大公報
2025年4月16日 星期三

涉亞冬會網攻 內地通緝美國三特工

哈爾濱公安局：嫌犯隸屬NSA 兩所美國高校涉案

2025年是《中華人民共和國國家安全法》頒布施行十周年，4月15日是第十個全民國家安全教育日。10年來，我國發展環境發生深刻複雜變化，應對網絡安全、信息安全等非傳統安全威脅的能力不斷提升。

4月15日，一張特殊的懸賞通緝令引發關注，其緣由是「2025年哈爾濱第九屆亞冬會」（以下簡稱：亞冬會）遭受境外網絡攻擊事件。為依法嚴厲打擊境外勢力對我網絡攻擊竊密犯罪，切實維護國家網絡空間安全和人民生命財產安全，哈爾濱市公安局決定對3名隸屬於美國國家安全局（NSA）的犯罪嫌疑人進行懸賞通緝。調查顯示，兩所美國高校也涉嫌參與網攻。

專家：目標意圖明顯 美國動用數百類已知和未知手法施襲

【大公報訊】綜合央視新聞、人民郵電報、國際在線報道：前期，亞冬會受境外網絡攻擊事件引發廣泛關注。調查發現，3名特工曾多次對我國信息基礎設施實施網絡攻擊，具有NSA背景的美國加利福尼亞大學、弗吉尼亞理工大學也參與了本次網攻。

此次針對亞冬會開展的網絡攻擊是由美國國家安全局精心組織實施的一次網絡攻擊行動，實施此次網絡攻擊行動的組織是美國國家安全局信息情報部（代號S）數據偵察局（代號S3）下屬特定入侵行動辦公室（Office of Tailored Access Operation，簡稱「TAO」，代號S32）。美國國家安全局特定入侵行動辦公室為了掩護其攻擊來源，依託所屬多家掩護機構購買了一批不同國家的IP地址。

亞冬會遭到27萬次境外網攻

中國國家計算機病毒應急處理中心和計算機病毒防治技術國家工程實驗室的監測報告顯示，2025年1月26日至2月14日期間，亞冬會賽事信息系統遭到來自境外的網絡攻擊270167次，包括賽事信息發布系統、抵離管理系統和收費卡系統等，上述系統對於賽事的重要信息發布、人員和物資調配、賽事的組織管理起到至關重要的作用；黑龍江省域內的關鍵信息基礎設施也在攻擊範圍內，涵蓋能源、交通、水利、通信、國防科研院校等關鍵領域。這些攻擊妄圖破壞、干擾賽事正常進行，並通過攻擊我國關鍵信息基礎設施製造混亂並竊取敏感情報。

技術團隊發現，亞冬會期間美國國家安全局向黑龍江多個基於微軟Windows操作系統的特定設備發送未知加密字節，疑為喚醒、激活微軟Windows操作系統提前預留的特定後門。據360的實戰安全專家介紹，美國國家安全局主要圍繞特定應用系統、特定關鍵信息基礎設施、特定要害部門開展網絡滲透攻擊，涵蓋數百類已知和未知攻擊手法，攻擊方式超前，攻擊目標和意圖十分明顯。

外交部：採取必要措施保護網絡安全

4月15日的外交部例會上，有記者就懸賞通緝3名美國特工一事提問。外交部發言人林劍表示，此前我們已經多次闡述了中方的立場，在第九屆亞冬會期間，美國政府針對賽事的信息系統和黑龍江省內的關鍵信息基礎設施，開展網絡攻擊，對中國關鍵信息的基礎設施、國防、金融、社會生產、個人信息安全造成嚴重危害，性質十分惡劣。中方譴責美國政府的上述惡意網絡行為。中方將繼續採取一些必要措施，保護自身的網絡安全。

▶《全民國家安全教育日10周年》紀念郵票昨日在內地正式發行。

中方懸賞緝拿美國特工

「2025年哈爾濱第九屆亞冬會」遭受境外網絡攻擊，現成功追查到美國3名特工及具有美國國家安全局（NSA）背景的美國加利福尼亞大學、弗吉尼亞理工大學參與了網絡攻擊。

特工姓名

凱瑟琳・威爾遜
Katheryn A. Wilson

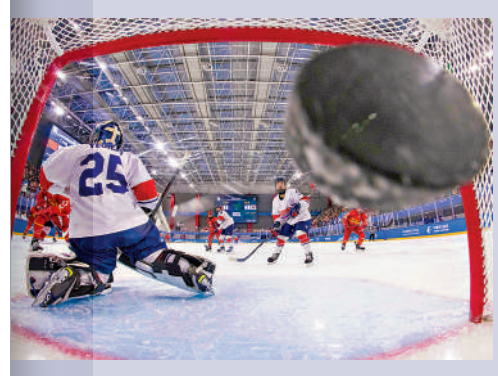
羅伯特・思內爾
Robert J. Snelling

斯蒂芬・約翰遜
Stephen W. Johnson

犯罪事實

- 亞冬會期間，意圖利用網絡攻擊竊取亞冬會參賽運動員的個人隱私數據，破壞賽事信息發布系統、抵離管理系統等
- 亞冬會期間，針對黑龍江重要行業開展網絡攻擊，意圖破壞關鍵信息基礎設施引發社會秩序混亂和竊取相關領域重要機密信息
- 曾多次對我國關鍵信息基礎設施實施網絡攻擊
- 參與對華為公司等企業的網絡攻擊活動

根據人民日報整理



▲亞冬會冰球比賽現場。 新華社

▲4月15日是第十個全民國家安全教育日。10年來，我國應對網絡安全、信息安全等非傳統安全威脅的能力不斷提升。圖為機器人在廣東省國家安全教育館進行講解。 新華社

亞冬會網攻 或是首例用AI智能體「作案」

專家解讀

360集團創始人周鴻禕表示，溯源攻擊者是全世界公認的難題。攻擊者會採取多種手段掩蓋身份，例如此次亞冬會攻擊中，美方在中國周邊國家購買大量跳板IP，每個IP只用一次，還會故意留下虛假線索誤導溯源方向。周鴻禕認為，有充分理由懷疑此次攻擊是人類首次利用AI智能體發起的網絡攻擊。

他解釋稱，以往黑客小隊執行攻擊任務時，需花費較長時間偵查目標對象、搜集情況、制定作戰方案、尋找針對性漏洞並打造黑客工具，攻擊範圍相對較小，而此次攻擊範圍極廣。研判攻擊代碼，此次攻擊採用了智能體技術進行工具方案規劃、漏洞探尋、流量監測，部分代碼明顯由AI書寫，可在攻擊過程中自動、快速編寫動態代碼實施無差別攻擊，且數字人反應速度遠超人類。這種攻擊方式是歷史上從未有過的，對國家安全防護防禦體系構成巨大挑戰。

透過此次事件可見，AI安全已成為網絡空間博弈的焦點，安全專家智能體「AI紅客」、安全大數據、多場景監測體系、面向實戰的安全大模型，將是未來應對AI大規模網絡攻擊的可行路徑。 人民郵電報

▲AI安全成為網絡空間博弈焦點。圖為安全員在遠程監控無人駕駛汽車。 新華社

國安部：部委人員偷錄會議 竊30萬份內部文件

【大公報訊】據紅星新聞報道：4月15日，國家安全部公布一起案例，部委工作人員張某因涉嫌非法竊取國家機密，主動向境外間諜情報機關洩密並意欲叛逃被依法嚴懲。

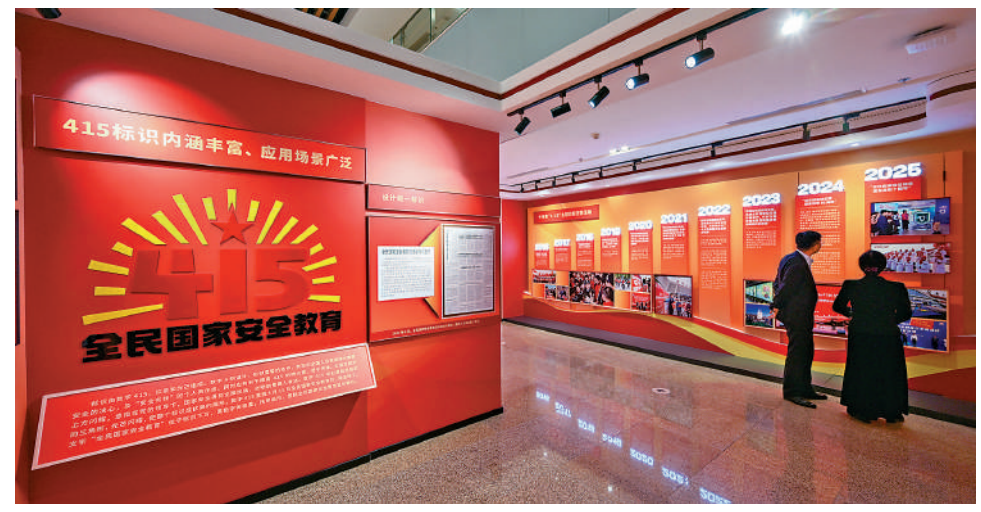
在一次涉密會議上，一支正在工作的錄音筆掉落在座椅下方，從痕跡看，這支錄音筆是用強力膠布粘住，因多次使用粘性減弱而掉落。這引起了高度警覺，單位立刻向國家安全機關報告。

經查，該單位工作人員張某有重大嫌疑。張某，女，出生於一個知識分子家庭，從高中起，張某就開始主動接觸反動思想。

她通過技術手段隱匿身份，主動向境外間諜情報機關發送投靠郵件，出賣國家秘密。張某她利用單位管理漏洞，長期從單位辦公系統違規下載文件，趁辦公室無人之機，竊取拷貝同事計算機內的電子文件，並多次潛入內部會議室投放錄音筆，對會議內容進行秘密錄音。

至案發時，張某累計竊取的內部文件資料近30萬份。案發後，張某隨時準備叛逃，在張某所在單位配合下，國家安全機關及時對其實施控制。

張某重大間諜案的發生，暴露出其所在單位防諜保密主體責任不落實，制度執行不嚴，紀檢部門對案件直接涉及的12名失職失責領導幹部和責任人員分別給予黨紀政務處分。



◀國家安全需要加強國安意識，普及國安教育。 新華社

谷歌地圖將南海標註為「西菲律賓海」混淆視聽

外交部：南海一直是國際社會公認通用地名

▲中國堅決維護南海主權。圖為中國海警3502編隊在南海黃岩島海域進行艦艇編隊訓練。 新華社

【大公報訊】記者馬靜北京報道：近日，谷歌地圖將菲律賓西部水域標註為「西菲律賓海」，而此前這裏顯示名稱為「南中國海」。菲律賓發言人對外表示歡迎這一舉措，稱這將幫助菲律賓保護主權。外交部發言人林劍15日在例會上回應指出，長期以來，南海一直是國際社會公認的通用地名，為世界各國及聯合國等國際組織廣泛接受。

中央廣播電視總台旗下的新媒體賬號玉淵譚天15日發布視頻強調，「西菲律賓海」一詞流行，很明顯是美菲組織的認知行動的一部分。

「西菲律賓海」這個概念如何出現的？玉淵譚天指出，所謂「西菲律賓海」實際上是從地理角度上對我國南海的重新定義。「西菲律賓海」這一叫法的提及量於2023年2月份之前還微乎其微，但此後卻不斷攀升，使用語言最多的是英語，其次才是菲律賓本土語言他加祿語，但在使用他加祿語的帖子裏，對「西菲律賓海」這個詞也特意單獨使用了英文。

為什麼要用「西菲律賓海」混淆視聽？玉淵譚天指出，「西菲律賓海」這個詞與菲律賓侵闖行動高度相關。美國海軍的政策文件中也暴露了行動背後的端倪，美軍希望在南海低成本地「秀存在」。

中國現代國際關係研究院海洋戰略研究所副所長楊霄對玉淵譚天表示，這只是菲律賓政府一段時間以來採取的一個措施，就是要在海上製造了一批「釘子戶」。

玉淵譚天指出，「中國南海」這個稱呼幾百年來被世界各國使用，美菲想顛倒敘事自然不是那麼容易。「西菲律賓海」的互聯網鬧劇在法律上改變不了我國南海的歸屬。

中國海警：堅決反對菲方海上挑釁「碰瓷」

中國海警15日對外披露，菲律賓海警4409船14日位黃岩島附近海域危險接近我海警中南艦，妄圖「碰瓷」擺拍。在海警多次喊話警告和規制下，菲海警船駛離我艦。事後，菲方罔顧事實，在媒體平台製造輿論話題熱點。

中國海警表示，菲方行徑嚴重違反國際法相關規定，以危險方式非法接近我正常航行的海警艦，我方操作專業規範、正當合法，責任完全在菲方。面對菲海警船挑釁「碰瓷」，中國海警將一如既往予以堅決反制，堅定捍衛國家領土主權和海洋權益。

責任編輯：陳晴妍 美術編輯：邱斌玲