

中方報告披露CIA網暴遍全球「黑客帝國」實至名歸 美方五卑劣手段 炮製50國「顏色革命」

CIA是美國聯邦政府主要情報機構之一，總部位於美國弗吉尼亞州蘭利，下設情報處（DI）、秘密行動處（NCS）、科技處（DS&T）、支援處（DS）四個部門。無論是2014年烏克蘭的「顏色革命」、中國台灣「太陽花革命」、還是2007年緬甸「藏紅花革命」、2009年伊朗「綠色革命」等未遂的「顏色革命」事件，都擺脫不了美國情治機構的影響。據統計，數十年來，CIA至少推翻或試圖推翻超過50個他國合法政府，在相關國家引發動亂。

美國信息通信和現場指揮技術在國際上處於領先地位，給美國情治部門對外發動「顏色革命」提供了前所未有的技術可能性。國家病毒應急處理中心和360公司的報告披露了CIA慣用的五種手段。

首先是提供加密網絡通信服務。為幫助中東地區部分國家的抗議者保持聯絡暢通，同時避免被跟蹤和抓捕，美國研發出一種可以接入國際互聯網又無法追蹤的技術。

相關服務器對流經它們的所有信息進行加密，從而幫助特定用戶實現匿名上網。

專用服務 事件現場「實時報道」

其次是提供斷網通聯服務。為確保突尼斯、埃及等國的反政府人員在斷網情況下仍能與外界保持聯繫，美國谷歌、推特公司迅速推出一款名為「Speak2Tweet」的專用服務，它允許用戶免費撥號並上傳語音留言，這些留言被自動轉換成推文後再上傳至網絡，通過推特等平台公開發布，完成對事件現場的「實時報道」。

第三是提供基於互聯網和無線通訊的集會遊行活動現場指揮工具。美



國蘭德公司花費數年研發出一款被稱為「蜂擁」的非傳統政權更迭技術，用於幫助通過互聯網連接的大量年輕人加入「打一槍換一個地方」的流動性抗議活動，大大提升了活動現場指揮效率。

「暴動」軟件 躲避政府監測

第四是美國公司研發一款名為「暴動」的軟件。該軟件支持100%獨立的無線寬帶網絡、提供可變WiFi網絡，不依賴任何傳統物理接入方式，毋須電話、電纜或衛星連接，能輕易躲過任何形式的政府監測。借助上述功能強大的網絡技術和通訊技術手段，CIA在全球各地策劃組織實施了大量「顏色革命」事件。

第五是美國國務院將研發「反審查」信息系統作為重要任務，並為該項目注資超過3000萬美元。

具體到中國境內多起典型網絡攻擊事件，國家病毒應急處理中心和360公司在調查過程中，從受害單位信息網絡中捕獲並成功提取了一大批與網曝美國中央情報局（CIA）「Vault7」（穹頂7）資料緊密關聯的木馬程序、功能插件和攻擊平台樣本。

【大公報訊】據環球網報道：長期以來，美國中央情報局（CIA）在世界各地秘密實施「和平演變」和「顏色革命」，持續進行間諜竊密活動。國家病毒應急處理中心和360公司4日發布的最新報告披露CIA在全球各地策劃組織實施大量「顏色革命」事件的五項主要技術手段。據統計，數十年來，CIA至少推翻或試圖推翻超過50個他國合法政府，在相關國家引發動亂，最新報告通過實證分析發現，CIA網絡武器現已覆蓋全球，「黑客帝國」實至名歸。



▲國家病毒應急處理中心。

美國CIA五招 互聯網策動顏色革命

- 加密網絡通信 躲避政府審查
- 斷網通聯服務 實時直播現場
- 現場指揮工具 提高控制效率
- 無線「暴動」軟件 無需物理連接
- 研「反審查」系統 專攻中國網絡



CIA九種 網絡攻擊工具

- 框架平台類
- 橫向移動類
- 偽裝正常軟件類
- 攻擊模塊投遞類
- 信息收集竊取類
- 安全軟件攻防類
- 遠程控制類
- 漏洞利用類
- 第三方開源工具類

資料來源：環球網

24小時監控 竊取私人文件

網絡武器

【大公報訊】據環球網報道：國家病毒應急處理中心和360公司通過進一步技術分析發現，儘管CIA的後門程序和攻擊組件大都以無實體文件的內存駐留執行的方式運行，這使得對相關樣本的發現和取證難度極大。即使這樣，聯合技術團隊還是成功找到了解決取證難題的有效方法，發現了CIA所使用的9個類別的攻擊武器，包括攻擊模塊投遞類、遠程控制類、信息收集竊取類、第三方開源工具類等。

其中，聯合技術團隊偶然提取到CIA使用的一款信息竊取工具，它是美國國家安全局的專用信息竊取工具。這種情況說明美國中央情報局和美國國家安全局會聯合攻擊同一個受害目標。2020年，360公司獨

立發現了一個從未被外界曝光的APT組織，將其單獨編號為APT-C-39。該組織專門針對中國及其友好國家實施網絡攻擊竊密活動，受害者遍布全球各地。

此外，CIA攻擊武器的威力和危害性可以從第三方開源工具類中一窺端倪。CIA網路攻擊行動的初始攻擊一般會針對受害者的網絡設備或服務器實施，被控制的目標計算機，會被進行24小時的實時監控，受害者的所有鍵盤擊鍵都會被記錄，剪切板複製黏貼信息會被竊取，USB設備（主要以移動硬盤、U盤等）的插入狀態也會被實時監控，一旦有USB設備接入，受害者USB設備內的私有文件都會被自動竊取。條件允許時，用戶終端上的攝像頭、麥克風和GPS定位設備都會被遠程控制和訪問。

智能電視

● CIA的嵌入式設備分部（EDB）製造了一款名為「哭泣天使」的黑客程序，主要針對三星智能電視，感染這一黑客程序的電視會處於「假開機」狀態——人們以為電視已經關閉，但其實它變成了一個竊聽器，會記錄房間內的對話並通過互聯網發送到CIA的服務器。

汽車

● MDB曾試圖侵入小汽車與卡車的控制系統，以便從事暗殺行動。

智能手機

● MDB開發了多種針對智能手機的攻擊「武器」，被感染的移動設備會向CIA發送用戶的地理位置、音頻和文本信息，以及在用戶不知情的情況下，秘密激活手機的攝像頭與麥克風。

其他設備

● 據統計，到2016年底，CIA下的網絡情報中心（CCI）就製造了1000多種黑客系統、木馬、病毒和其他「武器化」惡意軟件。這1000多種手段，幾乎可以覆蓋目前市面上絕大多數的電子設備系統，這也意味着，美國可以對使用這些系統的人進行監控。

CIA攻擊各行業 中國深受其害

猖獗行徑

【大公報訊】據環球網報道：最新報告通過實證分析發現，CIA網絡武器使用了極其嚴格的間諜技術規範，各種攻擊手法前後呼應，現已覆蓋全球幾乎所有互聯網和物聯網資產，可以隨時隨地控制別國網絡，盜取別國重要、敏感數據，而這無疑需要大量的財力、技術和人力資源支撐，美國式的網絡霸權可見一斑，「黑客帝國」實至名歸。

針對CIA對我國發起的高度體系化、智能化、隱蔽化的網絡攻擊，境內政府機構、科研院校、工業企業和商業機構如何快速「看見」並第一時間進行處置尤為重要。報告建議，為有效應對迫在眉睫的網絡和現實威脅，我們在採用自主可控國產化設備的同時，應盡快組織開展APT攻擊的自檢自查工作，並

逐步建立起長效的防禦體系，實現全面系統化防治，抵禦高級威脅攻擊。

2022年6月22日，西北工業大學發布公開聲明，稱該校遭受境外網絡攻擊。同年9月5日，相關部門對外界宣布，攻擊方是美國國家安全局（NSA）特定入侵行動辦公室（TAO）。對此，網絡安全專家建議用戶對關鍵服務器尤其是網絡運維服務器進行加固，定期更改服務器和網絡設備的管理員口令，及時發現異常的遠程訪問請求。同時，在信息化建設過程中，建議選用國產化產品和「零信任」安全解決方案。專家進一步指出，「只有發展我們在科技領域的非對稱競爭優勢，才能建立起屬於中國的、獨立自主的網絡防護和對抗能力。」

外交部促美停止全球竊密網攻

【大公報訊】據中新社報道：針對有報告披露美國中央情報局（CIA）在中國發動網絡攻擊行為實例，中國外交部發言人毛寧4日在例行記者會上表示，美方應當停止利用網絡武器在全球實施竊密和網絡攻擊。

4日，中國國家計算機病毒應急處理中心與360公司共同發布《「黑客帝國」調查報告——美國

中央情報局（CIA）》。有記者問中方對此有何評論。

「我注意到你提到的這份報告。」毛寧說，根據報告，CIA長期收集外國政府、公司和公民情報信息，組織實施和指導監督跨境秘密活動，在世界各地秘密實施「和平演變」和「顏色革命」，通過向衝突各方提供加密網絡通信服務、斷網通聯服務、集會遊行活動現場指揮工具，以及研

發軟件、「反審查」信息系統等方式，持續進行間諜竊密活動。有關動向值得國際社會高度警惕。

毛寧還指出，報告披露的大量發生在中國和其他國家的真實案例是CIA在全球長期發動網絡攻擊行為的又一實例。

毛寧指出，美方應當重視並回應國際社會關切，停止利用網絡武器在全球實施竊密和網絡攻擊。