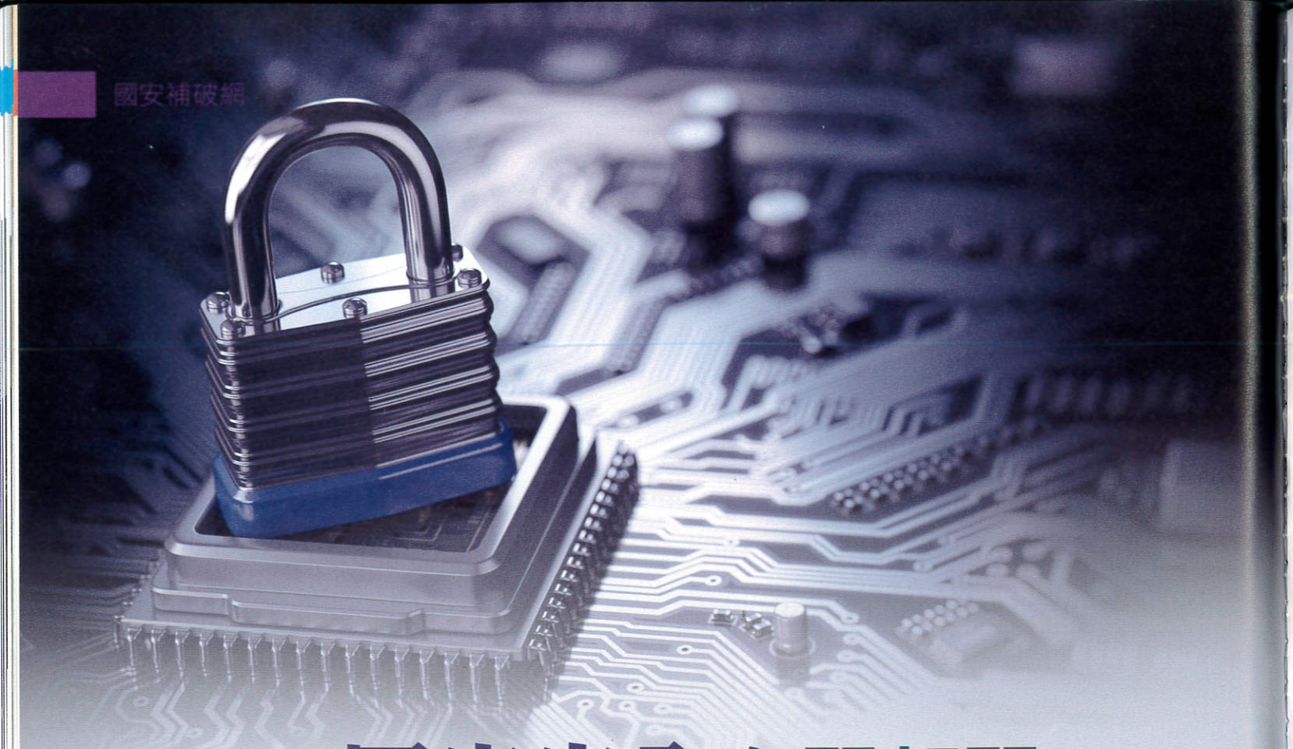


國家安全有關部門因應網路威脅之治理趨勢

／中央警察大學恐怖主義研究中心主任　汪毓瑋

在網際網路節點中引入政府監管職能的呼聲越來越大，且將域名系統的職能從傳統的地址解析轉換成網際網路內容監管的實施者，可能將更多的應用於對政治性內容的審查。

網際網路治理與個人自由

當提及網際網路治理時，必須認清治理的控制點，既不會是法律控制點，也不會限制在一個國家的範圍之內。而通常是由多種因素來決定和展現的，包括網路架構設計理念、全球性網際網路治理機構的決策、私營企業的策略、與國家法律體系常態化對抗中的所有全球性獲勝方、政府之間條約以及區域文化理念等。

但隨著更多的資訊安全要求與網路威脅不斷浮現，網路治理必然趨於更緊縮與嚴格的管理形態，不僅對網際網路技術架構的穩定性造成威脅，且會直接影響到匿名、安全和言論自由等方面的個人權利和自由。這些必須面對的議題包括了：

一、在國家治理與跨國界治理模式之間，應該實現什麼樣的平衡？

二、在判斷是文化表達還是政治交流時，企業應該承擔什麼樣合適的「社會責任」？

三、在維持網際網路創新和商業模式的營利性與個人匿名和知識獲取之間，應該實現何種樣態的最佳平衡？

這些議題引發無法提出有效解決辦法之具體問題，包括了：

一、在網際網路「互連點」不斷試圖且強化引入政府的管制。

二、多方利益共享者治理和政府控制之間不斷升高的緊張關係。

三、被描述為「浮士德交易」的在線廣告中，用戶以隱私換取網際網路產品而不自覺。

四、網際網路技術架構的發展趨勢與在線匿名之應有本質已逐漸偏離。

五、網際網路相互操作性持續地受到侵蝕。

六、將「域名系統」（DNS）作為網際網路主要的內容控制機制。

2011 年 8 月 11 日，灣區快運（BART）為了阻止抗議行動關閉站內移動通信近 3 小時，引起民眾大肆抨擊，後於 8 月 22 日又群起抗議。（圖片來源：美聯社／達志影像）

政府介入網際網路治理之藝術

2011 年 8 月，由美國政府營運的「灣區快運」（BART）交通系統為了阻止站內的一起抗議行動而關閉其站內移動通信近 3 小時，結果引起民眾大肆抨擊並向「聯邦通信委員會」提告其不僅違反了《國家通信法》且違背憲法第一修正案。

這一事件的脈絡，絕非表象上的只是關閉通信而已，實際上是反映出安全、駭客攻擊、言論自由、隱私保護、法律實施的目的及集會遊行權等之各種層面的複雜糾結。

資訊基礎設施可以經由不同的機制進行干預，且儘管情境不同、方式不同，但是概具有政治性的共同特徵。且涉及了以下四種對於網際網路治理的機制：

一、深度封包檢測（Deep packet inspection, DPI）

這是一種流量控制技術，是將有限的寬帶資源分配給不同資料包的一種技術，可以想像為「開閘放水」，能夠細察到資料包的全部內容，包括負載與包頭，因此，可以對網際網路上傳輸的內容包進行檢

測、分析，且做出不同的策略處置。對於情治機構之資訊蒐集，或是政府想要實施監控或審查都是非常有效的工具。

而此技術的「檢測能力」與「資訊操縱能力」的不當使用，將有違平等原則、經濟自由和言論自由，且涉及的政策問題包括了：

1. 對個人發送與接送的資訊進行檢測，在什麼程度上算是保留了個人隱私？
2. 「激冷效應」下的資訊揭露是否影響了個人在線自由？
3. 消費者應該期待什麼樣合理的私人活動透明性？
4. 網路營運商優先傳輸自己內容的合法性是否與網路中立相抵觸？
5. 來自情治機構或媒體內容公司等第三方的各類內容管控要求，是否使私營企業的營運負擔不斷地加重？
6. 如何在機械性的執法環境中，保護合法交易或公平使用受版權保護的內容？

二、阻斷連接的「終止開關」（kill-switch）方法

網際網路在設計上之底層的分布式、網狀架構可為網路破壞提供最大保護，因為可能仍有被實體攻擊後的倖存「節點」可以持續的工作；但是相對的，由於傳統的交換「節點」集中、分級組織的網路架構仍然很容易遭受大規模的破壞。

這些可以引起網路破壞的薄弱控制點，如下表所示：

表 1　九種可以導致網際網路破壞的控制點類型

類 型	方 式
制度層破壞	ISP 服務中斷（BGP ／ DNS）、移動服務中斷
應用層阻斷	社交媒體站點、電子郵件、SMS、Web、Skype
與內容相關的阻斷	搜索關鍵詞、用戶生成內容、新聞媒體、社交媒體內容
網路管理層破壞	網路性能調控 DDoS 攻擊、時延、DPI 過濾
協議層阻斷	BitTorrent、VoIP、SMTP、HTTP、IPv6、FTP
金融和交易服務中斷	信用卡交易、在線支付服務、其他交易類服務
域名系統	DNS 過濾、托管服務、註冊管理、註冊服務
交換層基礎設施	路由器設施、互聯網交換點、網路交換機
海底光纜	電源系統、跨國骨幹網、外部基礎設施

資料來源：引用 The Global War for Internet Governance 一書內容

圖 1　資訊基礎設施涉及的網際網路治理機制

三、政府授權審查機制

政府想阻斷或是移除網際網路內容，常不會親自執行，除非想要屏蔽的內容託管在政府的網路服務器之中。而要求移除的在線內容，通常是為了推動本國的法遵執行，範圍包括了誹謗、國家機密、仇視性攻擊言論、褻瀆、兒童保護、色情、隱私、侮辱國家元首、在選舉和競選資助法律框架下的各種政治言論限制等。

私營企業在回應政府要求時，會經歷困難與複雜的決策過程，特別是因為政府對內容的干預已經明顯地進入政治言論的領域。這些私營企業承擔了仲裁員的角色，在面對政府壓力下要自行決定什麼該審查及什麼不該審查。且常陷入是對政府權力起監督作用抑或僅是作為執行政府請求的調和力量？或是介於兩者之間？如何決定是取決於公司自身的服務條款框架及所處的情境與特定的環境。

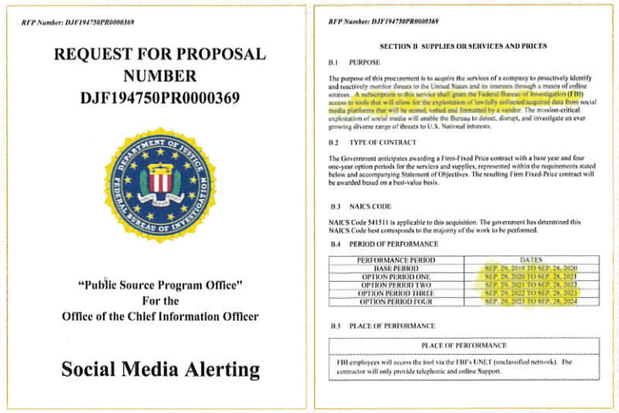
四、阻斷式服務攻擊

是使用「流量壓制」的技術手段，可以直接用於對抗民間團體，以及用大量垃圾流量對網站進行攻擊而遏制言論自由。

美國聯邦調查局之公私部門合作案例

2018 年 9 月，聯邦調查局局長克里斯托弗・雷（Christopher Wray）公開提醒，許多恐怖攻擊事件已經顯示出「鎖定年輕人的社交媒體宣傳及其對於年青人影響力」之煽動，並且使年輕人不斷的被激進化。而在 2019 年 4 月的「外交關係委員會」（Council on Foreign Relations）中亦警告「俄羅斯仍然是對選舉安全的重大威脅，因為他們利用社交媒體企圖讓我們互相攻擊，並破壞美國人對民主的信心」。

美國聯邦調查局局長克里斯托弗・雷在 4 月舉辦的「外交關係委員會」中警告俄羅斯在社交媒體運作上的威脅性。（Photo Credit: Federal Bureau of Investigation, https://multimedia.fbi.gov/item?type=image&id=3962）



RFP Number: DJF194750PR0000369

REQUEST FOR PROPOSAL NUMBER DJF194750PR0000369

"Public Source Program Office" For the Office of the Chief Information Officer

Social Media Alerting

RFP Number: DJF194750PR0000369

SECTION B SUPPLIES OR SERVICES AND PRICES

B.1 PURPOSE

The purpose of this procurement is to acquire the services of a company to proactively identify and reactively monitor threats to the United States and its interests through a means of online screens. A subscription to this service shall grant the Federal Bureau of Investigation (FBI) access to tools that will allow for the exploitation of lawfully collected/acquired data from social media platforms that will be stored, vetted and formatted by a vendor. The mission-critical exploitation of social media will enable the Bureau to detect, disrupt, and investigate an ever growing diverse range of threats to U.S. National interests.

B.2 TYPE OF CONTRACT

The Government anticipates awarding a Firm-Fixed Price contract with a base year and four one-year option periods for the services and supplies, represented within the requirements stated below and accompanying Statement of Objectives. The resulting Firm Fixed-Price contract will be awarded based on a best-value basis.

B.3 NAICS CODE

NAICS Code 541511 is applicable to this acquisition. The government has determined this NAICS Code best corresponds to the majority of the work to be performed.

B.4 PERIOD OF PERFORMANCE

PERFORMANCE PERIOD	DATES
BASE PERIOD	SEP. 29, 2019 TO SEP. 28, 2020
OPTION PERIOD ONE	SEP. 29, 2020 TO SEP. 28, 2021
OPTION PERIOD TWO	SEP. 29, 2021 TO SEP. 28, 2022
OPTION PERIOD THREE	SEP. 29, 2022 TO SEP. 28, 2023
OPTION PERIOD FOUR	SEP. 29, 2023 TO SEP. 28, 2024

B.5 PLACE OF PERFORMANCE

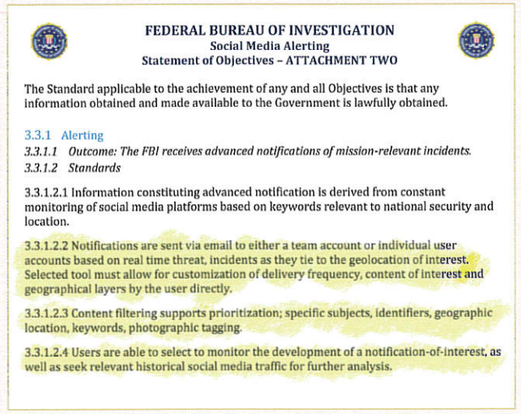
PLACE OF PERFORMANCE
FBI employees will access the tool via the FBI's UNET (unclassified network). The contractor will only provide telephonic and online Support.

美國聯邦調查局在 2019 年 7 月 8 日公告的「徵求建議書」，內容揭示徵求目的與履約期限。（Source: Federal Business Opportunities, https://www.fbo.gov/index?s=opportunity&mode=form&id=fe943e551236e0e62ee0843d5803781e&tab=core&_cview=0）

2019 年 7 月 8 日，「聯邦調查局」以「徵求建議書」（Request for Proposal, RFP）的方式，以固定價格合約形式公開招標有能力進行「主動識別和被動監控 」（proactively identify and reactively monitor）社交媒體帳戶而能夠提供識別和存儲各種各樣威脅之有興趣的承包商來競相投標，同時也要確保滿足所有隱私和公民自由合規的要求。合約基本是 1 年，將於 9 月 29 日開始，也可能延長為 4 年。

「徵求建議書」之內容指出，該局尋求「存取工具，允許從社交媒體平臺利用合法收集／獲取的資料，這些資料將由供應商進行存儲、審查和格式化」。強調對於社交媒體的運用將能夠偵測、破壞和調查對美國國家利益的各種各樣威脅。因為恐怖主義團體、國內威脅者、外國情報機構和犯罪組織利用社交媒體平臺進一步開展非法活動，因而需要有適當的工具來正確識別活動並作出適當的反應。

由於這些威脅已更多地使用社交媒體平臺，因此及時獲得一項能夠使該局從“Twitter”、“Facebook”、“Instagram”和其他社交媒體平臺中識別相關資訊的服務至關重要。因為該局需要及時進入各式樣的社交媒體以獲得最新資訊，才能更佳地促進其執法和情報任務的有效性。並希望收到「源自基於與國家



FEDERAL BUREAU OF INVESTIGATION
Social Media Alerting
Statement of Objectives – ATTACHMENT TWO

The Standard applicable to the achievement of any and all Objectives is that any information obtained and made available to the Government is lawfully obtained.

3.3.1 Alerting

3.3.1.1 Outcome: The FBI receives advanced notifications of mission-relevant incidents.

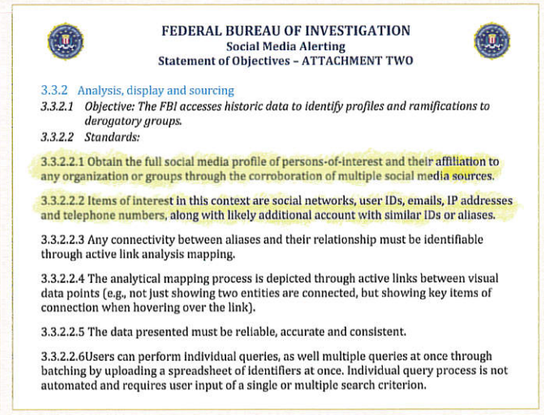
3.3.1.2 Standards

3.3.1.2.1 Information constituting advanced notification is derived from constant monitoring of social media platforms based on keywords relevant to national security and location.

3.3.1.2.2 Notifications are sent via email to either a team account or individual user accounts based on real time threat, incidents as they tie to the geolocation of interest. Selected tool must allow for customization of delivery frequency, content of interest and geographical layers by the user directly.

3.3.1.2.3 Content filtering supports prioritization; specific subjects, identifiers, geographic location, keywords, photographic tagging.

3.3.1.2.4 Users are able to select to monitor the development of a notification-of-interest, as well as seek relevant historical social media traffic for further analysis.



FEDERAL BUREAU OF INVESTIGATION
Social Media Alerting
Statement of Objectives – ATTACHMENT TWO

3.3.2 Analysis, display and sourcing

3.3.2.1 Objective: The FBI accesses historic data to identify profiles and ramifications to derogatory groups.

3.3.2.2 Standards:

3.3.2.2.1 Obtain the full social media profile of persons-of-interest and their affiliation to any organization or groups through the corroboration of multiple social media sources.

3.3.2.2.2 Items of interest in this context are social networks, user IDs, emails, IP addresses and telephone numbers, along with likely additional account with similar IDs or aliases.

3.3.2.2.3 Any connectivity between aliases and their relationship must be identifiable through active link analysis mapping.

3.3.2.2.4 The analytical mapping process is depicted through active links between visual data points (e.g., not just showing two entities are connected, but showing key items of connection when hovering over the link).

3.3.2.2.5 The data presented must be reliable, accurate and consistent.

3.3.2.2.6Users can perform individual queries, as well multiple queries at once through batching by uploading a spreadsheet of identifiers at once. Individual query process is not automated and requires user input of a single or multiple search criterion.

「徵求建議書」附件包含需求相關細項說明。（Source: Federal Business Opportunities, https://www.fbo.gov/index?s=opportunity&mode=form&id=fe943e551236e0e62ee0843d5803781e&tab=core&_cview=0）

安全和位置相關的關鍵詞的社交媒體平臺的持續監控」的警報，且對「特定主題、識別碼、地理位置、關鍵字、照片標記進行優先的內容過濾」。

在運作上，契約商是通過電子郵件將「通知」發送到該局之團隊帳戶或是基於及時威脅、異常事件的個人用戶帳戶，因為它們連結到感興趣的地理位置。且所選定的工具必須允許用戶可以直接客制化的次序傳送有興趣的內容和地理圖示。用戶可以選擇監控感興趣的通知的發展，以及尋求相關的歷史社交媒體流量，以深化進一步分析。也希望「通過多種社交媒體來源的確證」獲取有關人士及其與任何組織或團體的關係的完整社交媒體資料，包括了「用戶身份識別、電子郵件、IP 地址和電話號碼，且可能還有類似 ID 或別名的額外帳戶」。

結論

對比非民主國家之網際網路治理及與私部門合作之現實，美國聯邦調查局實際上也基於最大安全維護的考量，借重私部門的力量來預防與遏阻來自網路威脅的先期安全資訊掌握，且大概已是西方民主國家目前慣用手段。但如何可以兼顧民權之維護迄無有效辦法，而更多僅是政治上的言詞保證而已。