數位時代戰爭的重新定義：默克案與資安保險的演變

廖士傑*
游淑君**

壹、前言

據統計，我國產險公司資安保險之保費收入，已由2018年之新臺幣8,908萬元逐年提升至2023年之新臺幣5.28億元，呈穩定成長趨勢，投保產業類別上，2018年至2021年以金融保險業投保占比最高，2022年起電腦及週邊設備業、半導體業之保費收入已超過金融保險業。金管會表示，伴隨數位經濟加速發展，包括資訊服務業、貿易百貨業、教育及文化產業，廣泛運用網絡服務且保有大量個資，倘受到網絡攻擊恐造成業務中斷及資料外洩等損害，因此透過資安保險進行風險移轉，實為企業永續經營之重要策略。金管會提醒，企業除優化資安防護及應變措施，以精實資安作業韌性外，亦應重視資安事故發生時之風險有效移轉，藉由適時評估投保資安保險，完善風險管理，以確保企業得以在安全之基礎上穩定成長[1]。

隨著數位時代的到來，新的衝突形式層出不窮，國家與非國家行為者策劃的網絡攻擊變得日益頻繁且破壞性十足。傳統戰爭概念──如軍事入侵或轟炸──如今已被補充為更為複雜的網絡攻擊行動，目標包括基礎設施、金融系統和私人企業。2017年的「NotPetya」攻擊，便是這一趨勢的典型案例，該攻擊被廣泛認為由俄羅斯國家行為者發動，原本旨在破壞烏克蘭的穩定，但最終波及全球，對默克公司（Merck & Co.）等跨國企業造成重大損失，並導致數十億美元的經濟損失。

面對網絡攻擊風險的增加[2]，企業正轉向保險來減輕其潛在損害。然而，保險業者在調

＊本文作者係國立政治大學風險管理與保險學系兼任助理教授
＊＊本文作者係國立政治大學風險管理與保險學系博士生

註1：金融監督管理委員會保險局（2024），〈金管會提醒企業重視資安風險管理，適時評估投保資安保險〉，https://www.ib.gov.tw/ch/home.jsp?id=239&parentpath=0,2,238&mcustomize=multimessage_view.jsp&dataserno=202409260001&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News（最終瀏覽日：2024年12月24日）

註2：Marsh McLennan and Zurich Insurance Group (2024), Closing the Cyber Risk Protection Gap. p.4. Available at: https://www.marshmclennan.com/insights/publications/2024/september/closing-the-cyber-protection-gap.html (last visited Aug.22 2025)

整傳統保單以涵蓋與網絡相關的事件時，面臨諸多挑戰，尤其是那些涉及地緣政治衝突的攻擊。其中一個主要法律障礙便是保單中的「戰爭除外條款」（war exclusions），該條款限制了對戰爭行為所造成損害的理賠範圍。此類條款原本是針對傳統的物理戰爭而設計，但當其被應用於數位攻擊時，就引發了重要的法律與保單爭議。

默克公司的案例使這些問題成為輿論熱議的核心。默克公司的保險公司ACE American Insurance Co.以戰爭除外條款為由，拒絕賠償其因NotPetya攻擊所遭受的損失，並聲稱該攻擊屬於國家支持的行動。這場法律訴訟最終促成了一項具有劃時代意義的裁決：紐澤西法院判決指出，除非網絡攻擊涉及直接的軍事行動，否則戰爭除外條款不適用於此類事件。本文分析默克案對資安保險的影響，檢視保單條款調整的趨勢，並探討保險公司與企業如何做好準備，以應對未來的國家支持型網絡威脅。

貳、文獻回顧

隨著勒索軟體攻擊、資料外洩和國家支持的網絡行動愈發猖獗，企業需要更成熟的風險管理工具，這推動了資安保險的成長。然而，現有保險框架在應對這些複雜而新穎的威脅時存在不足。本節檢視資安保險的演變，探討保單承保範圍面臨的挑戰，並分析如何有效解決國家行為者攻擊的歸因問題及其引發的法律爭議。

一、資安保險的發展

自2000年以來，資安保險迅速發展，以因應資料外洩及網絡攻擊所造成的財務損失。最初，保單主要針對企業遭受的直接經濟損失進行賠償，例如系統停機、勒索贖金支付及災後復原成本。然而，隨著地緣政治緊張局勢升高，企業開始面對與國家支持行為者相關的攻擊。學者如Anderson與Moore（2020）認為，國家行為者的介入將網絡風險引入了新的層面，而傳統的資安保險保單並未設計用來應對這類型的風險[3]。

二、保單中的戰爭除外條款

戰爭除外條款長期以來一直是財產保險的標準條款。這些條款通常拒絕理賠因戰爭或

「網絡攻擊者正利用生成式人工智慧（AI）等進階技術，採取逐漸複雜的手段入侵系統。當前嚴峻的資安環境，因地緣政治緊張局勢升溫而雪上加霜，數位領域已成為國家或國家支持的網絡攻擊行為者之戰略場域。

在提升網絡韌性方面，已經取得重要進展，例如將可得的數據與各種資安控制措施的成效相連結。然而，仍有許多工作亟需完成；每一次網絡攻擊事件（包括日益頻繁的勒索攻擊）都帶來新的教訓，並推動風險管理策略的調整與應用。

近年來，資安保險市場快速成長，2023年的保費總額（Gross Written Premium, GWP）估計達140億美元，預計2027年將成長至超過兩倍。然而，即使如此增長，網路風險保障缺口依舊存在，據估計，網絡攻擊所造成的經濟損失與已投保損失之間的差距，估計高達0.9兆美元，約佔99%的經濟損失。此外，雖然企業轉嫁資安風險的需求持續上升，但這種成長並不均衡，中小型企業（Small and Medium-size Businesses, SMBs）仍普遍存在著未投保或保險不足的隱憂。」

註3：Anderson, R., & Moore, T. (2020). Risk and Insurance in the Cyber Age: Emerging Trends and Challenges. Journal of Cybersecurity, 5(2), 123-140.

軍事衝突（如武裝入侵或轟炸）所造成的損害。然而，將此類除外條款應用於網絡攻擊的合法性仍具模糊空間。法院和保單制定者目前面臨的挑戰是，如何在保險法框架內界定與國家相關的網絡攻擊是否構成「戰爭行為」。Gordon與Caputo（2021）等學者強調，保險業者需要重新定義這些條款，以反映現代網絡戰爭的現實[4]。

三、歸因挑戰與法律框架的演進

網絡攻擊的隱蔽性和國家與非國家行為者的交錯，使得準確歸因於某一國家行為者變得極具挑戰，這對保險業者造成了極大的困擾。是否能確認攻擊為國家支持，往往決定了戰爭除外條款的適用性。在默克案之前，如何將戰爭除外條款擴展至網絡事件仍屬法律空白。該案的裁決成為資安保險領域的轉折點，裁決內容表明，除非網絡攻擊涉及軍事行動，否則戰爭除外條款無法生效。

四、保險業對國家支持網絡攻擊的回應

在國家支持的網絡攻擊持續增加的背景下，保險業也開始調整其保單承保範圍的策略。例如自2023年起，倫敦勞合社強制規定，其保單需排除國家支持的網絡行動（Lloyd's Market Bulletin, 2023）[5]，以避免法律爭議，並確保條款透明清晰。然而，此舉在減少保險業風險的同時，也將企業暴露於重大網絡威脅之中，進一步推動了由政府協助支持資安保險計劃的呼籲。

學者Angad Chopra（2021）認為，對於網絡攻擊保險理賠爭議，短期內的應對措施，法院應運用contra proferentem principle（即對不明確條款進行解釋時，疑義利益歸屬於非起草方），評估保單語言的明確性以及雙方議價能力，分析具體的財產全險保險應該偏向被保險人還是保險人的有利解釋，然而，這僅是一個短期的臨時解決方案，對於可能演變成壓倒性損失的情況而言仍顯不足，如果法院偏向保險人，被保險人將不得不承擔巨大的損失，無法尋求足夠的補償；反之，如果法院偏向被保險人，保險人可能面臨高額索賠的責任，甚至威脅其償付能力。因此，長期而言，應當制定一個由政府協助支持的專門網絡安全保險計劃，針對因網絡攻擊引發的損失進行承保，此顯然是針對保險體系中必要補充方案[6]。

學者何啟豪（2024）則是進一步提出，即便國家已針對網絡安全建置相關法規，規範網絡安全責任主體、數據安全保護義務等面向，卻未同步建立網絡安全保險制度，因此，應在政府與保險業的公私合作框架（public-private partnerships），建立多層級網絡風險分散機制，提供可負擔的網絡安全保

註4：Gordon, P., & Caputo, M. (2021). "War Exclusions in the Context of Cyber Insurance: A Legal Analysis." Insurance Law Review, 48(4), 237-254.

註5：Lloyd's Market Bulletin. (2023). Cyber War and Operation Exclusions: Revised Guidelines for Underwriting. Lloyd's of London.

註6：Angad Chopra, Cyberattack-Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims, 82 OHIO ST. L.J. 121 (2021), p162.

險，並制定網絡安全保險標準保單，以減少賠付爭議與司法糾紛[7]。

參、案例研究：默克公司（Merck & Co.）與保險公司之間的法律爭端

一、NotPetya網絡攻擊概述

2017年6月爆發的NotPetya網絡攻擊，最初針對烏克蘭的政府機構、企業和關鍵基礎設施。然而，該惡意軟體迅速蔓延至烏克蘭以外地區，波及多家跨國企業，包括航運巨頭快桅（Maersk）、聯邦快遞（FedEx）和默克公司（Merck & Co., Inc.）。NotPetya攻擊透過加密電腦系統，導致資料無法恢復，並造成大範圍破壞。雖然該攻擊表面上看似勒索軟體攻擊，但它並未提供支付贖金的機制，因此專家認為其主要目的是破壞性行動。

二、拒絕賠償與「戰爭行為」除外條款

全球製藥業巨頭默克公司及其專屬保險公司International Indemnity, Inc.（以下統稱「默克公司」）購買了保險金額17.5億美元，保險期間為2017年6月1日起為期一年的財產全險保單（Property All Risks Policy），自負額為1.5億美元。

2017年6月27日，名為NotPetya的惡意軟體感染了默克公司的電腦和網絡系統。在此之前，有人侵入了一家烏克蘭公司的電腦系統，該公司開發了一種名為M.E. Doc的會計軟體，默克公司和烏克蘭的其他公司使用該軟體處理發票、稅務和其他財務數據，並傳輸資料給烏克蘭政府。

默克公司在NotPetya網絡攻擊中蒙受重大損失，40,000多台電腦停擺，導致生產中斷及供應鏈受損。公司估計，整體損失達14億美元。為此，默克公司依據其財產全險保單向保險公司申請理賠，以彌補相關損失。

默克公司的保險公司（包括ACE American Insurance Co.等保險公司共同承保）拒絕理賠，理由是本案應適用保單中之「戰爭行為」除外條款（the Hostile/Warlike Action Exclusion）[8]。保險公司辯稱，NotPetya是國家支持的網絡攻擊，且由於該攻擊源自俄羅斯

註7：何啟豪（2024），〈應對網絡安全風險的保險保障機制論要〉，《中國政法大學比較法研究》2024年第3期，第125、132頁。

註8：The Hostile/Warlike Action Exclusion Language in insurance policy wording, Section 6 “LOSS OR DAMAGE EXCLUDED” (A)(1), “This policy does not insure against: 1 Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack:

a)by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces;

b)or by military, naval, or air forces;

c)or by an agent of such government, power, authority or forces;

This policy does not insure against loss or damage caused by or resulting from Exclusions A., B., or C., regardless of any other cause or event contributing concurrently or in any other sequence to the loss.（中譯：損失或損害除外條款(A)(1)「本保單不承保以下情況導致的損失或損害：

與烏克蘭之間的地緣政治敵對行為，該惡意軟體是俄羅斯聯邦的工具，是其針對烏克蘭國家持續敵對行動的一部分，因此構成了戰爭行為。戰爭行為除外條款通常排除因戰爭、入侵或軍事行動所造成的損害的賠償。保險公司認為，NotPetya與國家行為者有關，因此符合除外條款的範圍，進而拒絕了默克公司的理賠請求。

三、法律訴訟與法院裁決

由於默克公司投保的是傳統的財產全險保單而非特定的資安保險，因此，對於惡意軟體NotPetya所引發網絡攻擊造成的損失，法律訴訟的主要爭議問題闕為，財產全險保單中未明文提及「網絡攻擊」是否在其保障範圍之內，以及是否得以適用敵意或戰爭行為除外條款，尤以該除外條款明文提及，歸因於國家或國家行為代理人行為所造成之損失除外不保。

默克公司對保險公司的賠償拒絕提出異議，其主張戰爭除外條款僅應適用於傳統的軍事行動，而不包括網絡事件。2022年，美國紐澤西州高等法院（Superior Court of New Jersey）裁定默克公司勝訴，認為敵意或戰爭行為除外條款「不適用」於NotPetya攻擊。法院強調，除外條款的文字依其字面上的意思，是指傳統戰爭行為（如轟炸和入侵），而且該條款未反應網絡衝突的現實。因此，保險公司必須為默克公司的損失負起賠償責任。

保險單中使用的措辭多年未作修訂，儘管各類網絡攻擊事件日益頻繁，且有時涉及國家行為，保險公司仍未採取措施修正保單條款，以明確排除此類風險的承保責任。法院指出，舉證責任在於保險公司，其需證明其解釋是唯一合理的詮釋，並至少適用於除外條款中的任一項規定。鑑於保險公司從未更新相關條款，默克公司基於保險法中的合理期待原則（Reasonable Expectations Rule），有充分理由認為豁免條款僅適用於傳統的戰爭形態，且此見解亦與相關判例法相符。

2023年，紐澤西州上訴法院（New Jersey Appellate Court）確認了初審法院的判決，強調相關除外條款的明文內容無法支持保險公司所主張的解釋。該條款僅排除因政府或主權力量在戰爭或和平時期進行的敵對行為或軍事行動所造成的損害，而非適用於針對非軍事性公司（例如提供商業用途會計軟體的企業）的網絡攻擊。無論此類攻擊的來源是私人行為者，還是由政府或主權力量發動，均不在條款除外的範圍內。本案的裁決對保險公司與企業投保人在面對日益嚴峻的網絡風險時，凸顯了保單條款需要更加明確且精準的措辭。

此外，2017年受到惡意軟體NotPetya攻擊

1.因敵對或類似戰爭的行為所造成的損失或損害，無論是在和平或戰爭期間，包括因阻止、對抗或防禦實際、即將發生或預期中的攻擊而採取的行動：
a)由任何政府或主權力量（合法或事實上的）或由維持或使用陸、海、空軍的任何機構發動；
b)或由陸軍、海軍或空軍發動；
c)或由上述政府、力量、機構或軍事力量的代理人發動；
本保單不承保因條款a.、b.或c.所述原因直接或間接造成的損失或損害，即使其他原因或事件同時或以其他順序對損失有所影響。」）Available at: Merck & Co., Inc., and International Indemnity, Ltd. v. ACE AMERICAN INSURANCE COMPANY, et al., No. UNN-L-002682-18 (Jan 13, 2022.)

的還有美國零食飲料跨國公司Mondelēz International, Inc.（下稱「億滋國際公司」），導致其遭受災難性的損失。這些損失不僅發生在美國境內，還波及其國際據點，包括位於澳大利亞塔斯馬尼亞霍巴特的Cadbury工廠。在億滋國際公司評估完成後，聯繫其財產全險保險公司（Zurich American Insurance Company），根據保單提出了1億美元的索賠，主張該保單「承保因惡意軟體代碼的惡意引入導致的電子數據、程序或軟件的實際損失或損害。」。

Zurich最終拒絕了理賠，援引其保單B(2)(a)敵對或戰爭行為除外條款，「在和平或戰爭期間的敵對或戰爭行為，包括以下任何一方為阻止、對抗或防禦實際、即將發生或預期的攻擊而採取的行動：(i)政府或主權權力（無論是合法的還是事實上的）；(ii)陸軍、海軍或空軍；或(iii)上述第(i)或第(ii)方的代理人或機構。」，聲稱NotPetya攻擊屬於該除外條款的適用範圍。另方面，億滋國際公司提出，該保單同時明確承保某些特定形式的針對電子和數據處理設備的「惡意網絡損害（Malicious Cyber-Loss Clause）」，因此，B(2)(a)除外條款與惡意網絡損害條款之間存在直接衝突，B(2)(a)除外條款因其措辭模糊，致原定排除的風險含糊不清而不應適用。因此，即便雙方後來協商過程進行中，保險公司曾提出金額相當於十分之一的理賠金額提案，億滋國際公司斷然拒絕，進而提起法律訴訟[9]。

四、雙方最終選擇和解以及對保險業的影響

儘管保險公司對默克案上訴法院的裁決再提出上訴，但該案件最終在送達紐澤西州最高法院獲得終局裁決前，雙方已於2024年1月達成和解，至於和解條件及相關細節則未對外揭露[10]。默克案為未來涉及資安保險索賠與戰爭除外條款的爭議樹立了重要的判例，成為相關領域的重要指引。

鑑於2022年1月，默克案自紐澤西州法院原審案件中作出支持被保險人的裁決，億滋國際公司的保險公司在同年11月選擇與億滋國際公司和解[11]。雖然該和解條款未對外公開，但從中可以推測，億滋國際公司的保險公司可能擔憂默克案上訴審判決結果，將進一步在司法實務鞏固對保險公司不利的法律見解，對其資安保險產品及相關除外條款的市場適用性造成重大影響。

此外，默克案判決後，保險業開始修改保

註9：Angad Chopra, *supra* note 5, p.143-146.

註10：Shelby Guilbert (2024), Merck-Settlement of $1.4 Billion Coverage Dispute Over NotPetya Cyberattack Places Renewed Spotlight on War Exclusions in 2024.
Available at:
https://www.propolicyholder.com/2024/01/merck-settlement-1-4-billion-coverage-dispute-notpetya-cyberattack-places-renewed-spotlight-war-exclusions-2024/ (last visited Dec. 24 2024)

註11：Lyle Adriano (2022), Zurich, Mondelez settle longstanding lawsuit over $100 million claim.
Available at:
https://www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx (last visited Dec.24 2024)

單條款，明確排除與國家支持的網絡行動相關的風險。例如倫敦勞合社（Lloyd's）在2022年8月16日發出的指導方針（即編號Y5381市場公告），要求所有單獨出單的資安險保單（standalone cyber-attack policies），必須排除國家支持的網絡攻擊所造成的損失，除非保單中明確涵蓋此類風險。此規範旨在減少因大型規模網絡攻擊事件所帶來的系統性風險，避免保險業承擔超出其承保能量的壓倒性損失，威脅其償還能力。保單條款需包含以下5點：

1.針對未包含戰爭排除條款之保單，排除戰爭造成的損失（無論是否宣戰）。
2.依據第3點，排除國家支持的網絡攻擊所引起的損失，若此攻擊嚴重削弱國家功能或安全能力。
3.明確規定承保範圍是否排除，在受攻擊影響國家之外遭受如同第2點所述影響的電腦系統。
4.提供明確的攻擊歸因（一國或多國）機制。
5.所有關鍵條款用語需明確定義。

而此指導方針自2023年3月31日起，對倫敦勞合社所有新簽或續保的保單開始生效。然而，此指導方針並不要求對於現行有效保單以附加條款方式進行修訂，除非該現行有效保單的到期日自2023年3月31日起超過12個月，對此，保險公司仍應及早因應[12]，否則將來進入訴訟爭議時，將礙難主張已明文排除於承保範圍之外[13]。

時至今日，網絡攻擊風險依然快速成長，對於風險管理需求越加重要，倫敦勞合社在2024年5月接續地針對資安險保單條款，提出處理國家支持網絡攻擊的相關要求，自2024年7月1日起，禁止任何新簽或續保業務使用不符合編號Y5381市場公告的保單條款，除非倫敦勞合社批准在特定期間內使用的特許權；自2025年1月1日起，倫敦勞合社聯合體不得在任何新簽或續保保單中，承保傳統戰爭中的國家支持網絡攻擊的條款，惟若有保險商品得以明確且獨立的承保條款來提供該保障，則不在此限[14]。

默克公司案的裁決對資安保險市場產生了重大的影響，迫使保險公司在制定保單時，

註12：CFC Underwriting, Cyber War Exclusion FAQs, Available at: https://www.biba.org.uk/wp-content/uploads/2022/07/CFC-Upgraded-war-exclusion-for-cyber-FAQs_A4.pdf (last visited Aug 22, 2025)

CFC Underwriting（是一間英國提供專業險的保險公司，在全球資安保險市場位居領導地位）針對資安險的戰爭除外條款已修訂更為清楚的定義，新定義除外條款保單的報價及保單條款自2023年5月1日當日起開始使用，並且該新修正定義條款不會立即使用在2023年5月1日以前已生效之保單，而是會在該保單日後續保時據以更新保單條款內容。

註13：Y5381 Market Bulletin (2022), State backed cyber-attack exclusions, Available at: https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf (last visited Jan 4 2025)

註14：Y5433 Market Bulletin (2024), State backed cyber attack wordings, Available at: https://assets.lloyds.com/media/6715b794-2ffd-40f7-b1c5-bcc02ca2e29b/Y5433%20-%20State%20backed%20cyber%20attack%20wordings.pdf (last visited Jan 4 2025)

在明確的除外條款和滿足企業需求的保障之間須謹慎平衡。此案進一步說明了，面對瞬息萬變的網絡威脅，保單條款必須具備高度的清晰性和前瞻性，承保範圍的清晰界定，得以確保提高企業即保單持有人對保單條款的理解程度，以因應未來的挑戰。

肆、分析：法律與保單影響

一、數位時代中戰爭除外條款的侷限性

默克案揭示了傳統戰爭除外條款在數位時代的顯著侷限性，這些條款原本是為傳統的物理戰爭而設計，常用如「入侵」（invasion）、「敵對行為」（hostilities）和「軍事行動」（military operations）等詞彙來描述國與國之間的武裝衝突。然而，紐澤西法院指出，在未明確更新條款的情況下，將這些條款適用於網絡攻擊並不合理，即使攻擊來自國家支持的行為者。這揭示了一項重要的法律漏洞：儘管網絡戰爭影響深遠，但它並不完全符合傳統法律對戰爭的定義。由於缺乏軍事部隊的參與和實體損害，將戰爭除外條款套用於網絡事件變得更加複雜。

在International Dairy Engineering Co. of Asia, Inc. v. American Home Assurance Company（1970）一案中，法院曾認為適用戰爭除外條款，因為原告的倉庫位於活躍戰區，並因一架身份不明的飛機投下的照明彈引發火災而焚毀。法院裁定，倉庫位於持續敵對和戰爭行動的地區，而照明彈是歸屬於作戰行動的一部分而投下的。然而，Universal Cable Prods., LLC v. Atlantic Specialty Ins. Co.（2019）一案中，第九巡迴上訴法院推翻了初審法院的判決。初審法院根據戰爭除外條款裁定被告保險公司勝訴，理由是原告因哈馬斯向以色列發射火箭而被迫遷移業務據點。但上訴法院認為該條款要求雙方應具有法律上或實質主權的主體，而哈馬斯不符合其中之一，因此不適用戰爭除外條款。至於Queens Ins. Co. v. Globe & Rutgers Fire Ins. Co.（1922）案，第二巡迴法院確認了初審法院的裁決，認為在戰爭期間兩艘船在海上相撞的損失應由海上保險承保，而非戰爭風險保險條款，法院指出，要讓保險公司在戰爭風險條款下承擔責任，所有形式的敵對或戰爭行動必須直接導致損失發生。由此三個案例表明，戰爭除外條款的適用需要明文表示個案中具體的情境，包括敵對或戰爭行動是否涉及軍事性質、主權實體，以及損失是否直接由戰爭或戰爭行動引起[15]。

此外，默克案的判決顯示法院傾向於狹義解釋保單中的除外條款，特別是在條款不夠明確時。該裁決促使保險公司在排除特定網絡風險時，需在保單中明確標示。學者指出，這可能推動保險業逐步採用「淺顯語言」（plain language），以確保被保險人能合理的理解其承保範圍的限制。

二、修訂保單與新除外條款

正如前述案例研究所示，自2022年起，倫

註15：Merck & Co., Inc., and International Indemnity, Ltd. v. Ace American Insurance Company, et al., 475 N.J. Super. 420, 293 A.3d 535 (App. Div. 2023)

敦勞合社分階段推行資安保單改革，明確要求市場成員在條款中排除國家支持的網絡攻擊，藉此降低承保範圍的不確定性並減緩系統性風險。此舉雖是對默克案裁決所揭示問題的直接回應，卻同時引發不同立場的關切與爭論：

- 對保險公司而言，新規範有助於減輕條款模糊帶來的大額理賠風險，提升風險管理的可預測性。
- 對被保險人而言，若攻擊歸因存在爭議或無法達到法律認定標準，則可能面臨「付出高額保費卻無法獲得保障」的處境。

因此，保險公司必須在維護自身風險控制與滿足被保險人保障需求之間取得更精準的平衡，並在條款設計上朝向「淺顯語言」（plain language）發展，以確保承保限制清晰易懂，降低爭議發生的可能性。

三、歸因問題與國家支持的網絡攻擊挑戰

資安保險中最複雜的議題之一是將攻擊歸因於特定行為者。在默克案中，NotPetya攻擊被廣泛認為是俄羅斯國家支持的駭客所為，儘管該攻擊的主要目標是烏克蘭。然而，在網絡戰爭中的歸因，並非總是直接且明確；此類攻擊經常透過中介組織發動，或被偽裝成犯罪行為。這引發了一個法律困境：若保險公司排除國家支持的攻擊，但歸因不明確時，該由誰承擔財務責任？

此外，歸因通常依賴於政府單位的情報，但這些情報往往缺乏透明性或結論性。保險公司和企業所依賴的證據，可能無法達到啟用戰爭除外條款所需的法律標準。這種不確定性對保險公司與被保險人都構成了重大風險，反映出建立標準化的網絡攻擊歸因機制以減少法律爭議的必要性。

四、法律判例與被保險人權益保護

默克案確立了一項重要的法律先例，強調在條款出現歧義時應作出有利於被保險人的解釋。這一原則與現有的contra proferentem principle一致，即當合約條款存在模糊時，解釋應不利於起草方。展望未來，保險公司需要撰寫更加明確的除外條款，以避免爭議並確保被保險人清楚了解其保障範圍。

此案也表明法院在處理保險與網絡風險交集時，正朝著更審慎的方向發展。裁決顯示，除非保單明確涵蓋相關情境，法院不太可能將傳統戰爭除外條款擴展至數位衝突。這進一步凸顯了保險公司需要調整保單，以反映當前的網絡威脅現實，同時確保對被保險人保持公平與透明的原則。

五、從傳統附加保險單（add-on policy）到單獨出單的資安保險（standalone cyber-insurance policy）

關於資安保險的爭議，在American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.一案中，美國法院認為，「在電腦技術主導我們專業與個人生活的時代，法院必須支持關於『物理損害』的更廣義定義，不僅限於對電腦電路的物理破壞或損害，還包括無法訪問、無法使用以及功能喪失。」，據此，網絡風險對被保險人或第三人財產造成損害，不僅是對有形財產的物理

損害，還包括無形資產的損失，例如因拒絕網絡攻擊導致的數據訪問中斷、系統無法使用，或網站功能喪失等情況，這些損失將造成重大損害，因此將無形資產的損失納入保險承保範圍，對於管理數位化環境中出現的新型損害有其必要。

隨著網絡攻擊變得更為複雜且潛在損害更大，問題集中在盜竊、公開（無論是錯誤還是蓄意）、以及濫用儲存於電腦網絡上的私人和機密電子記錄。例如，網絡安全漏洞（Cyber Security Breach）源自於駭客入侵零售商的網絡系統，竊取客戶的信用卡信息；未能妥善保護電子醫療資料，導致資料被公開在網站上。傳統保險可能無法涵蓋因數據洩露或網絡攻擊引起的損失，然而被保險人亟需尋求新的途徑以獲得保險賠償，此類爭議促使保險行業重新審視保單條款，並開發針對網絡風險的專屬保險產品，以滿足被保險人面對日益增長的數位化威脅時的需求。

近年來，勒索軟體攻擊數量急劇增加，成為資安保險訴訟爭議的關注議題。核心問題在於：政府協調的網絡攻擊是否屬於資安保單中的敵意或戰爭除外條款範疇。爭議涉及：(1)是否必須涉及傳統的軍事行動？(2)國家或政府支持的網絡攻擊是否等同於戰爭行為？(3)被保險人是否合理期待網絡攻擊應當屬於保單承保範圍，而不是用敵意或戰爭除外條款？

這些保險爭議案件顯示保險業進入資安保險爭議的全新階段，法院的最終裁決將對未來類似案件中戰爭除外條款的適用方式產生深遠影響，「沒有什麼比不利的法院判決更能促使保險公司修改其保單條款！」，除了推動保險行業對保單條款語言進行調整確有其必要，保險公司應該要提出專屬並且單獨出單的資安保單，提供符合被保險人保險保障需求的保險商品[16]。

伍、資安保險的未來

一、保單條款清晰化的必要性

默克案強調了保險保單條款清晰的重要性，特別是在網絡威脅不斷演變的情況下。保險公司需使用精確的語言來應對國家支持的網絡攻擊等複雜情境，確保被保險人充分理解其保障範圍的限制。倫敦勞合社的保單改革顯示，保險業正逐步朝向更明確的除外條款發展。然而，保險公司也必須在條款的清晰性與滿足全面保障需求之間取得平衡，若除外條款過於嚴苛，可能會降低企業購買資安保險的意願，不僅影響市場成長，還可能使企業面臨重大風險。

二、風險轉移與企業抗壓的平衡

隨著網絡風險日益複雜，保險作為風險管理工具的侷限性也逐漸顯現。雖然資安保險能提供財務損失的保障，但無法阻止網絡攻擊事件的發生，也無法保證企業的營運穩健性。因此，企業在購買保險的同時，還需投入資源於強化網絡安全、制定網絡攻擊事件

註16：Deborah L. Johnson, Demystifying the Elusive Quest for Cyber Insurance Protection: The Need for New Contract Language, 44 CARDOZO L. REV. 2361 (2023).

的應變計劃，並採取有效的風險管理策略。隨著網絡威脅不斷演變，企業必須採用整合性風險管理方法，將保險與主動的網絡安全防護措施相結合，才能更全面地應對此類型的風險。

此外，政府在彌補保險市場不足的方面也能發揮重要的作用。有專家建議，政府可參考恐怖主義保險的模式，建立公私合營的資安保險資金池，以應對規模巨大的災難性網絡事件。這類框架能縮小保險公司承保能力與不斷升級的網絡威脅之間的落差。

三、網絡戰爭保險新法律架構之探索

有別於傳統保險諸如財產全險保單（Property All-Risk Policy）以及商業綜合責任險（CGL），資安保險面臨更複雜的挑戰，與提供單一風險保障的保險（例如火險、車險等）不同，資安保險必須針對不同類型風險提供保障[17]，如數據洩露、網絡犯罪、勒索軟體等，亦即，資安保險為不同類型損失提供保障，從第一方營業中斷損失、網絡勒索損失、重置費用、硬體改善成本、應急處置費用，到被保險人過失（例如因技術錯誤與疏忽造成的損失）而造成第三方損失[18]，以及協力廠商責任險，即網絡安全事件發生後被保險人對協力廠商應承擔的侵權損害賠償責任的保險，承保包括資料洩露責任、網絡安全事件責任、產品責任或技術服務專業責任等。因此，從保險技術而論，特別是歷史數據資料，以及相關精算模型的採用，資安保險本身都有一定的困難度。

默克案突顯了在網絡戰爭與保險交集領域中建立新法律架構的必要性。雖然「塔林手冊」（Tallinn Manual）等國際法律文件對國家在網絡空間中的行為提供了一些指引，但在商業保險範疇之內，針對如何分類和因應國家支持的網絡攻擊，國際間仍然未達成共識。未來的重點應放在制定標準化的指導方針，以規範保單中的網絡戰爭條款，為保險公司、企業和法院提供更明確的參考依據[19]。

陸、結論

默克案在不斷演變的資安保險領域中樹立了重要的法律判例，揭示了傳統「戰爭除外條款」在應對國家支持的網絡攻擊時的侷限性。紐澤西法院裁定，除非條款明確更新以涵蓋網絡行動，否則針對戰爭行為的除外條款不適用於缺乏直接軍事參與的數位事件。此裁決促使保險業採用更清晰且具體的保單

註17：金融監督管理委員會保險局（2024），前揭註1，「目前市售資安保險商品，除針對大型企業資安需求之客製化商品外，亦有提供中小型企業投保之資安保險商品，包括(1)資訊系統不法行為保險，主要承保被保險人因第三人不法入侵電腦系統，所致資金或其他財產的損失；(2)資料保護責任保險，保障因個資外洩所生對第三人依法應負之賠償責任；及(3)資訊安全綜合保險，保障範圍包括被保險人受網絡攻擊、電腦勒索或管理錯誤行為等所致財產損失，以及對第三人依法應負之賠償責任等。」

註18：何啟豪，前揭註7，第133、137頁。

註19：Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. (2017). NATO Cooperative Cyber Defence Centre of Excellence.

語言，如倫敦勞合社推動的保單改革。

然而，保險業朝向明確排除國家支持網絡攻擊的趨勢，為保險公司和企業帶來了新的挑戰。企業可能面臨無法獲得充分保障的困境，尤其在歸因網絡攻擊於國家行為者時，因其複雜性與不確定性，使情況更為棘手。為了有效管理這些風險，企業不僅需依賴保險，還必須投入資源於提升網絡安全韌性。同時，政府與企業利害關係人也必須攜手合作，建立框架以填補保險市場未涵蓋的風險缺口[20]。

默克案凸顯了在保險與網絡戰爭交集上建立新法律架構的必要性。清晰的保單語言、平衡的風險管理策略，以及國際間的合作，將是保險公司與被保險人應對國家支持網絡攻擊風險的關鍵。隨著數位衝突日益頻繁且愈發複雜，自默克案的經驗汲取教訓，將為未來的法律糾紛和保單改革提供方向，推動資安保險的持續發展。

（投稿日期：2025年4月1日）

註20：Marsh McLennan. (2024). Cyber Protection Gap: Call for Public-Private Collaboration to Bridge Insurance Shortfalls. Available at: https://www.marshmclennan.com/insights/publications/2024/september/closing-the-cyber-protection-gap.html (last visited Mar 20 2025)