCC）」即藉由社會科技能力，強化、加速探索 AI 自動修補漏洞的潛力，並嘗試將其低成本化以期快速應用於當前的網路戰環境。同時，國際社會當前亦嘗試建立更清晰的網路戰規範，特別針對「前進滲透部署」的合法性與歸因、究責機制做出進一步釐清，當前各國正在研議的《塔林手冊 3.0》，預期將提供進一步明確的指引。

伍、結語

主動式防禦作為網路戰的核心策略，透過持續監控、動態防禦與自動化回應，顯著提升了對 APT 與新興威脅的應對能力。前進滲

透部署進一步將防禦延伸至敵方網路，實現情報優勢與戰略嚇阻，但其合法性與道德風險需謹慎評估。隨著 AI、量子技術與國際規範的演進，主動式防禦將在未來網路戰中扮演更關鍵角色，促進全球網路安全生態的進步。

本文作者詹祥威為淡江大學國際事務與戰略研究所博士，現為財團法人國防安全研究院網路安全與決策推演研究所助理研究員。主要研究領域為：地緣戰略、台日海洋安全、日本網路安全政策。

Active Defence – Forward Penetration Deployment

Siông-ui, Tsiam

Division of Cyber Security and Decision-Making Simulation

Abstract

This paper explores Active Cyber Defence (ACD) within the context of cyber warfare, emphasising its proactive, intelligence-driven approach to counter Advanced Persistent Threats (APTs). Unlike traditional passive defences, ACD focuses on predictive analytics, dynamic adaptation, and active countermeasures to neutralise threats before or during their inception. The study examines Forward Penetration Deployment (FPD). This strategy involves establishing covert footholds in adversary networks for intelligence gathering and disruption, as seen in cases such as Stuxnet and the Russia-Ukraine conflict. It examines FPD's technical mechanisms, legal controversies under frameworks like the Tallinn Manual, and ethical challenges. The paper also highlights emerging technologies, such as AI and quantum computing, which enhance both defensive and offensive capabilities, while addressing technical, legal, and moral challenges. ACD's evolution is poised to reshape global cybersecurity and strategic deterrence.

Keywords: Cybersecurity, Active Cyber Defense, Forward Defending