2025 年全球網路資訊熱戰升級

■文：編輯部

隨著數位化轉型的加速推進和新興技術的廣泛應用，2025 年，全球網路資訊安全威脅呈現出前所未有的複雜性和破壞性。2024 年 7 月至 2025 年 6 月期間，全球範圍內共發生嚴重資料安全事件 209 起，美洲、亞洲、歐洲成為資料安全事件的高發頻發地區。與此同時，全球網路攻擊次數相較於去年同期驟增 44%，勒索軟體攻擊從 2024 年的 32% 飆升至 44%，網路安全形勢日趨嚴峻。

最近 1 年網路安全事件

1. 資料洩露與隱私侵犯事件

2024 年 11 月至 2025 年 11 月期間，全球發生了多起影響深遠的資料洩露事件，這些事件不僅造成了巨大的經濟損失，更嚴重損害了企業信譽和用戶信任。

Finastra 資料洩露事件 (2024 年 11 月 20 日) 成為金融科技領域的標誌性事件。這家總部位於倫敦、服務全球頂級銀行的金融軟體公司確認其內部檔案傳輸平臺遭到入侵，攻擊者通過內部託管的安全檔案傳輸平臺 (SFTP) 竊取了超過 400GB 的敏感性資料。該事件的影響範圍極其廣泛，波及全球金融機構，暴露了金融科技企業在供應鏈安全方面的脆弱性。

進入 2025 年，資料洩露事件呈現出規模更大、影響更深的特徵。Community Health Center 資料洩露事件 (2025 年 1 月 30 日) 成為醫療行業的重大安全事故，超過 100 萬患者的敏感個人和健康資訊被暴露。該事件發生於 1 月 2 日，涉及犯罪分子未經授權訪問 CHC 系統，暴露了醫療機構在數位安全防護方面的嚴重不足。

TransUnion 資料洩露事件 (2025 年 8 月 28 日) 進一步凸顯了信用報告機構面臨的安全威脅。這家美國信用報告巨頭披露，始於 7 月的攻擊影響了 446.151 萬名個人，攻擊者通過協力廠商應用程式漏洞獲取了高度敏感的個人記錄。該事件的嚴重性在於，信用報告機構掌握著海量的個人身份資訊，一旦洩露將給受害者帶來長期的身份盜竊風險。

在零售和電商領域，Google 和 Workday 的 Salesforce 資料洩露事件 (2025 年 8 月) 展現了 SaaS 平臺的安全風險。ShinyHunters 駭客組織利用 Salesforce 平臺的 OAuth 權杖漏洞，成功入侵了 Google 和 Workday 的客戶資料庫，暴露了數百萬商業連絡人的資訊。這起事件的獨特之處在於，攻擊者利用了協力廠商集成的安全性漏洞，而非直接攻擊目標企業，體現了現代網路攻擊的間接性和隱蔽性特徵。

Stellantis 資料洩露事件

(2025 年 9 月 21 日) 則成為汽車行業的重大安全事故。這家全球知名汽車製造商披露，其 Salesforce CRM 系統遭到未授權訪問，影響了 1800 萬北美客戶記錄。攻擊者通過 vishing(語音釣魚) 活動竊取員工憑證，利用 Salesloft Drift AI 聊天集成的 OAuth 權杖漏洞，執行未授權的 API 調用批量匯出 CRM 資料。該事件不僅暴露了企業在員工安全意識培訓方面的不足，更凸顯了 AI 集成應用帶來的新型安全風險。

2. 勒索軟體攻擊事件

勒索軟體攻擊在 2025 年呈現出爆發式增長態勢，攻擊頻率和勒索金額均創下歷史新高。根據 Check Point 公司發佈的《2025 年網路安全報告》，勒索軟體攻擊從 2024 年的 32% 飆升至 44%(16)，成為最具破壞性的網路威脅之一。

Collins Aerospace 勒索軟體攻擊事件 (2025 年 9 月 19 日) 嚴重擾亂了歐洲航空業。HardBit 勒索軟體變種攻擊了 Collins Aerospace (RTX) 的 MUSE 乘客處理軟體，影響了多個歐洲資料中心，迫使希思羅、布魯塞爾、柏林和都柏林等主要機場恢復手動值機和行李處理常式。攻擊造成超過 50 萬份行程被加密，影響了數千名乘客和航空公司的運營連續性。攻擊者通過包含虛假 RTX 固件更新的魚叉式網路釣魚郵件獲得初始存取權限，利用未修補的 API 閘道漏洞 (CVSS 9.8) 進行許可權提升，最終部署勒索軟體加密乘客清單資料庫。

Kuala Lumpur 國際機場勒索軟體攻擊事件 (2025 年 3 月 23 日) 展示了關鍵基礎設施面臨的嚴重威脅。俄羅斯關聯的 Qilin(又稱 Agenda) 勒索軟體組織攻擊了馬來西亞最大的機場運營商，要求 1000 萬美元贖金，並聲稱竊取了多達 2TB 的數據。攻擊導致航班資訊螢幕、值機櫃檯和行李處理系統離線，工作人員被迫使用手動替代方案。雖然航班繼續運行，但乘客和工作人員經歷了嚴重的延誤和不便，中斷持續了數天直到系統從備份中恢復。

Kettering Health 醫院勒索軟體攻擊事件 (2025 年) 成為醫療行業的典型案例。Interlock 勒索軟體組織攻擊了美國俄亥俄州的大型醫療網路，該網路包括 14 家醫院和多個診所，每年為數萬名患者提供服務。勒索軟體滲透了醫院網路，禁用了 14 家醫院的 IT 系統，包括電子健康記錄系統、內部電話線和臨床資料通道。許多計畫中的手術被迫取消，急診患者被轉移到其他醫院，因為數位系統無法訪問。Kettering 還確認敏感性資料 (包括財務資訊和可能的患者記錄) 已被竊取。

在政府和公共服務領域，Slovakia 土地和地籍系統勒索軟體攻擊事件 (2025 年) 成為國家級基礎設施遭受攻擊的典型案例。該國土地測量、製圖和地籍管理局 (ÚGKK) 遭受了可能來自 Kapor 駭客組織的攻擊，攻擊者要求 1200 萬美元贖金，這是今年披露的最大贖金請求之一。攻擊使整個地籍系統癱瘓，電子服務無法使用，物理辦公室被迫關閉。全國各地的房地產交易和登記服務陷入停頓，房地產銷售、貸款流程甚至布拉提斯拉瓦的停車許可證發放等相關服務都被暫停。專家警告，從備份中恢復登記冊的完整功能可能需要數月時間。

3. 供應鏈攻擊事件

供應鏈攻擊在 2025 年呈現出前所未有的複雜性和破壞性，攻擊者通過滲透協力廠商供應商和合作夥伴，實現了對多個目標的批量攻擊。

Blue Yonder 供應鏈勒索軟體攻擊事件 (2024 年 11 月) 成為供應鏈安全的典型警示。這家為全球主要零售商、消費品公司和製造商提供供應鏈管理軟體的供應商遭到勒索軟體攻

擊，影響了為 46 家全球前 100 製造商、64 家前 100 消費品公司和 76 家前 100 零售商提供的託管服務。該事件凸顯了在繁忙的假日季節組織面臨的供應鏈風險升級，單一供應商的安全性漏洞可能導致整個產業鏈的癱瘓。

Clop 勒索軟體對 Oracle E-Business Suite 的攻擊 (2025 年) 展現了針對企業軟體的大規模供應鏈攻擊模式。Clop 勒索軟體組織利用 Oracle E-Business Suite 的零日漏洞 CVE-2025-61882 (CVSS 評分 9.8)，對多個企業發起攻擊。美國航空旗下支線航空公司 Envoy Air 證實其 Oracle E-Business Suite 應用遭到入侵，可能導致部分商業資訊及聯繫方式洩露。Allianz UK 也確認遭受了與 Clop 勒索軟體組織相關的網路事件，該漏洞影響了管理家庭、汽車、寵物和旅行保險政策的系統。

Volvo Group 資料洩露事件 (2025 年 9 月 25 日) 進一步暴露了企業在供應鏈安全管理方面的不足。DataCarry 勒索軟體組織攻擊了 Volvo 的瑞典人力資源軟體提供商 Milj?data，導致 Volvo Group 確認了重大資料洩露。該事件始於 8 月 20 日左右，展示了攻擊者如何通過供應鏈中的薄弱環節，間接攻擊目標企業。

4. 國家級網路攻擊事件

2025 年的國家級網路攻擊呈現出更加複雜和隱蔽的特徵，各國政府和關鍵基礎設施成為主要目標。

哈爾濱亞冬會網路攻擊事件 (2025 年 1 月 26 日至 2 月 14 日) 成為國際體育賽事遭受網路攻擊的典型案例。根據中國國家電腦病毒應急處理中心發佈的監測分析報告，第 9 屆亞洲冬季運動會期間，賽事資訊系統遭到來自境外的網路攻擊達 270,167 次。這些攻擊不僅針對賽事資訊系統，還波及黑龍江省域內的關鍵資訊基礎設施。

巴基斯坦與印度的網路戰 (2025 年 5 月 7 日) 展示了地緣政治衝突向網路空間的延伸。在印度軍隊發動 " 辛杜爾行動 " 對巴基斯坦境內恐怖營地進行精確打擊後，巴基斯坦關聯的駭客組織立即展開了大規模網路攻擊報復。巴基斯坦關聯的駭客組織對印度目標進行了一系列網路攻擊，雖然沒有造成重大破壞，但攻擊規模巨大。印度機構識別出七個 APT 組織對印度進行了超過 150 萬次網路攻擊，這些攻擊據報告主要來自巴基斯坦、孟加拉和西亞地區，攻擊向量包括網頁篡改、DDoS 攻擊、惡意軟體分發和資訊戰活動。

5. 重大經濟損失統計分析

2025 年網路安全事件造成的經濟損失呈現出規模巨大、影響深遠的特徵。根據多家權威機構的統計資料，全球網路犯罪造成的損失正以驚人的速度增長。

總體經濟損失規模方面，Cybersecurity Ventures 預測，網路犯罪成本可能在 2025 年達到每年 10.5 萬億美元。這一數位反映了網路犯罪對全球經濟造成的巨大衝擊。2023 年，網路犯罪給全球企業造成了約 8 萬億美元的損失，預計到 2027 年將上升到近 24 萬億美元。

資料洩露成本呈現出顯著的地區差異。2025 年全球資料洩露平均成本為 444 萬美元，較 2024 年的 488 萬美元下降了 9%。然而，美國的資料洩露成本卻逆勢上升，達到 1022 萬美元，成為全球資料洩露成本最高的地區。在洩露類型方面，惡意內部攻擊的平均成本為 492 萬美元，供應鏈洩露為 491 萬美元，釣魚攻擊為 480 萬美元，本地洩露為 401 萬美元。涉及多個環境的洩露成本更高，達到 505 萬美元。

勒索軟體攻擊成本創下歷史新高。2025 年勒索軟體支

付達到創紀錄的每次事件 176 萬美元，許多組織仍選擇支付贖金。根據區塊鏈分析公司 Chainalysis 的研究，2024 年約有 8.1355 億美元用於支付勒索軟體贖金。然而，調查顯示，80% 支付贖金的受害者很快再次遭到攻擊，46% 雖然獲得了資料存取權限，但大部分數據已被損壞。

產業特定損失呈現出明顯的差異化特徵。醫療行業繼續成為網路攻擊的重災區，2025 年醫療行業的總洩露成本達到 113 億美元，是所有行業中最高的。教育機構的恢復成本平均為 158 萬美元 (基礎教育) 和 142 萬美元 (高等教育)，但恢復過程有時需要數月時間。雖然近一半被攻擊的機構支付了贖金來恢復資料，但只有 2% 完全找回了所有資料。

重大事件損失案例進一步印證了網路攻擊的破壞性。英國零售業在 2025 年遭受的網路攻擊造成的損失最高可能達到 5.9 億美元。Marks & Spencer 在遭受網路攻擊後市值損失超過 7 億英鎊 (9.3 億美元)，並經歷了數周的線上訂購暫停和倉庫關閉。韓國運營商 SK 電訊的資料洩露導致季度利潤暴跌超過 90%。Jaguar Land Rover 在 8 月份遭受的重大網路事件導致其英國主要工廠停產，CMC 模型估計總經濟損失為 19 億英鎊，影響了超過 5000 家英國組織。

全球資訊安全面臨的核心挑戰

1. 威脅態勢的根本性轉變

2025 年，全球網路安全威脅態勢發生了根本性轉變，傳統的攻擊模式正在被更加複雜、智慧和隱蔽的新型威脅所取代。

勒索軟體攻擊的爆發式增長成為 2025 年最顯著的威脅特徵。根據 Check Point 公司發佈的《2025 年網路安全報告》，全球網路攻擊次數相較於去年同期驟增 44%。勒索軟體攻擊從 2024 年的 32% 飆升至 44%，但防禦者開始掌握主動權。這一變化反映了攻擊者與防禦者之間的技術競賽正在加速，雙方都在不斷提升自己的能力。

AI 驅動的網路犯罪正在重塑威脅格局。72% 的受訪者報告組織網路風險增加，勒索軟體仍是首要關注點，近 47% 的組織將生成式 AI 驅動的對手進展視為主要擔憂。生成式 AI 正在增強網路犯罪能力，導致社會工程攻擊增加。攻擊者利用 AI 技術顯著提升了攻擊效率，某 APT 組織利用生成式 AI 將 0day 漏洞利用代碼生成效率提升 5 倍，2025 年第一季度全球新發現 APT 攻擊中 AI 參與率達 63%。

供應鏈攻擊的複雜化成為企業面臨的新挑戰。Verizon 發佈的第 18 版《2025 資料洩露調查報告》追蹤了 22,052 起安全事件，其中 12,195 起涉及資料洩露，分佈在 139 個國家。報告顯示，利用漏洞作為初始訪問媒介的情況顯著增長，在分析的 12,195 起已確認的資料洩露事件中占比達到 20%。協力廠商參與資料洩露的比例從 15% 翻了一番，達到 30%，協力廠商環境中憑證重用的情況日益普遍。

了安全防護的難度。零日漏洞 (Zero-Day Exploits) 的數量在近年來呈現出爆炸式增長，成為網路安全的首要威脅。2025 年 1 月的 " 補丁星期二 " 更新中，微軟修復了 159 個漏洞，包括 8 個零日漏洞和多個關鍵的遠端代碼執行漏洞。這種漏洞發現和修復之間的時間差，為攻擊者提供了可乘之機。

2. 技術層面的挑戰

AI 技術帶來的雙重挑戰成為 2025 年網路安全領域最複雜的問題。一方面，AI 技術被廣泛應用於攻擊活動中，WormGPT 等 AI 驅動工具被網路犯罪分子用於降低技能門檻和自動化攻擊流程，包括釣魚和社會工程。另一方面，雖然 66% 的受訪者認為 AI 將在未來 12 個月內影響網路安全，但只有 37% 的組織具備安全部署 AI 的流程。

量子計算的威脅正在從理論走向現實。量子電腦理論上可在幾分鐘內破解 RSA-2048 加密，對銀行、軍工、區塊鏈等領域構成滅頂之災。這種威脅不僅影響現有的加密體系，更對整個數字經濟的安全基礎提出了挑戰。

物聯網安全的嚴峻形勢不容忽視。2025 年全球 IoT 設備超過 750 億台，70% 存在預設密碼、未修復漏洞等風險。智慧攝像頭被劫持成為 DDoS 攻擊 " 肉雞 "，工業感測器資料遭篡改引發生產線癱瘓，這些案例表明物聯網設備正成為網路攻擊的新前線。

雲安全的複雜性持續增加。雖然雲技術帶來了靈活性和成本優勢，但也引入了新的安全挑戰。雲原生應用的複雜性、多租戶環境的隔離問題、雲服務配置錯誤等都成為新的攻擊向量。2025 年的多起雲資料洩露事件表明，即使是大型科技公司也難以完全避免雲安全事故。

3. 管理和運營層面的挑戰

網路安全技能短缺已成為全球性難題。自 2024 年以來，網路安全技能缺口增加了 8%，三分之二的組織報告存在中等至嚴重的技能缺口，包括缺乏滿足安全要求的必要人才和技能。更令人擔憂的是，只有 14% 的組織對他們今天擁有的人員和技能有信心。公共部門受到的影響尤其嚴重，49% 的公共部門組織表示他們缺乏實現網路安全目標所需的人才，比 2024 年增加了 33%。

合規負擔的加重給企業帶來了巨大壓力。78% 的私營組織領導者認為網路和隱私法規能有效降低其組織生態系統中的風險，但三分之二的受訪者認為監管要求的複雜性和擴散是一個挑戰。法規的激增和不和諧正在給組織帶來重大挑戰，超過 76% 的首席資訊官認為如此。

成本效益的平衡難題日益突出。儘管超過 60% 的 CEO 和 CISO 報告網路風險管理已集成到其組織的企業風險管理中，但許多人仍難以準確評估所需的投資水準。事實上，今天只有不到一半的 CEO 相信他們的組織在網路安全方面投入了足夠的資金。這種投資不足與風險認知之間的矛盾，加劇了企業面臨的安全風險。

供應鏈安全管理的複雜性持續增加。54% 的大型組織將供應鏈挑戰視為實現網路韌性的最大障礙。供應鏈日益複雜，加

上對供應商安全水準缺乏可見性和監督，已成為組織的主要網路安全風險。關鍵擔憂包括協力廠商引入的軟體漏洞和整個生態系統中網路攻擊的傳播。

4. 地緣政治因素的影響

地緣政治緊張局勢對網路安全性原則產生了深遠影響。近 60% 的組織表示地緣政治緊張局勢影響了其網路安全性原則。地緣政治動盪也影響了風險認知，三分之一的 CEO 將網路間諜活動和敏感資訊 / 智慧財產權盜竊列為首要擔憂，而 45% 的網路安全領導者擔心運營和業務流程的中斷。

國家支持的 APT 攻擊呈現出更加隱蔽和專業的特徵。2025 年的多起事件表明，國家支援的駭客組織正在使用更加先進的技術和策略。這些組織不僅具備強大的技術能力，還擁有充足的資源和耐心，能夠進行長期的隱蔽攻擊。

跨境資料流程動的安全挑戰日益突出。隨著全球化的深入發展，資料的跨境流動變得越來越頻繁。然而，不同國家和地區在資料保護法規、安全標準等方面存在顯著差異，這給跨國企業的安全管理帶來了巨大挑戰。

各國政府網路安全政策與應對措施

1. 歐盟的綜合性網路安全政策體系

歐盟在 2025 年建立了全球最為完善和嚴格的網路安全政策體系，通過立法、技術標準和國際合作等多重手段，構建了全方位的網路安全防護框架。

歐盟網路團結法案 (EU Cyber Solidarity Act) 於 2025 年 2 月 4 日正式生效，標誌著歐盟在網路安全領域的重大突破。該法案旨在加強歐盟檢測、準備和應對重大和大規模網路安全威脅及攻擊的能力。法案包括歐洲網路安全警報系統，該系統由歐盟各地的國家和跨境網路中心組成，使用人工智慧和資料分析等先進技術檢測和跨境共用威脅警告。

歐盟人工智慧法案 (EU AI Act) 作為全球首個全面監管 AI 的框架，於 2025 年全面實施。該法案根據風險對 AI 系統進行分類，並對不同風險等級的 AI 系統施加特定義務。高風險 AI 系統必須滿足嚴格的合規要求，包括風險管理、人工監督、透明度、資料治理等多個方面。

歐盟網路韌性法案 (EU Cyber Resilience Act) 於 2025 年正式生效，要求數位產品和連接設備製造商遵守網路安全標準。該法案提出了 " 設計即安全 " 的理念，要求製造商在產品設計階段就考慮網路安全因素，提供軟體物料清單 (SBOM)，並提供生命週期支援。

NIS2 指令的全面實施標誌著歐盟在關鍵基礎設施保護方面的重大進展。2025 年 6 月 26 日，歐盟網路安全局 (ENISA) 發佈了指導檔，規定了受監管組織為遵守歐盟關鍵基礎設施網路安全法 (NIS2) 應具備的安全措施。NIS2 指令將關鍵基礎設施的範圍從原來的 11 個擴展到 16 個領域，要求相關組織實施更嚴格的安全措施，並在發生重大安全事件時及時報告。

2. 美國的多層次網路安全戰略

美國在 2025 年繼續強化其全球網路安全領導地位，通過行政命令、立法、監管等多重手段，構建了覆蓋聯邦政府、企業和個人的多層次網路安全防護體系。

2025 年 6 月發佈的最新網路安全行政命令標誌著美國網路安全戰略的重大調整。該命令旨在簡化過去幾屆政府的網路安全行政行動，剝離被視為過於規定性或意識形態化的授權。新命令更加注重實際效果和成本效益，強調公私合作和技術創新。

網路安全成熟度模型認證 (CMMC) 2.0 的全面實施成為美國國防供應鏈安全的重要里程碑。2025 年 9 月 10 日，美國國防部在聯邦公報上發佈了最終的 CMMC 規則，該規則於 11 月 10 日生效，正式啓動了為期三年的國防部合同網路安全要求推出計畫。CMMC 2.0 對與美國國防部合作的公司強制執行，為處理政府資料的承包商引入了更嚴格的驗證流程。

《2025 年保險網路安全法》(Insure Cybersecurity Act of 2025) 於 2025 年 1 月 24 日在參議院提出，體現了美國在網路保險監管方面的新動向。該法案要求國家電信和資訊管理局 (NTIA) 建立網路保險政策工作組，定義為提供網路攻擊和相關事件造成的損失、損害和費用保險的政策。這一立法反映了美國政府對網路風險保險市場規範化的重視。

聯邦機構的安全強化措施持續推進。2025 年，美國各聯邦機構都在加強自身的網路安全防護能力。例如，美國網路安全和基礎設施安全局 (CISA) 發佈了多項安全公告和指導，提醒各機構注意新型威脅和漏洞。財政部等關鍵部門在遭受協力廠商攻擊後，加強了對供應商的安全審查。

國際合作機制的深化成為美國網路安全戰略的重要組成部分。美國繼續通過多邊機制，如五眼聯盟、G7、G20 等，加強與盟友在網路安全領域的合作。特別是在應對跨國網路犯罪、打擊勒索軟體等方面，美國與其他國家的執法合作日益密切。

3. 其他主要經濟體的網路安全舉措

中國：中國通過《網路安全法》、《資料安全法》和《個人資訊保護法》構建了全面的網路安全法律體系。中國強調網路主權原則，加強對關鍵資訊基礎設施的保護，並推動本土網路安全產業發展。

英國的網路安全和韌性法案在 2025 年進入關鍵實施階段。該法案建立了新的網路安全監管框架，加強了對關鍵國家基礎設施的保護，並引入了針對網路安全事件的新的報告要求。法案還賦予了英國國家網路安全中心 (NCSC) 更大的權力，包括在發生重大網路安全事件時強制要求企業採取特定措施的權力。

日本的網路安全戰略更新體現了該國對網路安全威脅的高度重視。日本政府在 2025 年發佈了新的網路安全戰略，重點關注關鍵基礎設施保護、供應鏈安全、5G 和 6G 網路安全等領域。日本還加強了與美國、澳大利亞等盟友在網路安全領域的合作，特別是在應對來自朝鮮等國家的網路威脅方面。

澳大利亞的網路安全合作機制進一步深化。澳大利亞在 2025 年加強了與美國、英國、加拿大、紐西蘭等五眼聯盟成員在網路安全領域的合作。特別是在應對中國相關的網路威脅方面，澳大利亞與盟友分享情報，協調應對措施。

4. 國際合作與標準制定

多邊合作機制的加強成為 2025 年網路安全領域的重要趨勢。各國政府認識到，面對跨國網路威脅，任何單一國家都難以獨立應對，因此加強國際合作成為必然選擇。聯合國、G20、OECD 等國際組織在推動全球網路安全標準制定、最佳實踐分享等方面發揮了重要作用。

技術標準的國際化進程加快。2025 年，多個重要的網路安全技術標準得到了國際社會的廣泛認可和採用。例如，ISO 27001 資訊安全管理體系標準、NIST 網路安全框架等在全球範圍內得到了更廣泛的應用。這些標準的推廣有助於提高全球網路安全防護水準的一致性。

跨境執法合作的深化取得了顯著成果。2025 年，多國執

法機構聯合行動，成功打擊了多個跨國網路犯罪組織。例如，在打擊 Darknet 市場、勒索軟體團夥等方面，國際執法合作發揮了關鍵作用。

AI 技術在網路安全攻防兩端的應用與發展趨勢

1. AI 在網路攻擊中的應用與演進

2025 年，人工智慧技術在網路攻擊中的應用呈現出前所未有的複雜性和破壞性，攻擊者通過 AI 技術顯著提升了攻擊的效率、精准度和隱蔽性。

AI 驅動的自動化攻擊工具正在重塑網路犯罪格局。WormGPT 及其後續變體等 AI 驅動工具被網路犯罪分子廣泛用於降低技能門檻和自動化攻擊流程，特別是在釣魚和社會工程領域。這些工具能夠自動生成高度個性化的釣魚郵件，模仿目標群組織的通信風格和格式，使得傳統的基於規則的檢測方法失效。攻擊者利用 AI 技術實現了攻擊流程的全自動化，從目標偵察、漏洞掃描到惡意軟體分發，整個過程可以在數小時內完成。

深度偽造技術的威脅升級成為 2025 年最令人擔憂的安全趨勢之一。Deepfake 視頻和生成式 AI 帶來了新的風險，使身份冒充和欺詐更難檢測。攻擊者利用 AI 技術創建高度逼真的虛假視頻和音訊，能夠完美模仿企業高管的聲音和形象，進行商業郵件詐騙 (BEC) 等高級欺詐活動。這種技術的濫用不僅造成了直接的經濟損失，更嚴重損害了企業的信譽和客戶信任。

AI 增強的漏洞利用能力達到了新的高度。某 APT 組織利用生成式 AI 將 0day 漏洞利用代碼生成效率提升 5 倍，2025 年第一季度全球新發現 APT 攻擊中 AI 參與率達 63%。AI 技術使攻擊者能夠更快地發現和利用系統漏洞，自動生成針對特定目標的攻擊代碼。攻擊鏈完全由 AI 自主決策，具備 " 認知對抗 " 能力，能夠識別並欺騙安全分析師的思維模式。

社會工程攻擊的智慧化升級展現了 AI 技術的巨大破壞力。AI 生成的釣魚郵件檢測難度提升 400%，社會工程攻擊成功率升至 32%。攻擊者利用機器學習演算法分析大量的公開信息，包括社交媒體資料、新聞報導、企業公告等，構建高度精准的目標畫像。基於這些畫像，AI 系統能夠生成極具說服力的社會工程攻擊，大大提高了攻擊的成功率。

多模態攻擊的興起體現了 AI 技術的綜合應用能力。攻擊者不再局限於單一的攻擊手段，而是利用 AI 技術整合多種攻擊向量，包括網路釣魚、惡意軟體、勒索軟體等。AI 系統能夠根據目標的特點和環境，自動選擇最有效的攻擊組合，實現攻擊效果的最大化。

2. AI 在網路防禦中的創新應用

面對日益複雜的 AI 驅動威脅，網路安全防禦領域也在積極擁抱 AI 技術，通過智慧化的防禦手段提升整體安全防護能力。

AI 驅動的威脅檢測系統正在成為企業安全防護的核心。企業部署的 AI 驅動威脅檢測系統通過即時行為分析處理 PB 級日誌資料，將勒索軟體檢測回應時間從數天縮短至數分鐘。這些系統能夠識別傳統安全工具無法檢測的複雜攻擊模式，通過機器學習演算法不斷優化檢測模型，提高對新型威脅的識別能力。

AI 原生的安全防護方案展現了技術創新的巨大潛力。深信服安全 GPT 基於自主研發的安全大模型，針對 0day 漏洞、複雜邏輯漏洞、Webshell 加密攻擊、流量側隱蔽威脅等高級攻擊，實測檢出率超過 99%，遠超傳統安全手段。結合 XDR 體系，安全 GPT 能夠深度挖掘並識別混淆變種、橫向滲透和惡意外聯等高級威脅，實現從

端點到流量的全鏈路智慧檢測。

AI 增強的安全分析能力正在改變傳統的安全運營模式。AI 智慧體工具開始深度融入安全運營，實現 7×24 小時告警覆蓋與秒級研判，同時輔助安全人員完成高級威脅分析。這些工具能夠自動關聯不同來源的安全資料，識別隱藏的攻擊模式，提供全面的威脅情報分析。

預測性安全防護成為 AI 技術應用的新方向。通過分析歷史資料和當前威脅情報，AI 系統能夠預測潛在的安全風險，提前採取防護措施。這種預測能力使企業能夠從被動防禦轉向主動防護，大大提高了整體安全防護的效率和效果。

3. AI 安全的技術發展趨勢

"以 AI 對抗 AI" 的防禦理念正在成為行業共識。2025 年，AI 武器化進一步加劇攻防不平衡的狀況，企業面臨空前嚴峻的網路安全挑戰，以 AI 對抗 AI 成為必選題。這種理念要求安全團隊不僅要使用 AI 技術進行防禦，還要深入理解攻擊者使用的 AI 技術，通過技術對抗技術，實現更有效的安全防護。

AI 安全的標準化和規範化進程加快。面對 AI 技術帶來的新型安全挑戰，行業正在推動 AI 安全標準的制定和完善。這些標準涵蓋了 AI 系統的設計、開發、部署、運營等各個環節，旨在確保 AI 技術在提升安全防護能力的同時，不會引入新的安全風險。

4. AI 安全面臨的挑戰與應對策略

AI 模型自身的安全風險成為必須正視的問題。AI 系統本身也可能成為攻擊目標，攻擊者可能通過投毒攻擊、對抗樣本等手段操縱 AI 模型的行為。因此，確保 AI 系統的安全性和可信度成為一個關鍵挑戰。企業需要採用安全的 AI 開發實踐，包括模型驗證、魯棒性測試 (Robustness Testing)、對抗訓練等技術手段。

人才短缺的加劇制約了 AI 安全的發展。雖然 AI 技術為網路安全帶來了新的機遇，但也對安全從業人員提出了更高的要求。掌握 AI 技術的安全專家嚴重短缺，這成為 AI 安全發展的主要瓶頸之一。企業需要加大對 AI 安全人才的培養和引進力度。

成本效益的平衡成為企業面臨的現實問題。AI 安全技術的部署需要大量的投資，包括硬體設備、軟體工具、人員培訓等。企業需要在安全需求和成本控制之間找到平衡點，確保 AI 安全投資能夠帶來實際的安全收益。

監管合規的複雜性增加了 AI 安全的實施難度。隨著各國對 AI 技術監管的加強，企業在部署 AI 安全解決方案時需要考慮合規要求。不同國家和地區的監管標準存在差異，這給跨國企業的 AI 安全部署帶來了挑戰。

晶片技術在資訊安全方面的改進與進步

1. 硬體級安全功能的全面升級

2025 年，晶片製造商在硬體級安全功能方面取得了重大突破，通過集成更加強大的安全處理器、加密引擎和防護機制，為現代計算系統提供了前所未有的安全保障。

AMD 安全處理器 (AMD Secure Processor) 提供了全方位的安全保障。這是一個集成的片上安全處理器，設計用於幫助保護敏感性資料並在代碼執行前驗證代碼，有助於保護系統和資料免受設備上運行的未授權軟體和應用程式的侵害。結合 AMD 安全處理器 (ASP)，Microsoft Pluton 安全處理器幫助保護使用者的機密和個人資料，無論他們是在移動中還是連接到企業網路，即使筆記型電腦丟失或被盜也能得到保護。

平臺安全啟動 (AMD Platform Secure Boot) 功能提

供了針對固件級遠端攻擊的防護。這項功能旨在提供安全防護，以應對日益猖獗的固件級別遠端攻擊，AMD 安全啓動功能有助於將信任鏈從系統 BIOS 延伸到作業系統開機載入程式。

2. 後量子密碼學晶片的商業化突破

面對量子計算帶來的潛在威脅，後量子密碼學晶片的研發和商業化成為 2025 年晶片安全領域的重要突破。

三星 S3SSE2A 晶片的革命性意義標誌著後量子密碼學進入實用階段。2025 年 2 月 25 日，三星半導體業務部門宣佈已完成 S3SSE2A 晶片的開發，這款晶片號稱是 " 業界首款配備硬體後量子密碼學 (PQC) 的安全晶片 "，旨在保護移動設備上的關鍵資料免受量子計算帶來的嚴重威脅。S3SSE2A 不僅僅是一顆晶片，它還是一個包含硬體和軟體的安全元素 (SE) 一站式解決方案，通過硬體加速和軟體優化，能夠在保證安全性的同時，節約設備資源，提高運行效率。

後量子密碼學的產業化進程正在加速推進。根據行業分析，後量子密碼 (PQC) 晶片研發已進入產業化臨界點，頭部企業如英飛凌、紫光同芯已實現 256 位元抗量子攻擊晶片量產，預計 2030 年相關產品將佔據高端市場份額的 30%。這一進展為應對量子計算威脅提供了切實可行的技術方案。

硬體級抗量子密碼演算法的集成成為新的技術標準。新一代安全晶片普遍集成了多種抗量子密碼演算法，包括格密碼、雜湊密碼、代碼密碼等，確保在量子計算時代仍能提供足夠的安全保障。這些演算法經過嚴格的數學驗證，能夠抵禦量子電腦的攻擊。

3. 物聯網安全晶片的專業化發展

物聯網設備的爆發式增長對安全晶片提出了更高的要求，2025 年物聯網安全晶片在專業化、集成化方面取得了重要進展。

低功耗安全設計的優化滿足了物聯網設備的特殊需求。物聯網設備通常具有嚴格的功耗限制，因此安全晶片必須在提供強大安全功能的同時，保持極低的功耗。新一代物聯網安全晶片通過優化電路設計、採用先進制程工藝等手段，實現了安全功能與功耗的最佳平衡。

4. 供應鏈安全與硬體信任根

隨著供應鏈攻擊的日益複雜，晶片供應鏈的安全性成為 2025 年關注的焦點，各大晶片廠商都在加強供應鏈安全和硬體信任根的建設。

2023 年底，非營利性組織 Open Compute Project Foundation (OCP) 宣佈了一個新專案 “OCP 安全評估框架和啓用 (S.A.F.E.)”，旨在提高所有資料中心 IT 基礎設施中設備的可信度。預計將通過 OCP 社區為每台設備開發安全檢查清單，減少設備安全審計的間接成本及冗餘，並提高整個供應鏈中設備硬體和固件元件的安全姿態。OCP S.A.F.E. 框架的嚴格驗證確保了產品的安全性。

設備來源追蹤技術的創新提供了前所未有的供應鏈透明度。新技術說明驗證整個製造過程中設計檔的真實性和完整性，提供了對晶片來源的前所未有的可見性，使客戶能夠驗證其資料中心元件從設計到部署的生命週期。

硬體信任根的強化成為抵禦供應鏈攻擊的關鍵。現代晶片普遍採用了基於硬體的信任根設計，通過物理不可克隆函數 (PUF)、熔絲程式設計等技術，確保每個晶片都具有唯一的身份標識和金鑰材料。這些信任根在晶片製造過程中被安全地植入，無法被複製或篡改，為整個系統的安全性提供了堅實基礎。

5. 晶片安全技術的未來發展趨勢

異構集成 (Chiplet) 技術的安全優勢日益顯現。異構集成技術通過將不同功能的晶片模組組合在一起，不僅提高了性能和功耗效率，還為安全設計提供了新的可能性。通過在不同的晶片模組中集成專門的安全功能，可以實現更加靈活和高效的安全架構。

AI 加速晶片的安全集成成為新的發展方向。隨著 AI 應用的普及，專門的 AI 加速晶片 (如 GPU、NPU 等) 在系統中的地位越來越重要。這些晶片不僅需要提供強大的計算能力，還需要具備相應的安全功能，包括資料隱私保護、模型安全、推理安全等。

邊緣計算晶片的安全增強滿足了分散式運算的需求。邊緣計算環境通常具有資源受限、網路不穩定等特點，對晶片的安全功能提出了特殊要求。新一代邊緣計算晶片通過集成羽量級密碼演算法、硬體亂數產生器、安全存儲等功能，為邊緣計算應用提供了必要的安全保障。

車規級安全晶片的嚴格要求推動了技術創新。隨著自動駕駛技術的發展，汽車晶片的安全性要求達到了前所未有的高度。車規級安全晶片不僅需要滿足功能安全標準 (如 ISO 26262)，還需要具備網路安全能力，能夠抵禦來自車內和車外的各種安全威脅。

結語

2025 年，全球網路安全格局正處於深刻變革的關鍵時期。網路攻擊的規模、複雜性和破壞性都達到了歷史新高，造成的經濟損失已經突破萬億美元級別。勒索軟體攻擊從 32% 飆升至 44%，AI 驅動的攻擊使威脅檢測難度提升 400%，供應鏈攻擊的比例從 15% 翻倍至 30%，這些資料充分說明了網路安全形勢的嚴峻性。

面對日益複雜的威脅環境，全球各國政府、企業和安全性群組織正在採取積極的應對措施。歐盟通過網路團結法案、AI 法案、網路韌性法案等立法，構建了全球最完善的網路安全法律框架；美國通過 CMMC 2.0、保險網路安全法等舉措，強化了關鍵基礎設施和供應鏈的安全防護；其他主要經濟體也都在加強網路安全立法和執法合作。這些政策措施的實施，為全球網路安全治理提供了重要支撐。

技術創新正在成為應對網路安全挑戰的關鍵驅動力。在攻擊端，AI 技術被廣泛應用於自動化攻擊、深度偽造、智慧漏洞利用等領域，使攻擊的效率和隱蔽性達到了新的高度。在防禦端，AI 驅動的威脅檢測系統將勒索軟體檢測回應時間從數天縮短至數分鐘，自主安全運營中心實現了 7×24 小時的智慧防護，" 以 AI 對抗 AI" 的理念正在成為現實。

晶片技術的安全改進為整個資訊安全體系提供了堅實的硬體基礎。從邊緣物聯網芯片到中央處理器，所有環節的芯片供應商都在加固其安全措施，防止自己的產品成為系統的安全短板，硬體級安全防護已經進入了新的發展階段。

展望未來，網路安全領域將面臨更加嚴峻的挑戰和更加廣闊的機遇。量子計算的威脅日益臨近，後量子密碼學的產業化進程需要加快；AI 技術的雙刃劍效應需要更加審慎地對待，" 智慧治理智慧 " 的新範式需要不斷探索和完善；供應鏈安全的複雜性持續增加，需要建立更加完善的安全管理體系。

參考資料：

綜合 CrowdStrike、Palo Alto Networks、Fortinet、Check Point、McAfee、趨勢科技等知名網路安全公司的最新研究成果，以及美國、歐盟、英國、日本等主要經濟體的官方政策檔。CTA