

編號：3183

議題研析

一、題目：強化數位防禦能力相關法制研析

二、議題所涉法規

國家安全法、軍事營區安全維護條例

三、背景說明（緣起）

據報導¹，外媒社論指出近期我國遭遇一波前所未有的網路攻擊，攻擊者運用具自主行動能力的 AI 代理工具，竊取文件、入侵電子郵件服務，並在政府網路應用程式中建立後門。顯示 AI 已可能從輔助駭客工具，進一步成為能自主尋找與利用漏洞的攻擊力量，引發資安界對 AI 改變網路攻防結構的高度警戒。相較於傳統駭客攻擊，AI 代理工具最大的威脅在於降低攻擊成本、提高速度與規模。AI 的攻擊能力是過往一支專業駭客團隊的效能，防禦方雖同樣利用 AI 尋找系統漏洞，但修補漏洞仍須投入時間及專業人力。報導同時指出我國面對的情況，將是西方民主國家未來必須面對的挑戰。

四、問題爭點

鑒於 AI 改變傳統駭客網路的攻防結構，不僅涉及相關產業資安防護問題，AI 針對包括軍事機關在內之公部門進行網路攻擊，更攸關國防及整體國家安全，我國目前依國家安全法、軍事營區安全維護條例及其相關授權辦法等規定，尚未能完整有效防範具自主行動能力的 AI 網路攻擊模式，如何落實並強化防禦各種新形態網路攻擊事件之相關規範，自有由法制面進一步加以檢視之必要，爰就此提出研析及建議意見。

五、探討研析

（一）參考英國、美國作法，整體規劃「國家資安戰略」，並適時融

¹郭芳君，瑞媒：AI 代理工具攻擊台灣為西方一記警鐘，中央社，115 年 8 月 17 日，國外政治。

入「主動式網路防禦」概念，以強化數位防禦能力

依國家安全法（下稱本法）第4條規定：「國家安全之維護，應及於中華民國領域內網際空間及其實體空間。」²究其立法理由³略以：「……因應資訊化時代來臨，國家安全之威脅不再限於實體，而擴大到網際空間，全球實務上已發生駭客入侵資訊及網路系統，竊取個資、智慧財產、商業機密以及軍事機密資料之情事，對人權、經濟與國安均造成威脅。爰本條國家安全之維護範圍中，所稱網際空間，包含網際空間之設施、資料、檔案及連結等，均屬應受維護之國家安全範疇，不得為非法方式干擾或破壞運作」。換言之，本法規範國家安全之範圍，已由領土、領海、領空等傳統主權領域，進一步擴及到中華民國領域內之網路空間及其實體空間，以強化資通訊安全之防護。

考量網際領域之主權觀念及資通訊安全威脅風險等，面對國際地緣政治情勢動盪及網路攻擊加劇，英國、美國等國家，已提出國家層級的資安防護政策，將資安防護由過去被動的資安防護，融入「主動式網路防禦」（Active Cyber Defense, ACD）概念，以超前部署防範資安攻擊之策略³，殊值參採。爰此，為進一步強化我國資通訊安全之防護戰略，建議相關政府部門可參考英國、美國作法，評估整體規劃「國家資安戰略」，並適時融入「主動式網路防禦」概念之可行性，以強化數位防禦能力，落實本法維護網際領域國家安全之立法目的。

（二）為優化軍事營區安全維護，提升軍事營區數位防禦規範密度，建議主管機關適時研修相關規定，以與時俱進

依軍事營區安全維護條例（下稱本條例）第3條第1項規定略以：「本條例用詞，定義如下：一、軍事營區：指重要軍事設施或軍事機關之駐地；經軍事機關通報相關機關管制之軍事演習或軍事訓練場域，於演習或訓練期間，視為軍事營區……三、軍事機關：指國防部及所屬機關（構）、部隊、學校；國家安全局及國家中山科學研究院視為軍事機關……九、核心資通系統：指直接用於重要軍事設施且防

²參照 111 年 6 月 8 日修正國家安全法第 4 條立法理由。

³孫鈺婷，〈國際資安防護政策趨勢探討－關於「主動式網路防禦」〉，《科技法律透析》，第 32 卷，第 1 期，109 年 1 月 15 日，頁 37。

護需求等級為高之作戰指揮管制、戰備訓練及管理資訊系統。」究其立法理由⁴略以：「定明軍事營區之範圍……定明軍事機關之定義。另考量國家安全局雖非軍事機關，惟勤務性質與軍事機關相仿，其掌理事項與軍事演習及訓練場域等安全管制與勤務執行事項息息相關；國家中山科學研究院負有國防武器裝備研發、生產等重要工作，亦涉及軍事機敏資訊，有據以保護駐地安全或衛哨人員安全之必要，爰將其視為軍事機關……定明重要軍事設施之核心資通系統，以明確系統範圍。另所稱『防護需求等級為高』，係指國防部參酌資通安全責任等級分級辦法，訂定國軍資通安全責任等級分級作業指導，其資通安全責任等級列為 A 級者。」爰此，現行本條對於核心資通系統定義，僅指直接用於重要「軍事設施」且防護需求等級為高之系統，尚未將直接用於重要「軍事機關」且防護需求等級為高之資通系統涵蓋在內。

鑒於上開報導中有關防範 AI 針對包括軍事機關在內之公部門進行網路攻擊之重要性。爰此，為落實軍事營區安全維護，提升軍事營區數位防禦規範密度，建議主管機關適時評估修正本條例第3條第1項第9款規定為：「九、核心資通系統：指直接用於重要軍事設施或軍事機關且防護需求等級為高之作戰指揮管制、戰備訓練及管理資訊系統。」，以與時俱進。

撰稿人：康世宗

⁴參照 113 年 1 月 3 日制定軍事營區安全維護條例第 3 條立法理由。