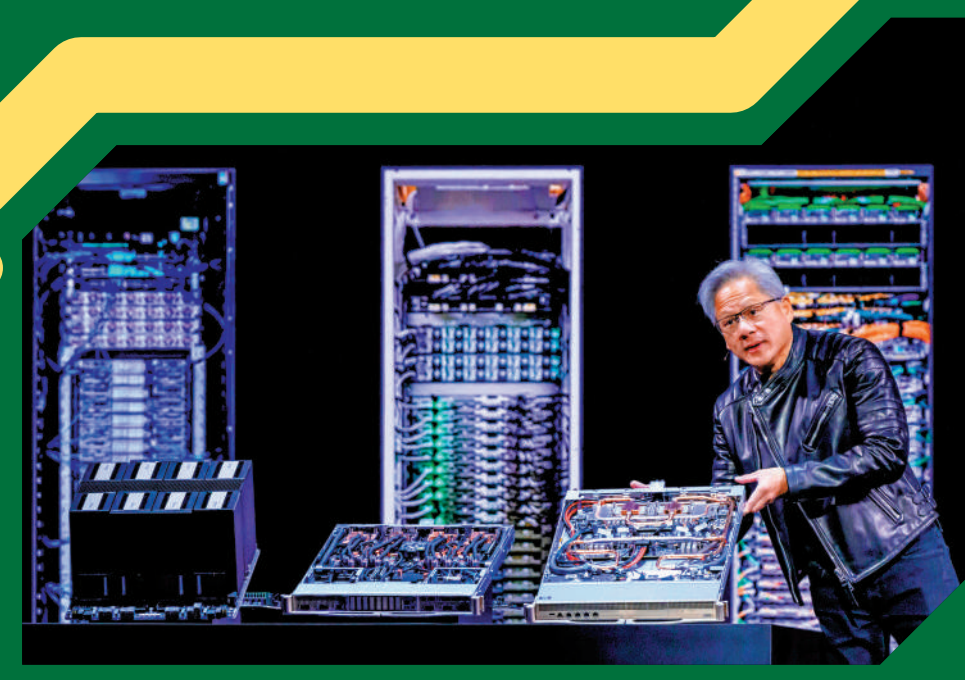
大公報
2025年8月11日 星期一

追蹤定位 遠程操縱 竊取數據

美國芯片暗藏「後門」安全隱患防不勝防

眞相揭秘

美國芯片公司英偉達的H20芯片存在「後門」安全風險，該公司日前被中國國家互聯網信息辦公室約談，令芯片安全問題再成爲焦點。專家表示，「後門」主要分爲硬件和軟件兩種，可實現追蹤定位、遠程關閉等功能，而英偉達具備相應的「後門」技術。另外，美國政府在科技產品留「後門」方面可謂劣跡斑斑。芯片作爲電腦系統的「神經中樞」，如果「帶病」上崗，其風險漏洞一旦觸發，所帶來的影響將是災難性的。



◀英偉達行政總裁黃仁勳在美國加州展示該公司新產品。 法新社

【大公報訊】今年5月，美國聯邦眾議員比爾・福斯特牽頭提出《芯片安全法案》，要求美國商務部強制美國芯片商在受出口管制的芯片中加入「後門」，以實現追蹤定位、遠程關閉和數據回傳等功能。「後門」指一種繞過標準安全措施、獲取對程序或系統訪問權的隱藏機制，主要分為硬件和軟件兩種。硬件「後門」是在芯片設計或製造環節留下的物理裝置，軟件「後門」則是在軟件中植入具有「後門」功能的指令。

有分析認為，上述法案本質上將芯片視為一種「數字武器」，攻擊者可能利用「後門」奪取系統控制權、竊取數據、實施遠程監控或干擾關鍵基礎設施運作。本月6日，英偉達發表聲明稱，該公司的芯片不存在「後門」，不會讓任何人有遠程訪問或控制這些芯片的途徑。但外界評論指出，僅憑一份聲明並不能平息質疑。

H20不安全 不先進 不環保

H20芯片是英偉達專門面向中國市場推出的「特供」芯片，其主要應用場景集中在AI計算和數據中心市場，涉及大量敏感數據，其安全問題顯得尤為重要。

單從硬件「後門」角度考慮，H20芯片完全可以實現「遠程關閉」等功能。只要在H20芯片的電源管理模塊中植入「遠程關閉」電路，並設定相應的觸發機制，就能在不依靠外部條件的情況下執行直接切斷芯片核心電源、將電壓調整至不穩定區域導致芯片功能異常等操作。另一種加入硬件「後門」的手段是修改固件引導程序。當芯片啟動時，引導程序會檢查地理位置信息、授權狀態等特定條件，如果條件不滿足，就可以拒絕啟動、禁用部分高級功能或限制芯片性能。

奇安信威脅情報中心安全專家表示，在生產階段加入硬件「後門」較容易實現，但成本也比較高，通過軟件或軟硬件配合的方式加入「後門」更靈活。英偉達開發的統一計算設備架構（CUDA），被視為利用軟件激活「後門」的重要抓手。CUDA是一種生態系統，覆蓋全球90%的AI研究機構，全球400萬開發者正在使用CUDA。想要使用CUDA的最新功能，就需要把更新的軟件導入其中，在此環節中，芯片所在的系統就可能被加入「後門」指令。這種「後門」可以實現追蹤定位、文件收集、屏幕截取等功能。

有分析稱，由此可見，H20對於中國來說算不上是一款安全的芯片。除了不安全，H20也不先進、不環保。相較於標準版H100芯片，H20的整體算力只有約20%；其GPU核心的數量比H100少41%，性能降低28%，這也導致H20無法滿足萬億級大模型訓練需求。對於採用14nm以下工藝的服務器GPU，節能水平的能效比需達到0.5 TFLOPS/W，H20也達不到這個水平。

構建自主可控技術體系

過去，美國在科技產品留「後門」方面可謂是劣跡斑斑。美國曾設計過「片上治理機制」，主張由美國政府成立相關部門，協調芯片設計、生產、製造的各個環節，包括協調企業和盟友，以實現對AI芯片的控制。該機制可實現許可鎖定、追蹤定位、使用監測、使用限制等功能。一份詳細介紹該機制的報告提到，英偉達的AI芯片其實已廣泛部署了上述大部分功能，只不過有些尚未激活。報告還提到，即便芯片還沒有這些功能，美國也可以「協調」盟友，通過產業鏈為芯片加入硬件「後門」。

中國科學院信息工程研究所研究員李鳳華表示，防範「後門」風險，中方可通過法律約束、技術突破和構建自主可控的芯片技術體系，同時建立進口芯片安全風險評測審查機制，依法對相關廠商進行追責和處罰。（綜合報道）

H20芯片深陷風波

專門面向中國市場

- **H20是英偉達專門面向中國市場推出的「特供」芯片，主要應用場景集中在人工智能（AI）計算和數據中心市場，涉及大量敏感數據。**

美政府突然「解禁」

- **今年4月，美國政府將H20芯片也納入出口管制。5月，美國聯邦眾議員比爾・福斯特牽頭提出《芯片安全法案》，要求美國商務部強制美國芯片商在受出口管制的芯片中加入「後門」，以實現追蹤定位、遠程關閉和數據回傳等功能。7月，美國批准對中國出售H20芯片。8月6日，英偉達行政總裁黃仁勳前往白宮與美國總統特朗普會面。隨後，美國商務部開始爲H20芯片發放許可證。**

存在嚴重安全風險

- **美國AI領域專家透露，英偉達算力芯片「追蹤定位」和「遠程關閉」等技術已成熟。如果H20芯片存在「後門」，攻擊者可能利用該「後門」竊取AI模型參數和訓練數據、破壞訓練結果的完整性，甚至進行遠程操控，導致系統級安全失控。**
- **有分析指出，英偉達可以通過在H20芯片的電源管理模塊中植入「遠程關閉」電路、修改芯片的固件引導程序等手段加入硬件「後門」，或通過統計計算設備架構（CUDA）生態系統加入軟件「後門」。**

大公報整理

芯片後門Q&A

「後門」是什麼?

- **「後門」指一種繞過標準安全措施、獲取對程序或系統訪問權的隱藏機制，主要分爲硬件和軟件兩種。硬件「後門」是在芯片設計或製造環節留下的物理裝置，例如具有「後門」功能的邏輯電路。軟件「後門」可以理解爲在軟件中植入具有「後門」功能的指令，通過運行軟件來影響用戶的系統。**

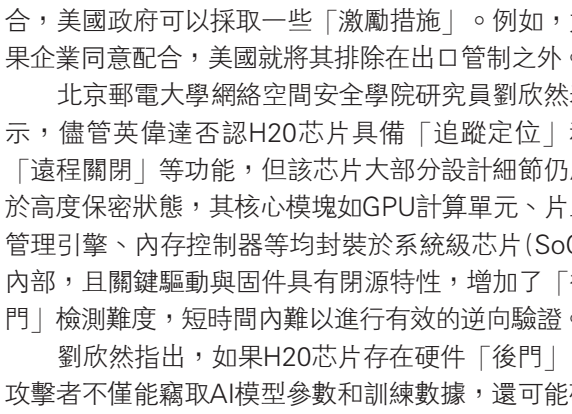
有什麼影響?

- **「後門」構成嚴重的安全威脅，可被用於追蹤定位、遠程關閉或奪取系統控制權、竊取敏感資料、干擾設備運作等。**

如何應對?

- **我國可以通過法律約束、技術突破和生態建設「三位一體」構建自主可控的芯片根技術體系，同時建立健全進口芯片安全風險評測和審查機制，重點檢測芯片後門、固件漏洞和隱蔽信道等技術風險，並依據相關法律對存在安全漏洞和隱蔽後門的芯片廠商進行追責和處罰。**

大公報整理



▲英偉達在中國市場銷售的芯片存在安全風險。 中新社

▲斯諾登揭露，美國政府從未放棄安插「後門」。 資料圖片

「Clipper芯片」被抵制 美政府仍不悔改

前科纍纍

美國政府和企業在留「後門」方面可謂前科纍纍。英偉達在6日的自辯聲明中提到「Clipper芯片」事件，並聲稱這是不應該留「後門」的歷史教訓。然而，美國中央情報局（CIA）前僱員、「棱鏡門」吹哨人斯諾登揭露，美國國家安全局（NSA）在「Clipper芯片」事件之後從未放棄安插「後門」，只是改爲秘密行事。

1992年，美國電話電報公司（AT&T）面向商務人士推出一款設備，可對電話語音傳輸進行加密，確保信息安全。這引起美國政府不滿，當局要求AT&T在設備中加入「Clipper芯片」。該芯片採用NSA的加密算法，包含一個「後門」，讓美國政府得以「解碼」設備上的信息。這個項目受到各方抵制，不到三年就宣告終止。

斯諾登爆料稱，NSA於2000年啟動新的項目，並開始與美國內外的科企合作，在這些公司的產品中加入「後門」。一些公司稱，它們受到美國政府脅迫，不得不交出主密鑰。在一個案例中，NSA曾在運輸途中攔截思科系統的通信設備並安插「後門」。

英特爾公司開發的自主運行子系統ME（管理引擎）也暗藏「後門」。ME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。硬件安全專家指出，ME就是一個「後門」，可以在操作系統用戶不知情的情況下完全訪問存儲器，繞過防火牆發送和接收數據包。2017年，兩名俄羅斯安全專家還通過逆向技術找到了疑似NSA設置的隱藏開關。

▶黃仁勳（右）與特朗普關係密切。 路透社

黃仁勳訪白宮 特朗普放行H20

令人生疑

H20是英偉達為了應對美國拜登政府的出口管制要求，專門面向中國市場推出的「特供」芯片，主要應用場景集中在人工智能（AI）計算和數據中心市場。今年4月，特朗普政府以「國家安全」為由，將H20芯片納入出口管制，但7月又改口允許對中國出售該款芯片。

英媒披露，英偉達行政總裁（CEO）黃仁勳7月前往白宮對美國總統特朗普進行游說後，特朗普撤銷針對H20芯片的禁令，但並未立即開始發放許可證。本月6日，黃仁勳再次前往白宮與特朗普會面。隨後，美國商務部開始發放許可證。值得注意的是，一份介紹「片上治理機制」的報告中提到，為在安插「後門」方面得到芯片商的配合，美國政府可以採取一些「激勵措施」。例如，如果企業同意配合，美國就將其排除在出口管制之外。

北京郵電大學網絡空間安全學院研究員劉欣然表示，儘管英偉達否認H20芯片具備「追蹤定位」和「遠程關閉」等功能，但該芯片大部分設計細節仍處於高度保密狀態，其核心模塊如GPU計算單元、片上管理引擎、內存控制器等均封裝於系統級芯片（SoC）內部，且關鍵驅動與固件具有閉源特性，增加了「後門」檢測難度，短時間內難以進行有效的逆向驗證。

劉欣然指出，如果H20芯片存在硬件「後門」，攻擊者不僅能竊取AI模型參數和訓練數據，還可能破壞訓練結果的完整性，甚至遠程操控任務流程，導致系統級安全失控，這對國家信息安全構成極大威脅。