美21歲士兵被捕 揭情報系統兒戲

司法部指控洩密或長期監禁 各界驚訝低軍銜可接觸最高機密

香港文匯報訊 美國「洩密門」風波前日終於水落石出，司法部公布在馬薩諸塞州拘捕21歲空軍國民警衛隊成員特謝拉，指控其為今次機密情報外洩源頭。然而事件仍有許多謎團未解，單是特謝拉僅以普通士兵身份，就能暗中獲取外洩的高度機密，就引起各界質疑美國當局能否眞正保護敏感資訊。分析擔憂現時曝光的機密文件，或僅是外洩災難的冰山一角，足以反映美國國家安全存在嚴重漏洞。


◆特謝拉(小圖)被多名持槍FBI特工押走。 美聯社

特謝拉昨日在馬薩諸塞州的美國地方法院提堂，被控未經授權下保留及傳送國防資料，以及蓄意保留機密文件罪名，若罪成料將被判處長期監禁。

特謝拉在軍隊中擔任網絡傳輸系統專家（Cyber Transport Systems Specialist），管理包括光纖和集線器在內的軍方溝通網絡設施。美國網絡安全和基礎設施安全局（CISA）前局長科雷布斯解釋，特謝拉的職位其實就是空軍招聘系統中的網絡科技專家，需要維持空軍基地網絡運作，「他們負責設計部署電腦系統網絡，然後進行維護。」

密件應放在特定文件袋燒毀

科雷布斯指出，特謝拉的軍銜雖低，但工作性質意味他有機會接觸機密網絡科技系統。美軍通常將一些機密材料存放在敏感隔離信息設施（SCIF）中，科雷布斯猜測特謝拉或在處理互聯網系統時，發現了這些被丟棄的機密文件和材料，「印製的材料本應放在特定文件袋中燒毀，當局必須要探究（特謝拉接觸到材料的）細節。」

280萬人擁接觸情報安全許可

美國有線新聞網絡（CNN）提到，類似特謝拉這樣可接觸到美軍機密情報的人其實數目眾多。國家情報總監辦公室統計顯示，截至2017年10月，超過280萬人擁有接觸情報的安全許可，其中逾160萬人可接觸秘密或機密信息，近120萬人可接觸等級最高的絕密信息，另有一些軍隊內的文職人員和承包商也擁有安全許可，只是暫時不能接觸機密資訊。

聯邦調查局（FBI）前數據安全特工坎貝爾表示，相較其他情報機構，美國軍方的安全許可制度存在漏洞，「軍方聘用的擁有接觸情報安全許可人士最多，但軍方沒有和其他機構一樣，對這批人士再進行測謊等嚴格審查。每次發生情報外洩事故後，他們才會汲取教訓，升級情報系統監控力度。」

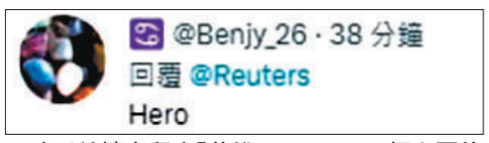
CIA局長：機密情報過度分類

在美國政府高層，不少高官也承認美國情報系統早就需要改善，包括總統拜登政府計劃提出修正案，削減冗雜的情報分類，減少機密情報數目。中央情報局（CIA）局長伯恩斯日前坦言，「我認為美國政府有時存在對機密情報過度分類的嚴重問題，這需要解決。」

康涅狄格州民主黨眾議員海姆斯就事件批評稱，美國一再爆出情報外洩醜聞，勢必影響美國盟友的信任，「我會原諒韓國人、以色列人、法國人或任何人說，『我們恐怕無法與美國人分享我們最敏感信息』，因美國似乎無法阻止這些情報落入21歲年輕人之手，或是出現在前總統的車庫中。」

美網民讚英雄 「憑什麼接受政府再三撒謊？」

香港文匯報訊 在社交媒體上，許多網民眼中的特謝拉並非傳媒形容的「幕後黑手」，反而是揭露美國情報機構暗中所作所為、將真相大白天下的「英雄」。更有不少網民直言，外洩情報揭露美國長期監聽盟友的事實，讓他們對美政府的信任度跌至谷底，質問「我們憑什麼要再次相信政府的說法呢？」



▲路透社讀者留言「英雄」。 網上圖片

▲《華爾街日報》讀者留言「不信任我們的政府」。 網上圖片

「眞理正義捍衛者」成替罪羊

在路透社和《華爾街日報》等外媒報道的帖文中，美國網民紛紛用「英雄」和「替罪羊」等形容特謝拉，有網民稱讚他是「真理和正義的捍衛者」，也有人質疑洩密事件的根源，本就是美國情報機構監督不力，「他們怎麼能讓一名21歲年輕人接觸最高機密？如今他（特謝拉）被拘捕，但為何每個人都能接受政府再度對我們撒謊？」

質問所謂「中國間諜氣球」在哪

還有網民提到，過往許多洩密事件或是美政府的一面之詞，最終都沒有下文，「（前眾議院議長）佩洛西的手提電腦在哪？（總統拜登之子）亨特的電腦呢？國防部不是說擊落了『中國間諜氣球』嗎？它現時在哪？最高法院推翻『羅訴韋德案』的草案是誰曝光的？我們需要一個解釋。」也有網民坦言，美政府暗中監聽盟國動向早已是公開的秘密，「真是可笑，美國的政策毫無作用，這就是一個美國自以為能對付全世界的幼稚遊戲。」

「謊言國家」幕後真相

鍾卓儀

環球點評

美國軍方以至情報部門掘地三尺，似乎總算找到「洩密門」幕後黑手。只不過這並非美方宣稱的「外國間諜」，也不是美媒形容的「種族主義者」。21歲的特謝拉只是一個普通士兵，一個希望身邊朋友不要盲目相信宣傳話術的年輕人，熱愛美國的他外洩的情報，卻親手揭開這個謊言國家又一層外衣，讓全世界進一步窺探毫無意外的眞相。

還記得「洩密門」曝光之初，從無視、冷落、否認，再到反覆辯解，眼見紙包不住火，美國當局愈發慌亂，前一天還是「虛假消息」，下一天就變成「被篡改過的眞實文件」。直到最後終承認機密文件屬實，還不忘加一句外洩的是「廢棄資料」，彷彿加上這些形容詞，就眞的能讓機密外洩損害降到最低。

從文字到圖像，外洩的機密接二連三被公之於衆，美國政府慣用的「敵國間諜說」，這次終於站不住腳。或許若是外洩文件再少一些，又或是能掩人耳目的機會再多一些，我們又要眼見憑空生出好些「間諜氣球」，變出許多「敵國特務」，冒出幾個美方聲嘶力竭要打擊的「邪惡對手」吧。

可笑的是，美國政界和傳媒擔憂的外交風暴倒是沒有出現。正如《紐約時報》自嘲一般的分析，這並非因盟友相信美國的說辭，反而是大家心知肚明：監聽監控、間諜滲透、刺探情報早就是美國的家常便飯。在公開場合宣稱為「牢不可破」的盟友關係背後，盟國對美國本就無限趨近低谷的信任度，今次恐怕又要削減幾分。

不少網民將特謝拉形容作「替罪羊」，不過仔細想來，搬出替罪羊的美國又能掩飾什麼呢？誰不知美國監視盟友已是常態，誰不知北約早已實際參與俄烏衝突，誰又不知如今劍拔弩張的國際秩序背後，唯恐天下不亂的幕後黑手就是美國自己。

出身軍人世家 分享密件免友被洗腦

香港文匯報訊 消息指美國聯邦調查局（FBI）在拘捕特謝拉前，已在其住所附近監視他數天之久，更動用「壓倒性武力」將他帶走。

美國有線新聞網絡（CNN）前日公布拘捕現場航拍錄像，顯示多名FBI特工持槍，指示身穿T恤的特謝拉雙手抱頭走向一輛裝甲車。FBI據報還搜查特謝拉住所，查看電子設備等任何或被用作洩密的物品。

美媒披露，特謝拉於2019年加入美國空軍國民警衛隊，近期剛晉升為一等兵，最近一直在基地上夜班。特謝拉繼父迪福是一名退役空軍軍士長。與特謝拉在社媒Discord上相識的朋友提到，特謝拉一直認為俄烏衝突是一場「令人沮喪的戰爭」，也無意危害美國國家安全，只是希望用自己的方式讓年輕朋友客觀看待一些事件，「他只是對國家的未來沒有信心。」

美媒分析洩密主因

◆持安全許可人數眾多
美國軍方基本依照工作內容，向軍方人員授予安全許可，包括接觸機密資料甚至絕密情報權限，且基本不會考慮持有權限者的年齡和軍銜。例如今次事件中，特謝拉作為軍隊內部的網絡科技專員，工作內容包括設計網絡傳輸系統，就可獲批安全許可，處理維護敏感信息的渠道。

◆所在單位接觸外國情報
特謝拉所屬的空軍國民警衛隊第102情報連隊，負責為派遣至美國各地或海外的飛行員提供全球情報，用於培訓飛行員所需。意味特謝拉有很多機會在工作中接觸到這些情報。

◆軍方保密措施寬鬆
相較美國情報機構，美軍的保密措施寬鬆，相當於允許任何擁有安全許可人士，都能不受限地查閱機密資料及情報。雖然美軍要求獲批許可人士簽署保密協議，但內部追查違規行為的效率極低。

◆汲取教訓反揭新漏洞
「棱鏡門」事件後，美國國防部不允許任何人攜帶電子設備進入五角大樓，還嚴格限制任何人透過網絡或電子設備，接觸儲存在政府電腦「敏感隔離信息設施」的文件及材料。然而今次曝光的許多材料都是紙本文件，說明情報機構雖限制電子途徑洩密，卻又暴露紙本文件洩密的漏洞。

◆國民警衛隊被揭援烏
儘管美方一再否認，但外洩文件顯示國民警衛隊已參與援助烏軍行動，包括分析烏軍無人機作戰過程等。特謝拉作為國民警衛隊情報連隊成員，自然不難獲取俄烏衝突情報。

日政府准大阪建賭場 公眾接力提訴阻撓計劃

香港文匯報訊 日本政府昨日正式批准大阪的綜合度假村連同賭場的計劃，成為日本國內首個賭場設施，預計最快2029年啟用。不過日媒指出，有關計劃仍面對相當多問題。

日本政府昨日舉行綜合度假村計劃推進本部會議，批准大阪興建賭場計劃。擔任推進本部小組召集人的首相岸田文雄表示，「大阪的綜合度假村將是繼2025年大阪及關西世界博覽會後，作為關西發展及國家成長的中心，也是向世界展示日本魅力的觀光地點。」

國土交通大臣齊藤鐵夫在會議後的記者會上公布有關計劃，將在大阪灣的人工島夢洲，建設國際會議中心、酒店及賭場，目標在2029年秋季至冬季開業。

合約租金被指不合理

然而大阪的計劃面對多方面問題，能否成事仍是未知之數。其中反對派以「將地區發展經濟的資金用於賭場」為由，批評有關計劃。賭癮問題也成為反對派的一個理由，指最有效解決方法是放棄興建賭場。

早前有市民提訴指審議過程未充分諮詢公眾，訴訟雖被法院駁回，但本月初有多名市民再發起訴訟，要求禁止市長與營運商簽訂土地租賃合約，原因是有關的租金並不合理，因此有關訴訟仍有機會阻撓計劃。不過大阪以至關西一帶的觀光業界普遍對計劃表示歡迎。在夢洲營運酒店的人士指出，預期未來觀光需求大增，計劃亦有助改善當地交通。


◆大阪綜合度假村模擬圖

WhatsApp增安全設置 加強預防惡意軟件

香港文匯報訊 即時通訊程式WhatsApp前日宣布，將於未來數月更新功能，為用戶增加額外的私隱和安全設置。接下來將啟動三項新設置，包括通知用戶有人試圖將賬戶轉移至另一個設備上、更好預防惡意軟件的賬戶驗證設備，以及確保用戶使用安全連接聊天的自動認證功能。

後端賬戶認證檢測

為加強賬戶保護，若用戶需要在新裝置使用WhatsApp賬戶，WhatsApp將增設一項驗證程序，讓用戶先在舊裝置上進行認證。若賬戶在未經授權的情況下轉移至另一個裝置，用戶將收到通知。

另外，流動設備惡意軟件可在未經允許的情況下，利用用戶的手機並使用WhatsApp發送短訊。WhatsApp指出，目前這是威脅用戶私隱和安全的主要問題之一。為加強預防惡意軟件，WhatsApp將增添後端的賬戶認證檢測。用戶無需採取行動，也可繼續使用WhatsApp。

用戶目前已可使用WhatsApp的安全碼驗證功能，認證聊天對話是否使用安全連接，不過用戶需自行點擊聊天對象信息下方的加密選項查詢。為了讓這過程更簡單方便，新的安全功能將自動進行認證。用戶點擊加密選項時，能立即驗證用戶是否在使用安全連接聊天。