美國國家安全局的網絡攻擊武器
“Quantum（量子）攻擊平臺”
你的社交賬號正在監控之下

22日，360政企安全集團首次對外界完全披露美國國家安全局（NSA）針對中國境內目標所使用的代表性網絡武器——Quantum（量子）攻擊平臺的技術特點，同時證明美國的網絡攻擊屬于無差別攻擊，其可以劫持全世界任意地區任意上網用户的正常網頁瀏覽流量。

這是近一月內360第二次披露相關證據，證明美國國家安全局持續不斷對全球發起大規模網絡行動，尤其是針對中國實施網絡攻擊。3月初，360提出一系列證據證明美國國家安全局針對通信行業等關鍵領域視爲重點攻擊目標，全球數億公民隱私和敏感信息無處藏身猶如“裸奔”。中國是美國國安局重點攻擊目標之一，受害單位感染量或達百萬量級。

最新發布的報告則顯示，量子攻擊是美國國家安全局針對國家級互聯網專門設計的一種先進的網絡流量劫持攻擊技術，美國國家安全局利用量子攻擊技術針對世界各國訪問臉書、推特、油管、亞馬遜等美國網站的所有互聯網用户發起網絡攻擊，另外像QQ等中國社交軟件也同樣是他們的攻擊目標。

360公司研究人員對《環球時報》表示，全球遭美國國家安全局竊取的數據包括網絡配置文件、賬號和密碼、辦公和私人文檔、數據庫、網上好友信息、網絡通訊信息、電子郵件、攝像頭實時數據、麥克風實時數據等。這種攻擊是無差別的，除了中國以外，很多與美有合作國家同樣也是美國國家安全局網絡攻擊的目標。

美國頂級武器平臺曝光，完全實現工程化、自動化、人工智能化

量子攻擊系統是美國國家安全局最强大的互聯網攻擊工具，也是其進行網絡情報戰最重要的能力系統之一，創建于2004年，其下包含多個子項目，均以QUANTUM開頭命名。360雲端安全大腦現已發現其包含的九種先進網絡攻擊能力模塊，分別爲QUANTUMINSERT（量子注入）、QUANTUMBOT（量子傀儡）、QUANTUMBISCUIT（量子餅幹）、QUANTUMDNS（量子DNS）、QUANTUMHAND（量子掌握）、QUANTUMPHANTOM（量子幻影）、QUANTUMSKY（量子天空）、QUANTUMCOPPER（量子警察）、QUANTUMMACKDOWN（量子下載）。

量子攻擊系統主要針對國家級網絡通信進行中間劫持，以實施漏洞利用、通信操控、情報竊取等一系列復雜網絡攻擊。這位研究人員指出，“量子攻擊可以劫持全世界任意地區任意上網用户的正常網頁瀏覽流量，進行0day（零日）漏洞利用攻擊并遠程植入後門程序。”

根據介紹，爲了監控全球互聯網目標，美國國家安全局制定了衆多的作戰計劃，相關計劃涉及的具體任務會通過量子攻擊平臺實施，量子攻擊的完整實施過程分爲以下三個階段，現已完全實現了工程化、自動化和人工智能化。在第一階段，量子攻擊實施者會首先對被攻擊目標進行網絡定位，整個定位過程是通過美國國家安全局持有的一整套“量子能力”，網絡黑客攻擊工具完成，這些工作具有對全球互聯網巨頭網絡流量的遠程劫持操控能力。據美國國家安全局機密文檔顯示，“量子能力”的定位操作除了針對特定IP，更重要的是能够針對電子郵箱、社交網絡、搜索引擎、視頻網站等全球網民使用最多的互聯網服務及不同的網站賬號進行遠程定位，快速找出攻擊目標所處的網絡及上網地點。

在第二階段，相關武器會全面監控攻擊目標的互聯網賬號等相關網絡通信内容和其它網絡活動，包括上網終端中存儲的静態文件、上網流量及通訊内容等等。美國國家安全局機密文檔所示，量子攻擊系統後臺顯示了如何監控雅虎、臉書和Hotmail等美國互聯網産品網絡注册用户的部分細節，表明美國國家安全局實際上正在對全球各地使用美國互聯網産品的用户實施無差别監控。

第三階段，美國國家安全局開始實施漏洞利用攻擊，向受害者植入其專屬後門程序，大量竊取受害者個人隱私和上網數據等内容。整個攻擊過程中所采集的大量數據都是在用户毫不知情的情況下獲得的。

全球網民遭無差別攻擊，美國網絡“鐮刀”之下如何獨善其身？

美國國家安全局的全球化無差别入侵行徑，離不開龐大復雜的網絡武器平臺支持。最新報告對量子攻擊系統的應用場景和攻擊實施過程進行技術分析，結合真實案例，全面印證了美國國家安全局針對全球互聯網用户實施大規模無差别網絡攻擊的詳細情況，并總結出美國國家安全局實施網絡攻擊的一些特點。

根據上文中技術人員的介紹，首先，美國的網絡攻擊屬于無差别攻擊，目標是全球範圍，甚至包括美國盟友。美國針對各類電子郵箱、社交網絡、搜索引擎、視頻網站等幾乎所有互聯網用户發起無差别的網絡攻擊，美國的網絡戰略打擊是全球性的、無節制的，在美國網絡攻擊的“鐮刀”之下，没有哪一國能獨善其身。

德國《明鏡》周刊曾報道，美國國家安全局曾竊聽歐盟在美國和布魯塞爾的辦公設施，滲透其電腦網絡，并發動網絡襲擊。丹麥媒體也曾爆料，美國國家安全局利用同丹麥情報部門的合作關系，監聽包括德國總理默克爾在内的歐洲盟國領導人和高級官員。報道稱，美國國家安全局利用盟友監聽盟友，監聽範圍非常廣泛，不僅截獲手機短信和電話内容，還能獲取互聯網上的搜索内容、聊天信息等。

其次，美國的網絡戰戰略，或不僅限于網絡竊密。通過公開的資料已知，美國已經完成了其網絡戰戰略目標第一步——網絡竊密，像斯諾登曝光的“棱鏡”計劃都屬于這一範疇，但不排除美國的下一步目標野心將更大。一旦通過在對手的電腦網絡中安插硬件或軟件後門，實現關鍵目標遠程操控，包括軍事系統、國家公共安全領域的服務器、民航公路鐵路交通系統的主機、銀行金融系統的服務器等，其對手將毫無談判的餘地。

第三，當前美國國家安全局網絡武器攻擊已完全實現了工程化、自動化和人工智能化。網絡戰時代到來，網絡武器的自動化優勢成爲超越信息優勢的“進階優勢”，而美國國家安全局組織的量子系統可能僅是冰山一角，美國或掌握着更多更高度工程化的網絡攻擊平臺，其自動化的“思考”速度和質量，極大提高了美國自主作戰系統實現制勝目標的優勢，也爲全球網絡安全帶來無窮隱憂。

第四，爲應對網絡戰，美國政府充分利用一切先進技術和網絡資源。美國有着全球最先進的互聯網技術，這是盡人皆知的，但爲了掌握網絡戰主導權，美國將諸如量子攻擊系統等大量頂級技術手段、高端人才、情報力量納入作戰序列，由此可見美國對發展網絡作戰力量的重視程度，并不計成本地投入資源、增加籌碼。

評論：美國是威脅中國和世界網絡安全的“黑客帝國”

近期，中國國家計算機病毒應急處理中心披露了美國國家安全局對外網絡攻擊竊密的主戰網絡武器“NOPEN”。國内兩家企業也發布報告，披露了美國國家安全局的網絡攻擊武器“Quantum攻擊平臺”等，指出美國國家安全局等部門對中國、俄羅斯、日本、英國、德國、韓國等全球四十多個國家和地區實施長期網絡攻擊，滲透政府、國防、航天、關鍵基礎設施、企業等。上述事實表明，美國早已運用高度發達的網絡武器開展全球無差别網絡攻擊，其不但是中國網絡安全的主要威脅，也嚴重威脅世界各國網絡安全。

中國一向是美國網絡攻擊的重點目標。多年來，美國是持續對中國發動網絡攻擊的“黑客帝國”。中國國家互聯網應急中心歷年來統計顯示，從2017年至今，美國始終是中國遭遇網絡攻擊的最大來源國。美國政府也毫不掩飾對中國的網絡攻擊意願。2020年7月，美媒《華盛頓郵報》披露，特朗普政府在2018年簽署了“通知備忘録”，授權美國中央情報局不經國會批準即可對中國發動網絡攻擊，不但將媒體、金融機構、商業公司等納入網絡攻擊授權範圍，還授權“幹擾”“破壞”“摧毁”電力、石油等關鍵基礎設施。

美國叫囂對中國實施網絡攻擊不衹是嘴上説説，美國中央情報局、國家安全局等機構對中國政府、企業、公民發動的網絡攻擊屢見不鮮。2020年3月，360公司披露，從2008年9月到2019年6月，美國中央情報局使用網絡攻擊武器“Vault7”持續對中國政府機構、航空航天、科研機構、石油行業、大型互聯網公司等實施網絡攻擊。2021年1月，《華盛頓郵報》披露，美國國家安全局曾成功入侵華爲公司的設備，并制定了秘密網絡攻擊計劃“Shotgiant”，對華爲在中國的電信設施實施網絡竊密。近期中國兩家網絡安全企業還發現，中國公民使用的賬號密碼、辦公文檔、私人文件、電子郵件、攝像頭實時數據、麥克風實時數據、甚至QQ等社交軟件也是美國國家安全局的網絡攻擊目標。

美國常年對中國實施的網絡攻擊竊取了海量個人數據，侵犯中國公民權益，嚴重危害中國國家安全、關鍵基礎設施安全以及商業和技術秘密，違背了聯合國在網絡空間達成的國際規則，拋弃了中美2015年達成的網絡安全雙邊共識，嚴重影響了中美在網絡空間的互信。然而，美國不但不反思自身問題，反而在網絡安全問題上顛倒黑白，對中國進行無理指責，展示了赤裸裸的霸權主義行徑。

世界各國也飽受美國網絡攻擊之苦。美國網絡攻擊監控各國的舉動讓全球震驚。2013年，美國國家安全局承包商前雇員愛德華·斯諾登披露，美國國家安全局啓動“棱鏡”等項目，通過網絡攻擊海底光纜、網絡設施，監控全球各國，上至政要，下至普通公民，一舉一動都成爲美國家安全局存儲的“永恒記録”。“斯諾登”事件後，美國也未收手，其在全球的網絡攻擊活動不時曝光。2020年11月和2021年5月，歐洲媒體連續披露美國國家安全局網絡監控電纜進而對法、德等歐洲盟友進行竊密的醜聞。歐盟、拉美等國領導人均强硬表示美網絡攻擊活動“完全不可接受”“踐踏雙邊互信”等。

美國網絡監控盟友政要尚且毫無顧忌，對他國政要、關鍵基礎設施實施網絡攻擊更加肆無忌憚。美橙色特遣部隊網絡監控伊朗將軍蘇萊曼尼手機，從而爲無人機暗殺鎖定蘇萊曼尼車輛順序。此外，俄羅斯互聯網研究機構、伊朗核設施也曾遭到美國政府網絡攻擊破壞。當前，全球政企的大敵“勒索攻擊”的始作俑者也是美國。2017年，美國國家安全局網絡武器“永恒之藍”曝光。今天，該網絡武器的變種已導致全球航運、制造業、食品、支付等重要供應鏈多次停擺，成爲全球威脅。

“以力假仁者霸”。美國是全球網絡安全公敵，却醞釀成立所謂“未來互聯網聯盟”，主導小圈子討論網絡安全問題，甚至派遣網絡部隊“幫助”很多受美國網絡攻擊的國家“提升網絡安全能力”，扮演國際網絡安全維護者角色。但其實質是憑借網絡實力强推美國網絡霸權，并不符合全球各國的安全與發展利益。

2021年，各國在聯合國信息安全開放式工作組達成共識，認爲全球要共同應對網絡安全威脅，增進了對網絡空間人類命運共同體理念的認同。這昭示着網絡空間人類命運共同體理念的時代感召力、理論説服力和實踐引領力，必將推動建立各方平等參與、開放包容、可持續的網絡安全治理進程，制定各國普遍接受的網絡空間國際規則，加快構建網絡空間人類命運共同體，實現網絡空間共同安全。（周寧南 中國現代國際關系研究院助理研究員）