中國最新網路武器 GREAT CANNON

加拿大多倫多大學(University of Toronto)所屬的資安研究機構「公民實驗室」(Citizen Lab)，於 4/10 發布一篇名為「China’s Great Cannon」的報告，指出中國在網路防火牆(Great Firewall，或稱網路長城)之外，又發展了一個名為「巨砲」(Great Cannon)的網路審查武器，讓網路長城的威力擴大到能夠把中國境外使用者轉變為網路攻擊武器。2015/3/16，GreatFire.org 網站遭分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊，緊接著於 3/26，GreatFire.org 所經營的兩個 GitHub 專案也遭到同樣手法的攻擊。這場歷時五天的攻擊也是 GitHub 有史以來遭遇過最嚴重的 DDoS 攻擊，兩次攻擊行動均鎖定想繞過中國言論審查的服務。攻擊者先在百度服務中注入惡意 JavaScript，再讓受感染的使用者瀏覽器不斷載入鎖定目標的網頁。

當時外部一些研究認為，這是以經過精心策畫的中國網路長城機制所發動的攻擊，但經 Citizen Lab 研究後發現，這是與網路長城機制結合在一起、但功能與設計皆不同的另一套系統。Citizen Lab 稱之為「巨砲」（Great Cannon)。它是網路防火牆的延伸，會綁架流量到特定 IP 位址，並針對未加密內容發動中間人攻擊(Man-In-the-Middle Attack)篡改內容。研究人員指出，分析「巨砲」之後發現，中國的國家級資訊控制行動更加升級，廣泛使用各式工具，將使用者變成武器，以達到言論管制的目的。更重要的是，它的對象不再限於中國人民，而是企圖操控中國境外的「旁觀者」(bystander)，暗中對瀏覽器動手腳，以進行大規模 DDoS 攻擊。

以最近 GreatFire.org 與 GitHub 的攻擊為例，「巨砲」攔截連向百度代管廣告網站的流量，如果發現有 JavaScript 的呼叫，可以選擇不動作(約占 98.25%時間)，或是改為回傳惡意 JavaScript (約占 1.75%)。在此次攻擊中，一些中國境外的使用者若有瀏覽到具百度代管廣告的網站時，就可能被挾持，成為 DDoS 流量攻擊的一部份。Citizen Labs 並指出，「巨砲」雖然此次只是利用百度，但顯然它具有可針對與中國網站通訊的任何外國電腦進行攻擊的能力。不過研究人員指出，目前「巨砲」只能控制 HTTP 流量，因此想防止被挾持攻擊，啟用 HTTPS 加密已成為必要條件。