

● 作者/John Bumgarner ● 譯者/楊黎中

技術本位的恐怖分子

Tech-savvy Terrorists

取材/2011年第2季美軍太平洋司令部亞太防衛論壇季刊(*Asia Pacific Defense FORUM*, 2nd issue/2011)

拜電腦科技發達之賜，網際網路業已成為恐怖分子逞其陰謀的有效工具。打擊隱身於網路的恐怖分子，除須善用先進技術，以期先知勝敵外，另要考量大眾隱私與個人自由，此乃有關當局執法工作上不得不面對的重要課題。

2008 年11月底於孟買的某個夜裡，熙來攘往的街景頓時被突如其来自動武器掃射亂了秩序。當槍聲停歇後，

計有175人死、308人傷。恐怖攻擊在印度並非新鮮事，但此次由「拉什卡-塔伊巴組織」(Lashkar-e-Tayyiba，又稱「虔誠軍」[Army of the Righteous])

恐怖活動手法日新月益，令人防不勝防，且往往造成慘重死傷。圖為911事件中遇襲的美國五角大廈。(Source: DoD)



成員執行之恐怖攻擊，卻具備一項以往恐怖事件欠缺的重要部分——21世紀科技的運用。

有關當局在針對此一慘劇的後續調查中，發現孟買事件的恐怖分子於行動各階段均曾運用科技。在計劃階段，攻擊者利用Google Earth對其目標進行虛擬偵察。Google提供的高解析度圖像，讓恐怖分子得以極精確的策劃自殺任務，甚至細微到涵蓋各主要目標位置預計



2010年5月美國網路指揮部正式成立，並由亞歷山大(Keith Alexander)上將(右)擔任首任指揮官。(Source: DoD)

網路上的恐怖分子教室

極端分子團體也分別在公開與會員制入口網站散布訓練教材。這些教材包括多種美軍使用的訓練手冊(尤以美陸軍為主)，並在許多極端分子網站上唾手可得。這些描述戰技的手冊使得極端分子團體更趨暴力。例如，美陸軍為特種部隊編寫的TM 31-210《非常規/非制式彈藥手冊》(Improvised Munitions Handbook)，即已在極端分子團體網站間廣為流傳。該技術手冊對於製造非常規/非制式爆炸裝置提供了相當實用的資訊，而其材料大多可輕易自居家修繕賣場購得。雖然該手冊所敘述之技術業經恐怖分子團體成功運用數十年，網際網路顯然已降低了散布這些教材所需之成本。其他經常由極端分子散布在網站上的手冊包括：《恐怖分子手冊》(The Terrorist's Handbook)、《無政府

主義者食譜》(The Anarchist Cookbook，譯註：Powell William於1970年代為抗議美國政府捲入越戰而著，其內容包括製造爆裂物和盜用電話通訊裝置等方法)，以及《聖戰者毒藥手冊》(Mujahedeen Poisons Handbook)等。

許多恐怖分子或極端分子組織也藉由網際網路自行發展與散布訓練教材；線上串流視訊的進步，業已擴展了這些虛擬教具的功效。運用網路散布之舉也為這些團體帶來其他益處。例如，透過網路的訓練可能較實體訓練營安全，因為後者易遭實體攻擊。再者，無論是空中轟炸或是地面部隊的小規模攻擊，都會對訓練營與參訓人員造成威脅。反之，若1個訓練網站遭到關閉，其成員非但毫髮無傷，且可擇日再戰。

恐怖分子組織透過網路散布方式，可更有效率的將戰技授予更多人；網上訓練教材可快

使用的出入口。Google同時提供攻擊者該目標之地理座標，以供其載入全球定位系統裝置。運用前述資訊，攻擊者即可藉夜色掩護，順利到達其海上滲透點而不被發現。善用科技之舉，大幅降低了攻擊者在沿其突擊路徑行動時遭遇意外障礙之可能性，進而強化了攻擊的效果。

在孟買突擊事件的執行階段，恐怖分子使用的行動電話

配備了來自不同國家的「用戶識別模組」(Subscriber Identity Module)卡。攻擊者使用這些手機將最新狀況供予其策劃者，後者則利用「網際網路語音協定」(Voice over Internet Protocol, VoIP)通訊方式掩蔽其實際位置。調查人員推測，這些策劃者係利用即時電視轉播追蹤警察，以及回應攻擊的反恐突擊隊所在位置。據稱，這些策劃者係以其行動電話上「簡訊服務」

(Short Message Service, SMS)，將警方最新位置告知行動人員。上述通訊方式使得執法單位更難以截聽其通話，且在攻擊後不易追查其行蹤。

印度當局就境內恐怖分子未來可能使用黑莓機，或相當普遍的Skype網際網路語音協定服務來協調攻擊行動一事表達關切。這兩種通訊方式所特有的賣點之一就是強大之加密功能。印度政府最近要求黑

速分發至遍布全球的極端分子團體成員；教材可經成員下載(複製)且幾無需任何附加成本，另可供給為數可觀的成員同時使用。就極端分子組織招募新血與灌輸新成員思想等而言，前述教材同樣有所助益。

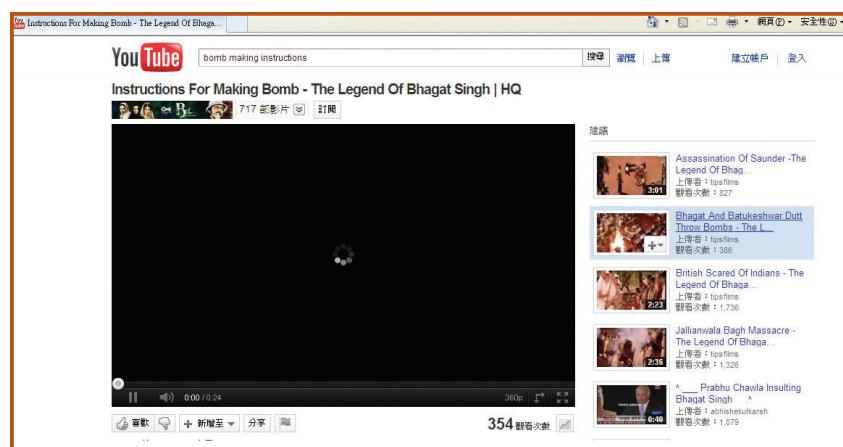
由恐怖分子團體發展的虛擬訓練教材，課目林林總總的包括非常規/非制式爆炸裝置的製造法，以及肩射/面對空飛彈的指導等。某個恐怖分子所製視訊，則示範車載非常規/非制式爆炸裝置(或稱汽車炸彈)的製作技巧。亞太地區發生的多起恐怖攻擊中，均成功使用過汽車炸彈，包括2002年的印尼峇里島事件、2008年的巴基斯坦伊斯蘭馬巴德事件，以及2009年的泰國納拉提瓦(Narathiwat)事件等。目前大多數恐怖攻擊的炸彈係由自殺炸彈客遞送，但全球定位系統的技術提供了另一種方法。該技術使恐怖分

子組織得以發展出1種炸彈，結合具有全球定位系統功能的起爆器與定時裝置，可採多重方式將其運送至目標處。

許多影片都廣為宣傳極端分子團體的激進暴力作為。例如，一些影片顯示路邊炸彈對抗駐伊拉克聯軍的戰術效能，某些影片則記錄極端分子團體對俘虜施加之暴行，另有些影片強調其他團體成員的殉道方式。支持多個涉及蓋達相關運動組織的「雲彩伊斯蘭媒體基金會」(As Sahab Foundation for Islamic Media Publication)，在綜合上述部分要件後，製作了1部獨特影片，用以描述2008年丹麥駐巴基斯坦大使館遭炸彈攻擊事件。影片以採訪1名自殺炸彈客為開場，然後使用電腦動畫模擬自殺炸彈攻擊丹麥大使館的過程，最後以熊熊火球收場。該部影片業經許多網站(包括YouTube)廣為流傳。

毒機製造商——位於加拿大的「行動研究公司」(Research In Motion)——將可解譯傳送中簡訊與電子郵件之金鑰供給該國政府；印尼亦要求該公司將加密金鑰供給政府當局，否則將採取法律行動。

證據顯示，恐怖組織不僅使用市面可得之加密程式，更開發出其自有之精密應用程式。例如，為解決日漸憂慮的竊聽問題，「全球伊斯蘭媒體陣線」(Global Islamic Media



YouTube是許多恐怖分子交流資訊與策劃活動的新溫床。(Source: Internet)

Front)先在一些權限管制的網路論壇中釋出1個名為「阿斯拉姆

加賀鼎」(Asrar Al-Mujahidin，意即「聖戰者的秘密」)之加密

恐怖的社交網路

極端分子團體亦普遍使用許多時下最流行的社交網站，包括Facebook、Friendster、LiveJournal，以及MySpace，俾與同情者聯繫，並藉此向大眾散布宣傳資料。例如，菲律賓的「莫洛伊斯蘭解放陣線」(Moro Islamic Liberation Front)便維持1個Facebook專頁，而幾名聲稱是「阿布沙耶夫」(Abu Sayyaf)成員者，也擁有Myspace帳號。藉由此一通往廣大用戶網路的途徑，這些入口網站有助於前述團體在全球從事人員招募與資金籌措的工作。

恐怖分子亦可使用Twitter微網誌服務向世界各地的成員發布行動資訊。例如，下列加密文字即包含亞洲某熱門旅遊景點的地理座標、將採取的攻擊方式、發動攻擊的日期，以

及下一個用以散布行動資訊的Twitter帳號：

T1HHTKampqYIsoTmfOEDxXgvd4COL1IX
g2YZSsvBmrwZsCZfa3pkNSKfKyP263gMTwU
JQK54tmPYCWhOi8Y2fFethEOb8KCbFw= =

許多社交網站提供的私人、近乎匿名之通訊架構，使極端分子組織成員得以藉此逃避大多數執法機構的查察。某些具備使用者控制選項的社交網站，使極端分子團體藉此預防或偵測滲透行為。例如，尋求成為團體成員的個人，可能須經過核准或透過邀請始可加入；因此，每個申請會員資格的個人，在獲准瀏覽團體網頁內容，或與其他成員參與論壇討論前，即可能經過徹底篩選。此外，許多社交網站允許團體監控論壇內容或其他網路活動。上述作為對於確保團體運作安全而言，實至關重要。

程式，後續則將其公布在數十個公開的檔案分享網站上。「聖戰者的秘密」支援多種先進加密演算法，其中甚至包括「進階加密標準」(Advanced Encryption Standard, AES)。美國政府於2001年核准以進階加密標準保護敏感的公眾資訊；美國國家安全局復於2003年核准使用該標準保護最高機密等級資訊。恐怖組織「真主黨」(Hezbollah) 極力讚揚諸如「聖戰者的秘密」等加密程式，可讓其成員在通訊時毋須擔憂其內容遭美國人破譯。

散布自如

恐怖分子組織亦在網際網路上散布其他應用程式。網際空間裏存在許多由極端分子維護的數位資料庫，內含許多可供組織成員逃避電子偵測的盜版市售程式。例如，某些應用程式可用來匿名上網，其他程式則可用來執行先進的「反電腦鑑識」(anti-forensic)工作，諸如以經過美國國防部核可之方式安全的刪除檔案，或是自某成員電腦中清除恐會留下網際網路瀏覽足跡的紀錄等。



實際破獲之非常規/非制式爆炸裝置。(Source: DoD)

在極端分子團體的心理戰方面，視訊應用程式也扮演了舉足輕重的角色。許多影片針對特定觀眾——如受過教育但遭褫奪公權者——進行「說服性傳播」(persuasive communications)，以宣揚該團體的意識形態。廣為流傳且有可能是不實資訊的宣傳活動，則可讓某恐怖分子組織藉此影響一些原本對其主張持同情立場——即使未直接認同——的第三方團體參與。蓋達相關運動組織現在影片中逐漸採用操英語的成員，藉此鎖定西方觀眾；影片亦

可能選在特定時機發布，俾儘可能造成最大影響。例如，一段事關非常規/非制式爆炸裝置攻擊的手機影片，或可在事件發生後立即公布，除吸引媒體關注外，另可能引發大眾後續關切；該影片可能因此強化民眾對於先前攻擊事件之情緒反應。一些恐怖分子團體曾利用YouTube散布有關其武力鬥爭的煽動性影片，例如斯里蘭卡的「泰米爾之虎解放組織」(Liberation Tigers of Tamil Eelam, LTTE)，即曾將1支有關其部隊訓練的影片張貼在YouTube上。

新興的攻擊能力

大部分在亞太地區活動的恐怖分子組織都已能發動「動能攻擊」，惟就如何以網路攻擊有效對抗數位目標部分，則仍處於懵懵懂懂的程度。不過本區內擁有世界級的頂尖電腦程式設計師，其對於如何開發網路攻擊工具可說是瞭若指掌。2000年被認為係網際網路史上破壞力最強的電腦蠕蟲之

一，亦即所謂的「愛蟲」(Love Bug)，就是由一些住在菲律賓的程式設計師所研發出來的。

恐怖分子團體使用的最基本網路攻擊技巧之一，係「分散式阻斷服務」(distributed denial-of-service)。攻擊者可租用專門提供電腦租借服務的網路罪犯電腦，或藉社交入口網站或權限管控式網路論壇，散發阻斷服務攻擊工具予同情者，俾

發動這類破壞性攻擊；前述工具可供其就世上任何數位目標進行大規模網路攻擊。伊斯蘭恐怖分子團體曾呼籲其追隨者從事反異教徒的「網路聖戰」(www.Jihad)；一些恐怖分子團體則已著手發展必要技能，俾於未來針對幾乎任何數位目標執行有效的網路攻擊。部分恐怖分子組織已意識到，網際網路可做為武器，且是一種十分

對抗網際網路極端主義的14種方法

由堪薩斯州李文沃斯堡(Fort Leavenworth)「外國軍事研究辦公室」(Foreign Military Studies Office)分析員湯馬斯(Timothy L. Thomas)彙編。

- 01 阻絕極端分子訊息。
- 02 就極端分子團體的弱點對其反擊。
- 03 強調極端分子組織的錯誤。
- 04 植入假的電子郵件訊息與網站貼文，期在極端分子組織間製造困惑、分歧和猜疑。
- 05 對於譴責恐怖分子暴力的重要神職人員，要宣揚其演說與論述。
- 06 找出恐怖分子重視的領域並加以破壞之。例如，推崇恐怖分子名譽的情感領域。
- 07 辨識、掌控，且甚至摧毀恐怖分子在網路上的活動領域。
- 08 利用擴獲的電腦硬碟學習如何發展反制訊息。

- 09 公布查獲的錄影帶，批露恐怖分子對孩童從事的洗腦課程，包括仇恨性卡通，以及極端分子為兒童設立之「營隊」等。
- 10 公布能彰顯極端分子組織內部士氣低落的信件。
- 11 判斷能使極端分子組織名譽掃地的事務，並戳破其在網路上的不實言論。
- 12 削弱極端分子行動在一般觀念，或神學意涵上代表的正當性，例如使用大規模毀滅性武器的道德正當性等。
- 13 說服極端主義之「支援網絡」不再幫助極端分子，並追究其責任。
- 14 研發可供辨識非傳統性武器與組件來源之技術系統。

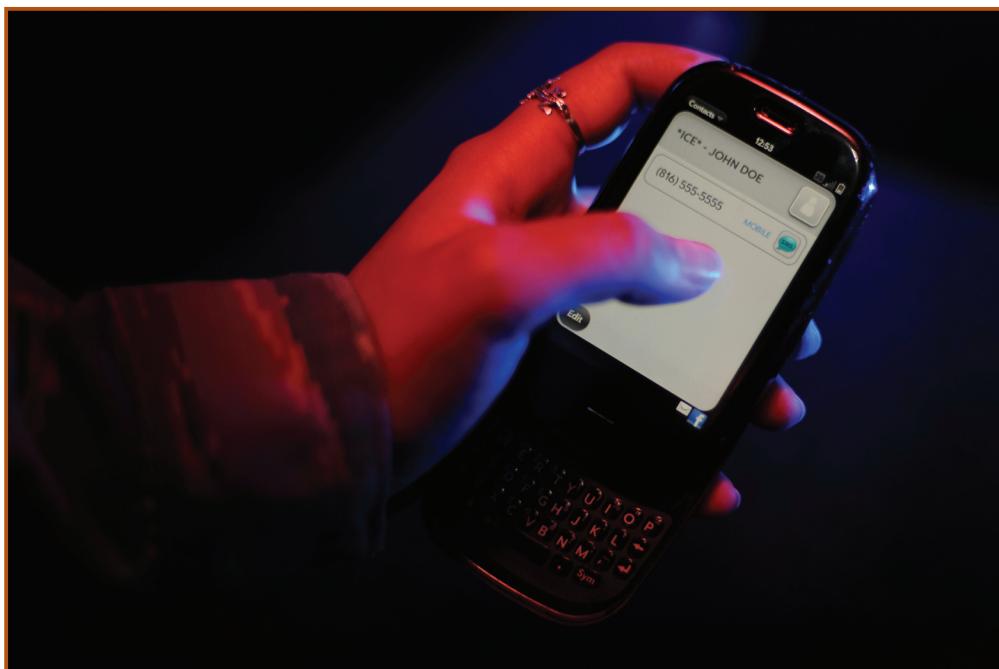
取材自Thomas T.於《資訊作戰領域》(IO Sphere)季刊2009年冬季號「對抗網際網路極端主義」(Countering Internet Extremism)乙文。



現代通訊技術一日千里，手機可搖控引爆非常規/非制式爆炸裝置。

(Source: US Army)

手機亦可遂行網路攻擊。 (Source: USAF)



精準、威力無窮的武器。

藉由提供一些替代面對面接觸及實體訓練營的應用程式和服務，網際網路有助於極端

分子組織宣揚其訴求。種族主

義或宗教民兵團體，更可輕易利用網際網路遂行成員招募、思想灌輸，以及訓練人員等工

作，以便在亞太地區內任一國家發動暴力攻擊。誠如孟買攻擊事件所示，暴力極端分子可利用網際網路規劃與協調恐怖行動的各項實際作為。此外，一些激進的極端分子團體更已開始研究以網際網路為武器，俾發動可對現實世界造成莫大災難之網路攻擊。隨著極端分子團體成員獲得更多技術知識，且科技日漸氾濫普及，這些團體將更廣泛運用網際網路。

值亞太地區網路極端分子日益猖獗之際，與其抗衡的力量亦須日趨茁壯且愈發精良。在一個開放、民主的社會裏，所有反制措施均須在力克恐怖主義卻不抑遏自由的考量下，戮力追求難以兼顧之平衡。

作者簡介

John Bumgarner是「美國網路影響社」(U.S. Cyber Consequences Unit)首席技術官員，並為許多著名媒體與刊物提供專業諮詢。

Reprint from *Asian Pacific Defense FORUM* with permission.