地緣政治緊張局勢和網路威脅：美國關稅的潛在影響

2025年6月

指數研究負責人Ilaria Sangalli

在不確定性中游走：美國關稅對全球貿易和網路安全的影響

4月2日，美國宣布對其最大的貿易夥伴徵收關稅。

加徵關稅意味著貿易戰可能升級，尤其是與中國、加拿大和墨西哥等國家之間的矛盾可能更趨白熱化。這一發展態勢令投資人擔憂各國可能採取反制措施，可能因而進一步妨礙全球貿易和經濟增長。此外，貿易緊張局勢也可能引發國家級駭客組織採取報復措施，包括網路間諜和網路攻擊。這些威脅或者會危及政府和不同的私營機構。

除網路風險增加的問題外，由於供應鏈可能也需應對新設的貿易壁壘，因此各大企業未來還會面臨成本上漲和物流運輸困難等難題。

4月9日宣布的90天暫停措施、5月8日與英國的貿易協議和5月12日與中國的臨時協議等消息令市場反彈。然而，儘管近期達成多項貿易協議並暫停徵收關稅，很多公司仍然面臨重大的不確定性。而且基於這些措施全屬暫時性，要完全了解其影響仍言之尚早。企業繼續對大幅調整供應鏈抱持審慎態度，傾向等待出現更穩定和可預測的局面方會採取行動。調整供應鏈的複雜性，以及調整可能導致出現新的網路安全漏洞，都令企業的取態加倍審慎。

借助地緣政治緊張局勢和關稅糾紛 發動含有政治目的之網路攻擊次數不斷遞增

在當前地緣政治緊張局勢不斷升級和網路威脅日益繁複精密的情勢下，全球各國都面臨前所未有的安全挑戰。據歐洲刑警組織[1]最新的報告披露，受到國家資助且採用混合式攻擊的駭客組織透過與犯罪團夥結成「影子聯盟」，對歐盟的攻擊次數持續增加，引發市場憂慮。這些駭客組織採用了一系列手法破壞網路安全，例如網路攻擊、竊取數據、製造假消息和破壞關鍵基礎設施等。歐洲刑警組織表示，目前的地緣政治環境為這些駭客組織提供了利用網路漏洞來散布假消息的機會。

儘管該報告並未明確將俄羅斯列為採用混合式攻擊的駭客組織，但當中暗示該地區的活動與混合式攻擊的手法同出一轍：「俄羅斯及其勢力範圍內的國家對關鍵基礎設施和公共機構發起含有政治目的之網路攻擊次數有所增加」。[2,3]

1 歐洲聯盟執法合作署，是歐盟的執法機構。歐洲刑警組織的使命是支援歐盟成員國防止和打擊嚴重的國際和有組織犯罪、網路犯罪和恐怖主義。

2 https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

3 波蘭副國務卿表示，一個國家級駭客組織最近對其國內一家醫院發動網絡攻擊，導致醫療服務中斷數小時。立陶宛當局指控俄羅斯軍事情報局(GRU)去年夏天發動縱火襲擊，焚燒維爾紐斯的宜家家居商場。
https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol#%3A~%3Atext%3DThe%20Europol%20report%20also%20warns%2Cout%20hacking%20and%20cyber%2Dattacks

因應上述情況，歐盟執委會計劃加強安全協議，抵禦各種精密的網路攻擊，並有意為歐洲刑警組織增加一倍的人手和經費。此策略措施有望增加公私營機構的網路安全支出，並將會帶動對網路安全產品、服務和進階威脅偵測解決方案的需求。

微軟在其《2024年數位防禦報告》中指出，與地緣政治緊張局勢密切相關的網路攻擊活動增加是近年的大勢所趨。根據該報告，網路犯罪團夥正與國家級駭客組織合作，互相交流各種工具和技術以達成攻擊目標。這種合作關係已造成全球多起重大網路攻擊事件，當中除涉及來自俄羅斯的駭客外，中國、伊朗和北韓也有參與其中。

微軟還發現，在最近一屆美國總統大選之前，與選舉相關的同音字網域陡增，都是與官方網站極其相似、用以欺騙用戶的欺詐連結。這些網域被用於傳播可竊取資訊或破壞系統的網路釣魚攻擊和惡意軟體。微軟表示，謀取利益的網路犯罪分子和懷有政治目的之國家級駭客組織是這些網域背後的共同推手。[4]

鑒於近期緊張的關稅風波，尤其是中美之間的關稅戰，預期網路攻擊風險將會增加。貿易戰、制裁或關稅等經濟摩擦會令網路衝突升級，使各大機構面臨更大的安全風險。觀乎之前2018年爆發的中美貿易戰，網路間諜活動因中國由國家資助的駭客組織而激增。[5]此外，貿易戰可能激發網路行動主義，激起擁護民族主義的駭客對其假想敵發動獨立攻擊。

由國家資助的混合式攻擊增加和當前的地緣政治緊張局勢，正正突顯了強大的網路安全措施有著無可取代的重要性。近期的關稅糾紛可能導致網路風險上升，也令市場進一步重視提高防範警覺和積極採取網路安全措施的必要性。

全球供應鏈的網路安全隱患

近期的美國關稅大大增加了全球企業所面對的不確定性。這些關稅可能會對未來業務營運構成重大挑戰，逼使企業對供應鏈戰略進行重大調整。任何調整都可能對企業和其全球供應鏈的網路穩健性帶來深遠的影響。必須注意的是，截至目前，由於這些關稅未來如何演變和其影響尚有種種未知之數，故而尚未能預測這些措施造成的全面影響。

調整供應鏈結構的過程漫長而複雜，企業必須仔細評估新供應商、重新磋商合同和重新配置物流網路。在這過渡期間更可能會出現各種漏洞，如果新合作夥伴的安全標準參差不齊，或是整合系統時未有進行徹底測試更是如此。這可能會帶來新的安全漏洞，令駭客有機可乘，進一步增加受到網路攻擊的風險。

最新研究結果同樣強調防堵這些漏洞的重要性。世界經濟論壇「2025年全球網路安全展望」調查顯示，54%的大型機構認為供應鏈挑戰是維持網路穩健性的最大阻礙。在現今社會中，供應鏈更加複雜，而且更為依賴全球互聯和技術，令這些系統的漏洞愈發明顯。[6]

現今的供應鏈涉及眾多利益相關者，包括供應商、製造商、經銷商和零售商，分別在不同的國家和地區通力合作。諸如不安全連結這類的單一漏洞，都可能對整個網路生態系統造成多重影響。網路犯罪分子可以藉由針對第三方廠商，或如軟體廠商、開源軟體、雲端服務和硬體供應商等服務供應商進而入侵大量公司。2024年11月就曾經發生過此類事件，供應鏈管理軟體供應商 Blue Yonder遭受勒索軟體攻擊，並因此波及其眾多客戶，包括英國星巴克、連鎖超市 Morrisons 和 Sainsbury's。這次攻擊導致系統中斷，逼使這些企業轉用人手流程和啟動應急方案。截至2025年1月止的季度內，Morrison的銷售額增長從上一季度的4.9%下跌至2.1%，其將跌幅部分歸咎於系統中斷影響了公司在聖誕節期間維持最佳庫存水平的能力。

SolarWinds網路攻擊事件依然是史上最嚴重的網路攻擊事件之一。[7]2020年12月，駭客入侵SolarWinds的軟體更新系統，並經由更新檔向SolarWinds的客戶散布惡意軟體，令其成功入侵包括美國政府部門和大型企業等多個組織單位的系統。這次入

4 https://blogs.microsoft.com/on-the-issues/2024/10/15/escalating-cyber-threats-demand-stronger-global-defense-and-cooperation/

5 https://www.secureworld.io/industry-news/trade-wars-us-tariffs-cyber-risk

6 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

7 一家提供IT管理軟體的公司

侵事件震驚全球，突顯出供應鏈安全漏洞和此類攻擊造成的潛在廣泛影響。自SolarWinds入侵事件以來，網路犯罪分子持續以供應鏈組織為攻擊目標，且攻擊愈加猖獗。透過攻擊單一供應商，攻擊者有可能進而入侵多個組織單位，並因此透過供應鏈攻擊賺取暴利，牽連甚廣。

隨著網路犯罪分子更頻繁地以供應鏈環節為攻擊目標，企業不單必須加強其內部網路安全措施，還須嚴格評估並加強其供應商的安全實務，考慮到近期實施的關稅以及對供應鏈中斷的潛在長期影響，這一點尤為重要。在今時今日的全球化社會中，要維持網路穩健性，就必須全面地防堵整個供應鏈網路生態系統的漏洞。

資料來源：納斯達克指數研究、彭博、FactSet。