星球永續健康線上直播

智慧數位資安 (3)

動態智慧資安

2026 年 4 月 15 日

傳統以防禦為主資安策略已難以應對高度自動化與快速演化的攻擊模式，人工智慧為核心的動態資安治理架構透過「辨識、保護、偵測、回應與復原」生命週期結合機器學習、異常偵測與強化學習等技術強化資安管理與入侵防禦。應用此人工智慧資安於醫療體系可在不中斷臨床服務的前提下，即時識別威脅並精準防禦。本週我們將探討醫療數位資安生命週期，以及醫療智慧數位資安防禦實例。

健康科學新知

美國-伊朗停火談判破局:「危機循環」

2026 年 4 月上旬，美國、以色列與伊朗之間的衝突迅速升高，雙方短暫停火又再度陷入衝突。自 2 月底美以聯合攻勢以來，區域衝突持續升高，伊朗隨後以飛彈、無人機及限制荷莫茲海峽通行等方式進行報復，使危機由軍事對抗延伸至全球能源與航運安全層面。美國與伊朗雖在衝突中尋求停火契機，但以色列上週仍對德黑蘭三座機場發動大規模空襲，目標涵蓋軍機、直升機及相關軍事基礎設施，攻擊重點擴展至伊朗整體空軍運作與後勤設施。其後美方針對荷莫茲海峽問題對伊朗發出強硬最後通牒，要求恢復航運通行，否則將攻擊其發電廠與橋梁等關鍵基礎設施，使戰爭目標由軍事設施擴展至國家民生與交通命脈。相關分析指出伊朗電力系統高度依賴天然氣火力發電，大型電廠多集中於人口與工業核心區域，且全國輸電網絡互相連結，一旦主要發電設施遭系統性破壞，影響將不僅止於停電，更可能連帶衝擊城市運作、工業生產、交通系統甚至核安風險，顯示能源基礎設施已成為影響整體社會運作的關鍵脆弱點。在軍事壓力逼近全面升級之際，美國與伊朗於巴基斯坦斡旋下達成為期兩週的有條件停火，並暫時恢復荷莫茲海峽通行。然而此停火協議自始即極為脆弱，各方對協議內容的理解存在差異。美方要求伊朗明確承諾不發展核武能力，而伊朗則強調其核計畫屬和平用途，並將談判視為

涵蓋核權利、制裁、賠償及海峽控制等多重議題的複合談判。隨著由副總統范斯領軍於巴基斯坦招開的美國-伊朗會談破局，美方宣布周一開始全面封鎖荷莫茲海峽並對伊朗港口實施海上封鎖，藉此限制伊朗相關收益並施加壓力。同時，美國部署海軍進行攔截與掃雷行動。儘管部分盟國支持航行自由，對實際封鎖行動的參與仍有限，加上其法律正當性存有爭議，使此舉在實際影響有限的情況下，仍可能進一步升高地緣政治緊張並波及全球能源市場。

中東衝突加深歐美分歧:「內外交迫」

歐洲當前正同時面對美國與伊朗達成附帶條件的兩週臨時停火，與後續荷莫茲海峽航運之不確定性，以及川普因北約盟友未加入對伊朗戰事而強烈不滿，甚至再度釋放美國可能退出北約的訊號，讓跨大西洋安全體系出現動搖。歐洲雖普遍歡迎中東衝突停火，但並未將其視為危機終點，強調必須進一步把停火轉化為涵蓋黎巴嫩、區域安全、航運恢復與長期外交談判的穩定安排，否則中東局勢仍可能再度升高。另一方美國對北約承諾的動搖使歐洲安全局勢更為嚴峻。川普上週不僅公開責備盟友未支持美方對伊朗的軍事行動，也以帶有威嚇與羞辱意味持續施壓歐洲國家，使退出北約或削弱北約功能的可能性成為現實政治議題，使北約集體防衛體系可信度受到動搖北約當前最大的風險之一為核心成員本身對同盟價值的懷疑與鬆動。在此背景下，北約秘書長呂特出訪美國與川普會談。呂特為少數能有效與川普互動並暫時穩住局勢的歐洲領袖，但面對北約信任基礎是否能夠維持的結構性難題使雙方會談難以達成具體安全協議，加上中東戰事美方要求軍事支援壓力使歐洲安全秩序面臨考驗。

英國及亞洲國家爭取航道安全:「權力重構」

2026 年伊朗戰爭使荷莫茲海峽成為全球能源與航運安全的關鍵節點。該海峽承載約全球五分之一的石油與天然氣運輸，在美國與以色列對伊朗發動軍事行動後，伊朗實質封鎖航道，導致航運量大幅下降、油輪滯留及國際油價上升，使原本依循國際海事法的通行機制，轉變為需透過與伊朗協商的選擇性通行制度，凸顯能源運輸高度政治化。面對此局勢，英國主導推動由四十多國組成的自願聯盟，試圖建立海峽安全通行機制，

並降低對美國維持航道安全依賴。然而該聯盟面臨資源不均與制度不足等挑戰，加上各國軍事能力差異，使整體協調與執行難度提高。即使衝突降溫，由於聯盟軍事控制能力差異航道安全仍難以迅速恢復。另一方面各國亦轉向與伊朗進行雙邊協商，以確保能源供應。部分亞洲國家已成功取得海峽通行，顯示能源運輸逐漸由多邊制度轉為政治條件下的協商機制，然而美方對海峽全面封鎖使能源運輸與海峽的實質控制權轉移，使全球能源市場更易受地緣政治影響，凸顯荷莫茲海峽在國際經濟與安全體系中的核心地位。

AI 算力擴建與地緣風險交織:「算力為王」

當前人工智慧產業正快速轉向以「算力與基礎設施」為核心的競爭模式。Anthropic 為因應生成式 AI 需求暴增，與 Google 及 Broadcom 建立長期合作，鎖定數吉瓦等級的 TPU 算力資源，以支撐模型訓練與商業擴張，並反映 AI 企業已進入高度資本密集與基礎設施導向的發展階段。同時，AI 產業的成長建立在龐大資本支出與高能源消耗之上，其財務結構與投資模式亦日益複雜，使整體體系對能源價格、利率變動與市場信心高度敏感。若能源成本上升或經濟環境轉差，可能動搖目前以高估值與長期預期支撐的產業擴張。此外，地緣政治風險開始直接影響 AI 基礎設施安全，例如中東衝突中資料中心成為潛在攻擊目標，顯示 AI 算力已具有戰略資產性質。這使企業在布局資料中心時，必須同時考量安全性、區域風險與供應鏈穩定性。

英國量子與核融合科技投資:「國力競技」

英國政府近期宣布投入約 20 億英鎊於量子運算，以及 25 億英鎊於核融合能源技術，作為其整體科學與技術戰略的一部分，目標在於提升關鍵前沿科技的自主能力並強化能源安全。政策獲學界普遍支持，但亦有觀點指出，現有資源仍不足以在全球競爭中取得領先，且此舉部分反映脫歐後為維持科研能量所進行的補強，因英國已失去部分歐盟資金與國際合作機會。在量子運算方面，英國採取從基礎研究到產業應用的完整布局，涵蓋技術研發、基礎設施建置、人才培育及新創發展，並透過政府採購創造市場需求，加速技術成熟與應用落地。然而，目前具備跨產業穩定優勢的大規模量子計算系統尚未實現，顯示該領域仍處於高度不確定與技術突破階段。在核融合領域，英國以 STEP 原

型電廠為核心推動高風險高回報計畫，並結合人工智慧超級電腦加速研究進程，期望達成能量輸出大於輸入的關鍵目標。同時，全球核融合發展已由國際合作轉向國家與企業競爭並行。然而，政策亦面臨潛在矛盾，即在強化前沿技術投資的同時，基礎研究資源可能遭到壓縮，長期而言恐影響人才培育與科研能力，進而限制英國在相關領域的持續競爭力。

AI 研究助理重塑科學研究模式:「機智共生」

人工智慧研究助理正逐步進入科學研究的核心流程，從文獻回顧、研究設計、實驗執行到論文撰寫皆可參與完成。以 The AI Scientist 為例，其已能產出完整論文，甚至通過機器學習會議 workshop 的初步同儕審查，顯示 AI 正從輔助工具轉變為知識生產的參與者。科技公司如 Google、OpenAI 與 Anthropic 亦積極推動研究自動化，意味著科學研究的運作模式可能出現結構性改變，影響研究者、學術機構與出版制度。然而，AI 在研究中的應用仍存在顯著限制與風險。模型容易產生「幻覺」，包括虛構數據與錯誤引用，且在長期、多步驟的研究流程中難以維持穩定與邏輯一致性。此外，AI 可能大量生成表面完整但缺乏實質價值的研究成果，甚至形成自動化的 P-hacking，進一步衝擊學術品質與審查體系。同時，AI 的不透明性也引發倫理問題，包括知識來源不明、學術貢獻難以界定，以及對年輕研究者訓練機制的潛在削弱。因此，AI 雖具備加速科學發現的潛力，但其影響已超越效率提升，涉及研究本質與學術制度的重塑。當 AI 開始介入研究核心，學界需同步建立透明性、規範與評估機制，以確保研究品質與可信度。未來關鍵不在於 AI 是否參與科學，而在於能否在其快速發展下，建立適當制度，使其成為促進知識發展的工具，而非削弱學術信任的來源。

健康數位資料治理模式:「數據共治」

真實世界資料（RWD）在醫療體系中具有高度潛力，但長期受到分散、專有與缺乏互通性等問題限制，難以有效應用於公共衛生、精準醫療與即時決策。為解決此一困境，本文主張應將健康資料視為公共基礎設施，並採取聯邦式、標準化且以社群為導向的治理模式，以強化資料共享、提升社會信任並促進公共利益。公共事業模式可作為健康資

料治理的重要參考。透過政府監管、標準化機制與多方參與，可建立穩定且可持續的資料體系，同時兼顧資料可用性與隱私保護。在技術與制度層面，需整合不同資料標準、支援多元資料型態，並在資料連結與再識別風險之間取得平衡，以確保資料能安全且有效地被利用。然而，目前 RWD 系統仍面臨治理碎片化、誘因不足與法律架構不完整等挑戰。為此，本文建議透過新的制度設計與法規調整，強化資料存取透明性、病人自主權及多元利害關係人參與。最終，透過公共事業模式的導入，可在維持資料所有權的同時，促進資料共享與創新應用，進一步提升醫療體系的公平性與效率。

醫療數位資安生命週期

在各類敏感資訊中，情報資料的風險層級最高，一旦外洩，將直接危及人員安全並衝擊整體系統運作。因此，本週以電影《Skyfall》作為案例說明資安威脅如何演變為重大危機。影片開端描述龐德於伊斯坦堡追捕傭兵，試圖奪回一份遭竊的機密硬碟。該硬碟儲存北約所有臥底特務的身分名單，屬於極機密資訊，僅限內部存取。此名單一旦外洩，潛伏於全球的情報人員將面臨致命風險，並可能引發英國情報體系前所未有的資安危機。同時，此事件亦揭示攻擊並非單一事件，而是由前 MI6 特工席爾瓦所策動的長期滲透與報復行動，逐步瓦解情報系統的運作基礎。然而，在任務初期，硬碟未能成功取回，行動宣告失敗，龐德亦因此陷入生死危機。此一情境突顯，在數位時代中，資安事件不僅是資訊外洩問題，更可能擴散為組織運作失靈與實體安全威脅，進一步強化資安治理的重要性。

在事件發展過程中，MI6 的資安偵測機制發揮作用。當攻擊者嘗試破解失竊硬碟中的加密名單時，系統即時發出警示，顯示未經授權的解密行為正在進行。此一訊號同時帶來兩種意涵：一方面，代表攻擊者已進入破解階段，存在資料外洩的高度風險；另一方面，也提供了追蹤攻擊來源的機會，使情報單位得以進行定位與反制。面對此關鍵決策時刻，MI6 必須在「立即中斷系統以防止資料外洩」與「暫時允許攻擊持續以利追蹤來源」之間取得平衡。最終決策選擇後者，即在監控攻擊行為的同時加速定位攻擊者。然而，隨後的追蹤結果顯示，入侵來源竟來自 MI6 內部系統，甚至直接利用高層電腦作

為攻擊節點，顯示資安威脅已深入組織核心。進一步地，攻擊者透過系統入侵向 MI6 領導者發出心理威嚇訊息，並結合遠端控制技術，引發辦公大樓瓦斯爆炸，造成實體層面的傷亡與設施損毀。此一事件清楚揭示，數位資安攻擊已不再侷限於虛擬空間，而是能夠跨域連動至實體世界，形成複合式災難。最終，此次資安入侵不僅帶來人員與財務損失，更重創情報機構的信任基礎與公信力。

龐德再次被派遣執行任務，以追查攻擊源頭並遏止危機擴散。經過一連串行動後，最終鎖定攻擊核心位於一座廢棄孤島。該地點實為攻擊者所建立的情報與資安入侵中樞，大量伺服器與運算設備構成其技術核心，負責統籌整體攻擊行動與資料操作。進一步調查顯示，失竊的特務名單並非單純的情報洩漏事件，而是一項經過精心設計的誘餌機制。攻擊者利用名單吸引 MI6 投入大量資源進行追查，藉此逐步引導對方進入其預設的攻擊節奏，形成如同「特洛伊木馬」般的策略性滲透，最終達成其長期規劃的報復行動。攻擊主謀席爾瓦原為 MI6 情報人員，因過往任務中遭組織放棄而產生強烈報復動機，進而策劃整體攻擊行動。其選擇在孤島架設資訊基礎設施，具有明確的資安意涵：透過物理隔離（air-gapped environment）確保系統不直接暴露於外部網路，降低被反向入侵的風險；同時在必要時，再透過特定通訊管道對外發動精準攻擊，展現高度控制與隱蔽性。儘管龐德最終成功定位並逮捕席爾瓦，但隨後揭示此行動亦在對方的計畫之中。被捕本身即為其策略的一環，目的是進一步滲透 MI6 內部系統並推進後續攻擊。

在席爾瓦被逮捕並帶回情報指揮中心後，其角色由外部攻擊者轉變為內部滲透節點，形成典型的「特洛伊木馬」攻擊模式。其所攜帶的筆電表面上為關鍵證物，實則為預先設計的入侵媒介，使敵方得以藉由合法流程進入核心系統。在技術層面上，該筆電內部包含高度複雜的加密結構與動態變形機制。其運作類似拓樸網絡與多層次交互系統，一旦嘗試解碼，原有結構即會自動重組，使破解過程更加困難，呈現出高度對抗性的加密設計，增加追蹤與分析的難度。情報官 Q 在分析過程中，嘗試連接系統以進行解密與資料擷取。然而，在啟動破解程序的同時，筆電內預藏的惡意程式隨即被觸發，導致整體系統發生異常行為。該攻擊進一步引發錯誤警報機制，使情報中心誤判為火警並解除門

禁管制，最終讓攻擊者成功突破內部防線。此一事件揭示，當代資安攻擊已從單純的外部入侵，演變為結合社交工程、惡意程式與系統漏洞的複合式攻擊。攻擊者不僅利用技術手段，更透過設計誘導行為，使防禦方在正常操作流程中主動打開防線，造成「人機協同失誤」的風險。最終，MI6 不僅在行動層面損失關鍵人員與資源，其數位情報系統亦遭全面滲透，導致機密資訊外洩與系統失控。此案例突顯，資安防禦不僅需強化技術能力，更需重視整體系統設計與決策流程中的風險控管，以避免攻擊透過「看似合理」的操作途徑進入核心系統。

在人工智慧時代，若未能全面理解與掌握 AI 資安生命週期，無論是運用 AI 強化資安防禦（AI for Cybersecurity），或是確保 AI 系統本身的安全性（Cybersecurity for AI），皆將面臨重大風險。從資安治理的核心架構 IPDRR（Identify、Protect、Detect、Respond、Recover）觀之，資安已不再是單一防護措施，而是一個涵蓋風險辨識、預防、防禦、應變與復原的完整動態循環。

若缺乏對此生命週期的整體掌握，對於如情報資料等高度敏感的資訊系統，將難以建立有效的防護機制。正如前述案例所示，一旦資安治理出現斷點，攻擊者即可利用系統漏洞、決策延遲或人為操作流程，逐步擴大滲透範圍，最終導致系統性風險與連鎖性危機。因此，在智慧時代的數位資安治理中，關鍵不僅在於單一技術的強化，而在於如何整合 IPDRR 各階段，建立跨層級、持續運作的防禦體系。唯有透過全生命週期的策略規劃與動態調整，方能有效應對高度演化且複雜的資安威脅，確保關鍵資訊與系統運作的安全性與韌性。

在智慧時代下，數位資安威脅的態樣已產生根本性的轉變。首先，攻防速度急遽加快，以銀行系統為例，過去的攻擊與回應週期以「天」為單位計算，如今已縮短至「秒」級，自動化與高速攻擊對抗已成為常態，防禦端若無法同步提升反應速度，將面臨極大風險。與此同時，攻擊規模亦突破了傳統安全邊界。攻擊者採取大規模探索策略，且往往由小規模滲透逐步擴大。僅需一部小型電腦，即可透過殭屍網路（Botnet）將惡意載體大範圍傳播，實現以小搏大的攻擊效果。更值得關注的是，攻擊工具與技術門檻持續

下降，使得發動攻擊的邊際成本大幅降低。如同先前 Operation 007 案例中所揭露的，攻擊者甚至可利用設置於偏遠地區的伺服器，以極低成本執行大規模攻擊行動。此外，攻防雙方均朝向無人化與共演化（Co-evolution）發展，攻擊端的自動化程度不斷提高，使得攻擊行為能在無人介入的情況下持續進化與調適，防禦端亦須同步發展自動化應對能力。綜合攻防速度、攻擊規模、邊際成本與自動化協作程度的全面變化，AI 時代的資安核心風險已超越單純的「系統被駭」，不再僅止於病毒感染或系統被侵入。風險本質已轉變為系統被操控（Manipulated）、被誤導（Misled）、被竊取（Stolen）、被濫用（Abused）。以 Meta 遭受滲透的案例為例，攻擊者初期透過社交工程手段進行釣魚，製造爆炸事件以誤導判斷，進而竊取系統資源、操控系統運作、濫用系統功能，最終使整體決策結構產生看似可信卻錯誤的決策。這正是當前全球資安環境中普遍面臨的嚴峻挑戰。

在前述智慧時代資安威脅快速演化的背景下，若將情報體系的資安風險轉換至醫療領域，可發現醫療資料同樣屬於高度敏感且具高價值的關鍵資產，其保護需求不亞於國家級情報資訊。因此，建立對各類資安攻擊型態的系統性理解，成為數位資安治理的核心基礎。隨著攻擊速度加快、規模擴大、成本下降與自動化程度提升，現代資安威脅呈現多樣化且高度複雜的特性。傳統攻擊模式包括勒索軟體（ransomware）、惡意軟體（malware）、釣魚訊息（phishing）、SQL 資料隱碼攻擊（SQL injection）以及阻斷服務攻擊（DDoS），這些手法已長期存在並持續演進。同時，新型態攻擊亦不斷出現並與既有技術結合，例如中間人攻擊（man-in-the-middle attack），可在通訊過程中攔截與竄改資料；零日漏洞攻擊（zero-day exploit），利用尚未被修補的系統漏洞發動攻擊；DNS 隧道攻擊（DNS tunneling）則可隱匿資料傳輸行為；跨網站指令碼攻擊（XSS attack）與社交工程（social engineering）則進一步利用系統漏洞與人為弱點進行滲透。

在眾多數位資安攻擊型態中，本案例聚焦於勒索軟體（ransomware）。假設某醫學中心遭遇勒索病毒攻擊，其主要攻擊目標包括電子病歷（EMR）、健保申報資料以及 PACS 影像系統，這些皆屬於高度敏感且關鍵的醫療資料。在資安治理的「辨識風險

（Identify）」階段，醫院需導入 AI 進行系統性盤點與風險評估。首先為資產盤點（asset inventory），用以釐清哪些系統屬於核心關鍵系統，以及哪些系統包含敏感資料，例如病歷資料與基因資料。其次為使用者風險評估，需辨識哪些帳號權限過高，以及是否存在異常登入行為。在 AI 技術應用方面，透過機器學習（machine learning）進行風險分群，並利用關聯網路（graph-based risk mapping）分析系統與使用者之間的關聯結構，以提升風險辨識的準確性。在實務案例中，透過上述方法可發現潛在高風險節點，例如放射科某台未更新的舊 Windows 機器，即屬於資安防護中的弱點，需優先處理以降低整體系統風險。

在完成「辨識風險（Identify）」階段後，下一步即進入「防護（Protect）」階段，其核心在於預防攻擊發生。此階段包含動態權限管理（AI-driven access control）、敏感資料自動分類，以及網路釣魚（email phishing）的過濾機制。在 AI 技術應用方面，可透過自然語言處理（NLP）偵測釣魚信件，並利用 BiLSTM 模型分析敏感資料與文字特徵，以提升辨識準確度。在實務案例中，AI 可偵測出一封偽裝成健保署通知的 phishing mail，並即時進行自動攔截，有效阻止潛在攻擊進入系統。然而，若攻擊仍成功滲透系統，則需進入「偵測（Detect）」階段，即時發現異常行為。在實務情境中，例如某帳號於非正常時間登入、大量下載病歷資料，或從國外 IP 進行連線，皆屬於異常行為指標。此時，AI 可透過異常偵測（anomaly detection）技術，結合深度學習（DL）與時序模型，分析行為是否偏離既有正常模式（baseline）。當系統判定行為異常時，即可進一步識別為潛在攻擊事件，例如進階持續性威脅（APT），以利後續應變與防護措施的啟動。

在完成「防護（Protect）」與「偵測（Detect）」之後，當系統確認遭受攻擊，即進入「回應（Respond）」階段。此階段的核心在於即時處理攻擊事件，系統需能自動執行相關措施，包括封鎖帳號、切斷網路連線，以及隔離感染主機（network segmentation），以防止攻擊持續擴散。在 AI 技術應用方面，主要透過強化回饋學習（reinforcement learning, RL）進行最佳決策判斷，並結合自動化安全營運中心（Security Operation Center, SOC），即

時分析攻擊情境並採取適當行動。實務案例顯示，RL 模型可協助判斷是否應立即斷網或持續觀察，並在「醫療服務不中斷」與「資安防護」之間取得平衡。在攻擊事件處理完成後，系統需進入「復原（Recover）」階段，以恢復正常運作。此階段包含還原備份、重建電子病歷系統，以及評估資料是否外洩等關鍵作業。在 AI 應用方面，可透過數位雙胞胎技術模擬不同復原策略，並結合貝氏模式進行損害評估，以選擇對病患影響最小的復原方案。實務上可透過模擬比較不同系統的優先復原順序，例如急診系統與住院系統，評估何者對整體醫療運作影響較低，進而制定最適復原決策。

醫療智慧數位資安防禦實例

勒索軟體通常以多種途徑入侵系統，例如透過釣魚郵件取得初始存取權限，或經由其他管道將惡意程式植入系統，進而擴散至整體網路環境。以愛爾蘭衛生管理機構（HSE）事件為例，2021 年 5 月，該國醫療體系遭受 Conti 勒索軟體攻擊，導致全國醫療 IT 系統大規模中斷。此次攻擊的目標為全國醫療資訊系統，造成病患資料遭非法存取，並使預約、檢查與行政流程嚴重受阻。回溯事件發展，攻擊早於 2021 年 3 月即已潛伏，至 5 月 14 日全面引爆。攻擊者為 Conti（俄語系犯罪組織），在長時間未被偵測的情況下，逐步擴大存取權限並完成滲透。此事件顯示資安攻擊具有長期潛伏與分階段發動的特性。在影響規模方面，超過 80,000 台裝置受到影響，約 700GB 的敏感與病患資料外洩，醫療服務被迫降級，包括放射科、化療及急診等單位需改以紙本方式運作。在財務損失方面，攻擊者提出 2,000 萬美元贖金要求（最終未支付），而直接復原成本超過 6,000 萬歐元，此外，全國醫療服務中斷所造成的間接損失難以估算。

該事件起始於釣魚郵件攻擊。攻擊者透過電子郵件夾帶惡意 Excel 檔案，當使用者開啟檔案後，即在系統中建立初始存取點。該過程並不需要明確的安裝行為，而是透過檔案內嵌程式碼執行惡意操作。在初始入侵後，攻擊並未立即引發大規模影響，而是先於單一電腦中建立據點，並透過網路橫向移動（lateral movement）逐步擴散至其他系統。在此過程中，相關異常行為並未即時被整合與辨識。根據事件時間軸，2021 年 5 月 7 日

攻擊者首次入侵 HSE 伺服器，但未觸發任何警報。至 5 月 10 日，部分醫院系統已出現惡意活動，惟警報未升級，亦未引發全面警戒。5 月 12 日，醫院向中央 IT 部門通報異常，但由於資訊未整合，仍無法拼湊完整攻擊脈絡。至 5 月 13 日，防毒供應商針對 16 台系統發出「未處理威脅」之警示，然而營運單位僅採取重啟伺服器的措施，並未啟動進一步的深入調查與防禦部署。最終於 5 月 14 日凌晨，Conti 勒索軟體全面啟動，加密大量系統與資料，導致攻擊全面爆發。

當醫療系統遭受勒索軟體攻擊並被加密後，對醫療運作將產生重大影響。相較於金融體系可能導致交易異常，醫療體系的中斷則直接影響病患照護與臨床決策。在正常情況下，醫療院所透過數位化工作流程運作，包括電子系統開單與即時傳輸、影像系統隨時調閱歷史資料進行診斷，以及透過電子病歷系統整合並產出報告，整體運作具備高度效率與即時性。然而，一旦系統遭加密攻擊，醫療流程將被迫轉為應變模式。開單與傳遞需改為紙本手寫並人工傳送；影像調閱與診斷則因無法存取歷史數位影像，全院僅能使用非專用設備進行有限判讀；報告產出亦需改為手寫病歷與報告。在此情境下，數位影像無法存取，歷史檢查資料無法調閱，將直接影響臨床工作流程。病患可能需重複接受影像檢查，進一步導致腫瘤分期與臨床治療決策延遲。此外，影像檢閱工作站失效，使臨床檢查需仰賴傳統方式調閱實體影像資料，第一線醫療工作被迫回到以人工方式取得資訊的狀態，僅能維持基本醫療運作，整體醫療服務品質與效率大幅下降。

在愛爾蘭事件後，醫療系統雖逐步恢復運作，但已付出極高的時間與成本代價。另一案例為法國 Dordogne 醫療組織，其資安事件同樣突顯醫療體系在數位化環境下的脆弱性。該組織涵蓋 11 間醫院、近 5,000 名員工，其防禦範圍包括企業資訊技術（Enterprise IT）以及醫療營運技術與急診設備（Medical OT/ER devices）。整體系統高度依賴網路連結，從行政作業、臨床決策到醫療設備運作，皆需透過資訊系統即時運行。然而，醫療體系具有其特殊性：一方面設備老舊且不容許停機，另一方面全面斷網或隔離的傳統防禦手段，可能直接影響病患健康與生命安全。因此，在資安防禦上面臨高度限制與挑戰。在攻擊機制方面，Ryuk 勒索軟體呈現典型攻擊鏈流程。首先透過釣魚郵件或載入器進

行初始存取；接著進入潛伏偵查階段，於系統中長期隱匿並提升權限；隨後透過 RDP 或 SMB（Port 445）進行橫向移動與擴散；最終啟動加密機制，採用 RSA-4096 與 AES-256 混合加密技術，快速加密本機與網路磁碟資料。此類攻擊具備高度變異性與無固定特徵碼（signature-less）的特性，使傳統防毒軟體難以有效辨識，形成資安防護上的盲區。

法國醫療體系採用了以 AI 為核心的數位資安防禦機制，其運作邏輯與傳統防毒軟體存在顯著差異。傳統防毒系統主要依賴已知威脅特徵碼進行辨識，即透過黑名單機制偵測已知的惡意軟體或攻擊行為。然而，此類方法對於未知攻擊或無固定特徵碼的威脅，防禦能力有限。相較之下，AI 資安防禦採用非監督式機器學習方法，不依賴既有威脅特徵碼，而是從零開始學習系統的正常運作狀態，進而辨識異常行為並攔截潛在攻擊。此一機制類似人體免疫系統，透過全面認識「正常狀態」，精準排除異常活動。AI 可透過「生活模式（Pattern of Life）」建立多維度行為模型，整合時序行為、連線模式、資料流量、同儕比較與情境因素進行分析，持續監測系統運作。在此基礎上，資安防禦機制可隨環境變化自動調整，於動態環境中維持即時防護能力，並有效辨識未知或變異型攻擊，補足傳統防毒系統在面對新型威脅時的不足。

在防禦機制上，該醫療體系導入以 AI 為核心的資安系統（如 Darktrace），其運作方式模擬人類專家進行判斷與分析。整體流程包含：先從系統中擷取初始異常行為作為「線索（Lead）」，進一步提出可能的威脅「假說（Hypothesis）」，再透過跨系統的「查詢（Query）」進行驗證或推翻假說，最終產出自然語言的「報告（Report）」以說明事件根因與影響，形成完整的自動化調查循環。此機制可大幅縮短調查時間，並降低人工介入需求。在攻擊初始階段的偵測上，AI 採用異常行為分析，而非依賴既有特徵碼。例如在 Ryuk 攻擊中，惡意程式可能以.dat 檔形式出現，傳統防毒或入侵偵測系統（IDS）可能將其判定為正常活動而未觸發警報；然而，AI 可透過行為偏移偵測，辨識其不符合系統日常運作模式，及早發現潛在威脅。在回應機制方面，系統採用 Antigena 自主回應技術，以「最小影響原則」進行防禦。當偵測到異常行為時，系統僅針對可疑連線進行即時阻斷，而不影響其他正常通訊；同時透過生活模式（Pattern of Life）限制設備僅能

維持正常行為。必要時，系統可中斷設備對內與對外的連線，以防止攻擊擴散。此外，系統亦具備持續監控與動態調整能力，可降低可疑設備的傳輸速度，以減少資料外洩風險。在此過程中，AI 可辨識關鍵風險節點，進行精準隔離與控制，避免採取全面斷網等高衝擊措施，從而在維持醫療服務運作的同時，有效抑制資安威脅的擴散。

以上內容將在 **2026 年 4 月 15 日（三）10:00 am** 以線上直播方式與媒體朋友、全球民眾及專業人士共享。歡迎各位舊雨新知透過星球永續健康網站專頁觀賞直播！

- **星球永續健康網站網頁連結: https://www.realscience.top/7**
- **Youtube 影片連結: https://reurl.cc/o7br93**
- **漢聲廣播電台連結: https://reurl.cc/nojdev**
- **不只是科技：https://reurl.cc/A6EXxZ**

講者：

陳秀熙教授/英國劍橋大學博士、許辰陽醫師、陳立昇教授、嚴明芳教授、林庭瑀博士

聯絡人：

林庭瑀博士　電話: (02)33668033　E-mail:happy82526@gmail.com

劉秋燕　電話: (02)33668033　E-mail: r11847030@ntu.edu.tw