◎資訊安全宣導

—AI 時代的網路安全—

AI 對網路安全的影響大約從 2017 年被各國正視，美國的 FBI 甚至針對犯罪組織使用 AI 的問題召開過專門會議。由於網路是一個虛擬空間，讓侵害權利的犯罪行為得以隱身其中，並藉助科技帶來之轉換效果對真實世界的秩序造成破壞。英國倫敦大學學院的報告指出，犯罪者透過 AI 技術破解密碼、複製人類語音，以及其他諸多的非法侵權技術。其中深偽技術（deepfake）被列為犯罪結合 AI 後對網路安全的首要威脅之一，因為這有可能讓人們對任何影音或視頻資訊的傳遞失去信任感，嚴重妨礙人類社會資訊交換與傳播的現狀。

此外，上述報告也指出，運用 AI 的犯罪與傳統犯罪不同之處在於，它的犯罪效能可以在網路上被快速分享、重製與再現，甚至在犯罪組織的包裝下成為一種「服務」來銷售，以致國家司法機構難以有效抑制。

此外，COVID-19 疫情爆發後，各國遠距工作人數大增，導致網路端點之間的聯繫暴露在風險中。許多企業或是智庫的分析報告均指出，資訊科技（IT）與營運科技（OT）已成為網路犯罪者的主要侵權對象，特別是數位支付及加密貨幣的攻擊事件或竊取行為明顯增加。由於犯罪者可以透過 AI 的協助來生產惡意軟體或非法取得個資，再將之出售給其他犯罪者來營利，暗網交易變得越來越熱絡。相較於過去，網路侵權犯罪多半是由專業的駭客為之，但 AI 與暗網交易結合之後，資訊科技與營運科技會面臨更多元與廣泛的網路攻擊。顯然，AI 技術的普及化增加了我們正規生活中面臨威脅之風險。

【文章擷取-法務部調查局清流雙月刊】

臺中榮民總醫院提醒你!也關心你!