大公報
2026年4月16日 星期四

伊朗遇襲時 美製通信設備突集體癱瘓

產品疑暗藏「後門」依賴美國裝置存國安風險

加強防範

伊朗媒體14日報道，伊朗中部伊斯法罕省遭遇美國空襲期間，境內大量美國製造的通信設備突然失靈，操作系統崩潰，涉及思科、飛塔、朱尼珀等品牌。分析指，故障發生時伊朗境內並沒有國際互聯網接入，時機十分「可疑」，且設備存在「深層破壞」跡象，懷疑美國產品裏面藏有「後門」。伊朗媒體評論稱，該事件表明網絡安全依賴外國設備所帶來的國家安全風險。

大公報記者 郭嘉 綜合報道

伊朗法爾斯通訊社「科學與進步」欄目14日報道說，伊斯法罕省遇襲期間，伊朗境內通信基礎設施發生「詭異而驚悚」的事件。

現場監測顯示，大量思科（Cisco）、飛塔(Fortinet)和朱尼珀(Juniper Networks)等品牌的產品，以及基於拉脫維亞網絡設備公司MikroTik操作系統的設備，突然同步離線，操作系統集體「崩潰」。

報道並未具體說明是哪一次襲擊，但報道附帶了一張美軍飛機殘骸的照片。本月初，美軍一架F-15戰機在伊朗境內被擊落，兩名飛行員彈射逃生，墜機地點發生在伊斯法罕南部的三省交界區域。美方隨後派出飛機和特種兵進入當地展開營救。

斷網狀態下 系統仍集體崩潰

據悉，涉事設備發生故障的時間，與伊斯法罕省遭遇美軍空襲的時間窗口完全重合，時機非常「可疑」。更關鍵的是，這些設備失靈、系統集體崩潰時，伊朗當時無法訪問國際互聯網，基本排除了「境外網絡攻擊」的可能性。這表明設備內部存在「深層蓄意破壞」跡象。

知情人士透露，伊朗網絡實驗室將在不久後公布更多技術資料和證據，證明涉事設備製造商與美國和以色列政府存在直接或間接的「勾結」。

報道援引網絡安全專家分析認為，此次設備「失靈」可能源自四種精心策劃的惡意攻擊：一是隱藏訪問：相關產品中包含即使沒有互聯網連接也能激活的「後門」，能夠破壞設備；二是惡意數據包：從網絡內部發送特殊數據，致使系統瞬間癱瘓；三是潛伏式「殭屍網絡」：潛伏多年的惡意軟件，在特定事件發生時被激活；四是生產鏈污染：硬件和軟件在進入該國前已被篡改，即使更換操作系統也無法解決問題。

美震網病毒破壞伊核計劃

伊朗的設備並非第一次遭遇美國的「黑手」。2010年，伊朗納坦茲核設施電腦網絡遭遇名為「震網」的超級蠕蟲病毒攻擊，1000台鈾濃縮離心機癱瘓。美媒後來披露，這種網絡病毒由美國和以色列開發，專門用於破壞伊朗核計劃。

法爾斯通訊社評論稱，最新事件表明，「一個國家的網絡安全支柱絕不能依賴外國設備」，「這些大牌廠商表面提供技術服務，可一到危機時刻，就會變成基礎設施的戰略短板和致命軟肋。」報道指出，真正的安全始於自主擁有和生產本土技術，發展國產設備不再是一句口號，而是在網絡戰中生存的必要條件。

伊朗過去在通信設備等領域對西方產品存在一定依賴性。該國三大電信運營商的核心網絡中，諾基亞、愛立信、西門子設備一度佔比超80%。全國骨幹網交換機與基站普遍採用歐美標準，維護權限甚至長期由歐洲承包商掌控。另一方面，受美國長期制裁影響，美國公司無法直接合法向伊朗出售產品，流入伊朗市場的設備多經複雜第三方渠道，其供應鏈存在被篡改或漏洞利用的風險。伊朗方面近年已明確呼籲發展「國產設備」以提升自主性。

作為主要的路由設備生廠商，思科、飛塔和朱尼珀等設備在全球廣泛使用，但安全漏洞不斷。近年來，思科設備頻繁被曝出多個高危漏洞，飛塔的核心產品FortiOS及防火牆同樣屢現嚴重漏洞，引發大規模勒索軟件攻擊與數據洩露。朱尼珀設備則早在2015年就曝出過重大的「後門」事件。

◀伊朗伊斯法罕一處工業區3月14日遭空襲，現場升起滾滾濃煙。 法新社

伊朗網絡安全專家分析認為，該國的通信網絡此次可能遭受四種惡意攻擊。

- 隱藏訪問（後門）：設備內置毋須連接互聯網亦能激活的「後門」，在關鍵時刻遠程觸發，破壞設備。
- 惡意數據包：從網絡內部發送特殊數據，致使系統瞬間癱瘓。
- 潛伏式「殭屍網絡」：預先植入惡意軟件，長期潛伏，在特定事件被激活。
- 供應鏈污染：硬件或軟件在進入伊朗前就被篡改，即使重裝系統也無法解決。

◀德黑蘭遭襲擊期間，民眾從辦公樓內搬出電腦設備。 法新社

來源：伊朗法爾斯通訊社

大公報AI製圖

美國設備安裝「後門」黑歷史

Clipper芯片

預留後門解碼：

1993年，美國政府就在AT&T商用電話加密設備中強制加入Clipper芯片，使用美國國家安全局（NSA）的加密技術，當中預留「後門」，以便官方日後解碼通信。

思科（Cisco）

「棱鏡計劃」核心角色：

「棱鏡門」事件爆料人斯諾登披露，NSA曾利用一款名爲「JETPLOW」的惡意軟件，針對思科PIX、ASA系列防火牆植入後門，用於監控他國網絡。

物流攔截植入「後門」：德國《明鏡週刊》2014年報道，NSA會在監控目標訂購的思科、三星、戴爾等產品運輸途中，截獲貨物並轉運到秘密工廠，在硬件上安裝後門或間諜軟件，再重新發貨。

英偉達（NVIDIA）

芯片定位、遠程關閉：

去年7月，英偉達H20算力芯片被爆疑似存在「追蹤定位、遠程關閉」後門，中國國家互聯網信息辦公室爲此約談英偉達。英偉達否認芯片存在「後門」。

英特爾（Intel）

管理引擎(ME)「後門」爭議：

英特爾公司被揭發自主運行子系統ME（管理引擎）暗藏「後門」，自2008年起被嵌入幾乎所有英特爾CPU中，允許系統管理員遠程執行任務。

大公報整理

美國思科留「後門」劣跡斑斑

不可信賴

作為美國政府和軍方的通信設備和網絡技術設備主力供應商，美國大型通訊路由設備製造商思科（Cisco）屢次被揭發存在安全性漏洞，導致系統容易被操控、數據洩漏，在產品留「後門」方面可謂是劣跡斑斑。

2013年，前美國中央情報局技術分析師斯諾登向外界踢爆美國政府「棱鏡」大規模監控計劃時，就揭露了美國國家安全局（NSA）會在思科的設備中植入「後門」。負責撰寫「棱鏡門」報道的前英國《衛報》記者格林沃爾德2014年在其著作《無處可藏》揭露，NSA下屬的秘密行動小組（TAO）會在產品運輸途中攔截設備，被轉運至一個秘密地點以插入間諜軟件，然後再將設備送往目的地。

思科方面多次公開否認參與這項項目，並一再強調思科產品的安全性。不過，此後思科卻一再被發現留「後門」。2014年，思科針對小型企業的路由器中發現了一個新的無證「後門」，允許攻擊者訪問用戶權限。2017年，在維基解密洩漏數據的背景下，思科在自己的路由器中發現了一個漏洞，這使得中央情報局可以通過一個硬件漏洞遠端控制300多個思科交換機模型。2019年，思科路由器又被發現存在五個「後門」，其中一個名為「cisco」的硬編碼賬戶被曝光，其後門允許攻擊者遠程訪問超過850萬台思科路由器和交換機。

2019年，德國《每日鏡報》曾報道，經過多年審查，英國、德國及歐盟等發現美國思科設備經常能發現安全漏洞，從2013年到2019年，已發現了10起「後門」事件。

▲思科位於美國加州聖何塞的總部大樓。 法新社

馬斯克切斷「星鏈」重創俄軍通信

關鍵作用

【大公報訊】綜合報道：世界首富馬斯克旗下太空探索公司（SpaceX）研發的「星鏈」（Starlink）裝置，是俄烏雙方在戰場通信和作戰的關鍵設施。今年2月，烏克蘭聯合SpaceX封鎖了俄軍通過非官方渠道獲得的「星鏈」終端，使得俄軍的「星鏈」網絡完全失效，一度制約了俄軍的作戰能力，同時為烏軍創造了反擊機會。

從2022年俄烏衝突開始，基輔方面高度依賴數以萬計的「星鏈」衛星型網絡連線，用於前線通信、指揮協調，以及部分無人機任務的操控。俄軍無線電信號常被監聽，位置容易暴露遭受襲擊，因此俄軍也陸續通過第三方渠道引入「星鏈」終端設備，加強內部通信，並將其整合至俄軍的無人機操作系統中。

SpaceX對於俄軍使用「星鏈」，過去並未採取實質性的限制措施。今年2月初，烏克蘭軍方表示已要求SpaceX提供協助，一起阻止俄軍借助「星鏈」為無人機導航。馬斯克決定關閉俄軍在烏克蘭境內使用「星鏈」權限，對烏克蘭境內的「星鏈」終端機進行「白名單」驗證制度：只有經過烏克蘭政府登記並驗證的終端機才能獲得信號，讓俄軍手中設備瞬間淪為磚頭。

「星鏈」通信中斷一度讓俄軍措手不及。據稱，在俄軍「星鏈」服務被關閉後的幾天裏，烏克蘭在該國東南部收復了約77平方英里的土地。

不過，專家表示，臨時斷網措施一度成功阻緩了俄軍的推進勢頭，並不代表前線局勢會發生根本性轉變。分析師表示，俄軍已迅速尋找替代方案，包括重新啟用無線電通信。

▲俄烏戰爭期間，一名烏克蘭軍人正在操作「星鏈」系統。 法新社