社群網路對作戰之影響
—— 以恐怖主義與反恐作戰為例

作者簡介

曾祥穎退役少將，陸官校41期、陸院74年班、戰院78年班、兵研所82年班；曾任連長、大隊長、指揮官、組長、高級教官、副師長、聯合防空主任、署長等職。

提　要

一、虛擬社群網路使「恐怖組織」得以「分子化」－化整為零－製造暴亂，或「極大化」－化零為整－攻城掠地，是伊斯蘭國能以小搏大，將其恐怖主義傳達至全球的主要媒介，對正規與非正規作戰，都產生了新的挑戰。

二、恐怖主義定義迄今仍無共識，但是都認為它是具有以武力、暴力或脅迫手段，使人們心生恐懼或使社會動亂，進而影響政府或社會以遂其政治目的或特定私心之意涵。

三、傳統的社群受到具體的法制規範與傳統的道德倫理的約束；虛擬的社群沒有具體的法制規範，道德與倫理觀念薄弱。

四、現行的軍隊「社群」各個系統依然相對的獨立，連結的程度有限；未來將成為如「循環之無端」的社群型態。

五、目前雖在正規作戰方面尚無戰例可資佐證，但是於恐怖主義與反恐怖主義

作戰的領域，雙方都積極利用現有的虛擬社群從事活動已是不爭的事實。

六、對虛擬社群的防制與運用，是網路戰的一環；美國主要手段是「堵」；中共採取以「堵」為主，「疏」為輔，部署了以新疆為核心的「三道防線」；以色列是以「疏」—「定點清除」，「堵」—「全民反恐」併重。

七、在戰略層次，可以參考美國、中共與以色列做法，決定適合國情的作為；在野略、戰術層次，各軍、兵種應以不同的想定，從嚴從難，反覆推演，以預為籌謀，方可因形未來於無窮。

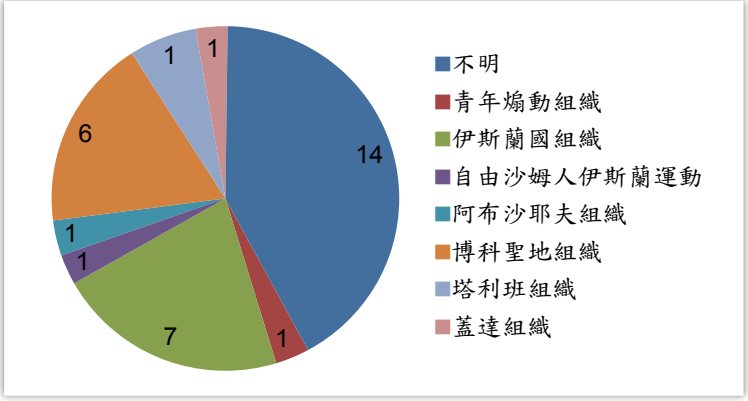
關鍵字：恐怖主義、虛擬社群、APP群組、反恐作戰

前　言

2011年，美軍將有生戰力全面撤出伊拉克與阿富汗，結束為期8年的反恐怖主義作戰。就理論而言，美軍完成任務撤軍回國，表示打擊恐怖活動已然收到預期成效，國際社會秩序一切都應將回歸到祥和安樂的常態；然而，恐怖活動並未終止，反有蔓延的趨勢，再加上美軍撤出後伊拉克權力的真空，族群與宗教派系的衝突以及敘利亞的動亂，使「伊斯蘭國」(the Islamic State of Iraq and the Syria ISIS)乘機坐大，以極盡殘暴之能事，旦夕間，儼然成為世界新的亂源。[1]不旋踵，不僅巴黎發生連環爆炸，其他各地恐怖攻擊事件亦層出不窮。[2](如圖一、二)這樣的事實告訴我們，未來的這類事件，仍將方興未艾，不可以掉以輕心。

不過，更值得我們深切探討的課題是：即使將所有恐怖事件的責任都歸咎於該

圖一　2015年10月恐怖攻擊統計圖

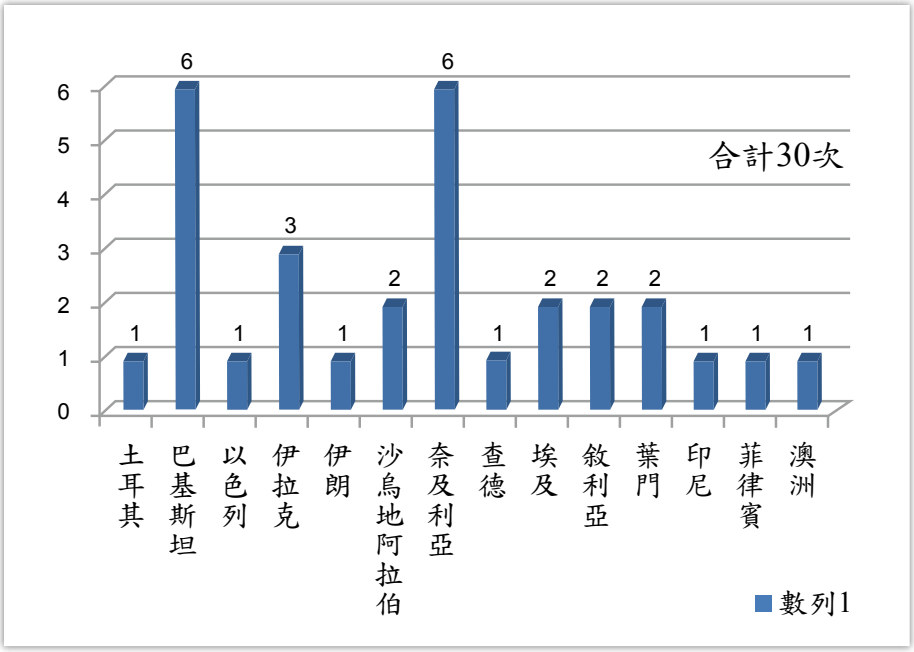


資料來源：中央警察大學恐怖主義研究中心。

1　該國之前身為伊拉克蓋達組織(AQI)，成員是以伊斯蘭教遜尼派瓦哈比派(Wahhabism)教徒為主，巴格達迪(Abu Bakr al-Baghdadi)奪權後指使教徒屢次公然在媒體前處決人質，以達其勒索之目的。柯伯恩(Patrick Cockburn)著；周詩婷、簡怡均、林佑柔、Sherry Chan等譯，《伊斯蘭國》(The Jihadis Return:ISIS and the New Sunni Uprising)，(新北市：好優文化，2104年11月)，頁13。

2　2015年12月初，查德、黎巴嫩與葉門相繼發生恐怖攻擊事件。

圖二　2015年10月遭受恐怖攻擊之國家及次數



資料來源：中央警察大學恐怖主義研究中心。

國的鼓動，那麼一個中東地區的准國家實體，[3]為何會擁有如此強大的能量，將恐怖活動遍及到全世界？何以伊斯蘭教的國家恐怖攻擊的事件對世局的影響遠大於其他地區？為何參與恐怖活動的分子，並不盡然來自「中東地區」，其中更不乏歐、美國籍的非阿拉伯裔人士？將這些不同文化背景的暴徒結合起來的「媒介」為何？這個「媒介」又將會對未來(正規與非正規)之作戰產生什麼樣的影響？

就以往的恐怖攻擊爆炸案觀察，在當前與未來的恐怖活動並不僅是以美、歐為對象，任何一個國家與地點都可能是下一個「受害者」。每一個事件當然都有其各自的目的，但是讓恐怖主義分子得以如此猖狂的「媒介」是什麼？作者以為主要的「媒介」便是各種免費「虛擬社群」的運作。

因為網際網路「虛擬社群」(virtual community)的蓬勃，[4]固然為人們帶來了無盡的便利，卻也同時為恐怖活動提供了極佳的掩護，使「恐怖組織」得以「分子化」－化整為零－製造暴亂，[5]或「極大化」－化零為整－攻城掠地，[6]甚至成立一個極權恐怖國家，恐怖分子這樣的分合作為對正規與非正規作戰，都產生了新的挑戰。孫子曰：「能因敵而變化者，勝。」換言之，我們如何因應這種變化對未來作戰的影響，必須要有「勝兵先勝」的準備，也是本文研究之目的。

「恐怖主義」的定義與類型

一、「恐怖主義」的定義

自從美國高舉「反恐怖主義作戰」之正義大纛以來，「恐怖主義」一詞，人人耳熟能詳，但是其中的定義卻始終莫衷一

3　國際間並不承認它是一個國家，而是一個武裝組織或准國家實體。周詩婷等譯，前揭書，頁41。

4　由網際網路使用者以各式各樣互動的網路社群構成的一種非實質的社會群體，例如「臉書」。

5　遠者可以溯至「911恐怖攻擊」，近者則為2015年底之「巴黎恐怖攻擊」。

6　遠者可以溯至1994年「第二次車臣戰爭」，近者則為2014年之伊斯蘭國「摩蘇爾之役」。

是，迄今仍無共識。原因便在於立場的不同－宗教信仰、意識型態、社會結構與國家利益－被某一個國家認定之「恐怖主義」，對另一個國家而言則可能是「生存手段」。[7]因此，就恐怖分子而言，顯然不會認同西方國家之定義，而是認為暴力與脅迫是「革命」的必要手段；更何況，截至目前為止，國際社會亦因文化與利益之差異，仍未能訂出客觀之定義。為有利研究，本文列舉國際社會、美國、學界以及中共與我國對此定義之討論，(如表一、二、三、四)做出歸納，以為以下論述之

表一　國際社會對恐怖主義之定義

時間	機構	定義
1798	法國革命法庭	足以令人心生恐怖的統制與制度。[8](恐怖主義之發端)
1937	國際聯盟	犯罪行為係用以對付一個國家，且企圖或計畫造成一種對特定之人員、團體或一般大眾之恐怖心理之狀態。
1999	聯合國	不論是否有政治、哲學、意識型態、種族、民族、宗教或是其它本質，凡企圖或計畫為其政治之目的，引起一種對大眾、團體或特定人員之恐怖狀態。
2004	聯合國	其企圖引起一般人民或是非戰鬥人員身體重傷害或死亡，以脅迫人民、政府或國際組織從事或是放棄所有行動為目的者。
2005	聯合國	凡旨在造成平民或非戰鬥人員死亡或嚴重傷害者，以脅迫一定之人民、某政府、或國際組織採取或取消特定作為為目的者，謂之。[9]
2011	維基百科	恐怖主義指一種為達成宗教，政治或意識形態上的目的，相關行動由非政府機構策動，故意攻擊非戰鬥人員(平民)或不顧其安危，蓄意製造恐慌的暴力行為的思想。

資料來源：terrorism.intlsecu.org/index.php/2010-05-13……/2010-05-13-04-06-22

表二　美國政府對恐怖主義之定義

單位	定義
國務院	係以國家團體或秘密代理人為非戰鬥人員，基於政治動機實施意圖影響公眾的預謀暴力。
聯邦調查局	非法使用武力或暴力對付平民或財產；以及恐嚇或脅迫政府以達成社會或政治之目標。
中央情報局	受由外國政府或組織支持與指揮，以對付外國、公共機構或政府的恐怖活動。
國防部	某革命組織為其政治或意識型態之目的，藉威脅或非法使用武力以暴力攻擊個人或資產，以恐嚇或脅迫社會。

資料來源：nccur.lib.nccu.edu.tw/bitstream/140.119/33840/6/98101006.pdf

表三　學界與智庫對恐怖主義之定義

學者	定義
詹姆士・洛奇	一種旨在影響政府政策而威脅群眾的有組織之暴力行為模式。
羅伯特・佛瑞德里蘭德	使用或威脅使用武力、暴力，以製造恐懼、威脅或強制氣氛以達其政治目的。[10]

註7～10　於下頁。

蘭德公司	使用實質或脅迫性暴力，製造恐懼氣氛，以誇大其力量與事業之重要性。[11]
布魯斯・霍夫曼	一種有目的之政治活動，旨在透過製造恐懼或透過事件之發展以遂其意願者。[12]
隆納・克林斯頓	為政治傳播目的使用或威脅使用暴力，旨在製造恐懼，迫使群眾、政府答應其政治訴求。
詹姆士・波蘭	有組織形式的暴力行為，透過使人民恐懼以影響政府之決策。
以色列傑菲戰略研究中心	任何被一非國家級組織領導以達成其政治目的者，均屬之。
理察・舒茲	威脅或使用超乎尋常的政治性暴力，以達成其既定之目標或目的。
C.J.M.德瑞克	一羣人長期或以威脅手段，並以政治動機或秘密之組織性暴力，攻擊民眾心理上之地標或重要場所為標的，以達成該羣人之要求。[13]

資料來源：nccur.lib.nccu.edu.tw/bitstream/140.119/33840/6/98101006.pdf

表四　我國與中共對恐怖主義之定義[14][15]

我國	言行或思想極端的激進分子，基於自我的民族意識、或宗教信仰、或政治理念，藉由暗殺、爆炸、綁架、縱火、劫持、恐嚇或武裝攻擊等手段，以宣示或企求達成其政治目的。[14]
中共	恐怖主義是實施者對非武裝人員有組織地使用暴力或以暴力相威脅，通過將一定的對象置於恐怖之中，來達到某種政治目的的行為。[15]

資料來源：參見註解12、13。

依據。

由以上三個領域以及我國與中共所列舉的定義可知，自1972年發生德國慕尼黑「黑色九月恐怖攻擊事件」後，[16]聯合國開始正式討論對抗恐怖主義以來，直至2005年，立場才似乎趨於一致；美國雖受恐怖主義為害最深，但是政府負責國家安全部門對此問題之看法因權責與地域之不

7　如伊斯蘭教基本教義派高喊之「聖戰」。所謂：「爾之毒藥，吾之蜜糖」是也。

8　丘臺峰，〈恐怖主義與反恐怖主義〉，(中央警察大學警政研究所，碩士論文，民國76年6月)，頁7。

9　UN Reform. un.org. 2005-03-21, May 7, 2011

10　Robert A. Friedlander, "Terrorism and the Law" Gaithersburg, MD: ICAP, 1981, p.3.

11　"RAND's Research on Terrorism" Santa Monica, California: RAND Cooperation, 1982, p.3.

12　張道宜等著，《圖解簡明世界局勢》，(臺北，易博士文化，2015年12月21日)，頁44。

13　http://www.pa-aware.org/what-is-terrorism/index.asp,visit 3/24/2005.

14　張平吾、丘臺峰，〈論恐怖主義及其起源與發展〉，《警政學報》，第21期，民81年7月，頁427。

15　www.baike.com/wiki/恐怖主義。

16　1972年9月5日巴勒斯坦武裝組織「黑色九月」闖入西德慕尼黑奧運會，襲擊以色列代表團，為首宗暴露在媒體前的恐怖攻擊事件。爾後以色列展開歷時九年餘的代名「上帝的復仇」行動，全球追殺「黑色九月」的恐怖分子。

同而有極大之差異；學界與智庫之定義雖眾說紛紜，亦各有千秋，並無定論，難以取得最大公約數，可供準繩。我國將恐怖分子定位為：「基於自我的民族意識、或宗教信仰、或政治理念，言行或思想極端的激進分子」；[17]中共則定位為「極左翼和極右翼的恐怖主義團體、極端的民族主義、種族分裂主義的組織和派別」，有影射「分離主義分子或團體」之意涵；[18]但是，定義的內涵仍不夠周延，[19]有極大之商榷餘地。

綜合以上各家之定義，雖然各有立論基礎，但是都不外包括了認為恐怖主義是以武力、暴力或脅迫手段，使人們心生恐懼或使社會動亂，進而影響政府或社會以遂其政治目的或特定私心之涵義。如果此認知為真，作者認為「維基百科」所陳述之內容較為宏觀，亦較易查索，比較符合上述要義以及實況，故爾，以其作為本文論述之依據。

二、「恐怖主義」的類型

既然恐怖主義的內涵是一連串企圖在人群中散播恐怖、驚慌與破壞之具有政治目的或特定私心的活動。那麼，在這種意識的作用下，其類型將是如何？本文依據學者的研究，對恐怖主義分類如下(如表五)：

在以上的分類中，我國的「反恐中心

表五　中外學者對恐怖主義之分類

保羅・威金森	以謀奪財務、財貨為主的罪犯恐怖主義、以宗教信仰而起的心理恐怖主義、以消滅敵人為主的戰爭恐怖主義、以暴力及恐懼手段獲取政治目的政治恐怖主義。[20]
菲特列・海格	追求神聖理想的十字軍型恐怖主義、以個人目的或利益的罪犯型恐怖主義、心理偏執的神經型恐怖主義。[21]
詹姆士・史密斯；威廉・湯瑪士	極左派的意識型態恐怖主義、種族與宗教合一的民族／分離型態恐怖主義、神聖淨化的宗教狂熱型態恐怖主義、極右派的種族優越型態恐怖主義、國際衝突後衍生的報復型態恐怖主義、國際犯罪組織的經濟型態恐怖主義。[22]
警大張中勇	民族主義的恐怖主義、意識型態的恐怖主義、宗教信仰的恐怖主義、單一議題的恐怖主義、國家支持的恐怖主義。
警大恐怖主義研究中心	生物、核武、毒品、航空、網路、海上等6種型態之恐怖主義。[23]
張道宜	宗教信仰的組織型恐怖主義、政治訴求的組織型恐怖主義、憤世嫉俗的「孤狼」型恐怖主義。[24]

資料來源：中央警察大學恐怖主義研究中心－恐怖主義分類。

17　我國將反恐中心設於中央警察大學，定義與內涵脫不了警備治安的範疇。

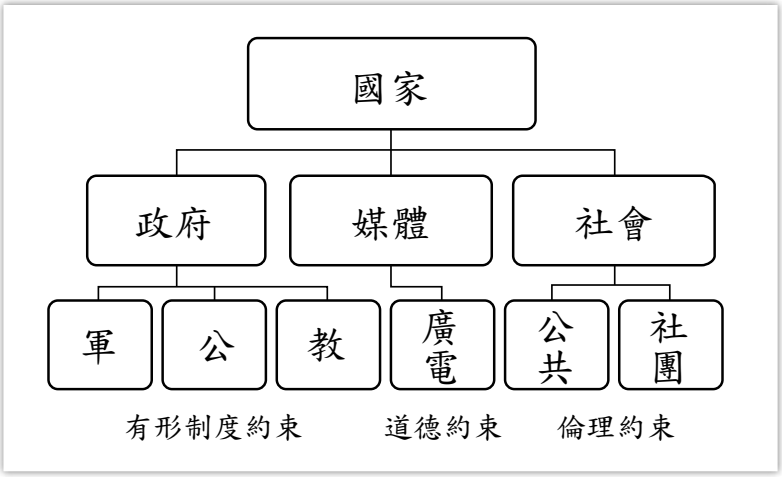
18　www.baike.com/wiki/恐怖主義，中共指的是「疆獨」、「藏獨」；「臺獨」只是個名詞，還沒有行動，而且並不排除以「戰爭」的方式解決紛爭，戰爭則是國與國之間無限暴力的行為。

19　我國與中共之定義均無法解釋「孤狼型」的恐怖攻擊－如美國波士頓馬拉松爆炸案－的動機。同時依據我國之定義，「太陽花運動」侵入立法院破壞公物與挾持輿論，脅迫公共安全的「政治勒索」行為都應屬於恐怖分子的行為。

20～24　於下頁。

」所作的分類雖然將網路恐怖主義納入考量，卻是著眼於便利執法及掌握預警的「警備治安」立場，有其侷限性。另一方面，部分學者的分類已經有些並不能符合近5年的現況，尤其是特定團體(ISIS)或組織(基地)以計畫性的暴力活動，或威脅使用暴力的方式，加諸無辜的群體或個人，希望能引起當地的恐懼以及世人的注意，以達到其政治、宗教或社會的訴求，成為21世紀以來的特有現象，亦應有修正之必要。因此，作者認為學者張道宜主張的未來的恐怖主義活動將以「宗教、政治」為主要原因，「孤狼」(lone wolf)型為次，較為符合當前發展之趨勢，而據以作為社群網路對作戰之影響分析之基礎。

圖三　傳統社群示意圖 ── 受有形制度與無形規範約束



資料來源：作者自製。

社群網路對作戰之影響

一、社群的定義

傳統上，社群(community)是指一個能彼此相互聯繫的團體(軍隊、村里)或人際關係(親朋、學術團體)網絡(如圖三)；[25]前者如宗親會，後者如基金會，其進出與存取都有一定的條件，具有主觀的實際性質，如果受到通信與交通限制，甚至是地域關係的守望相助的型態，[26]並且受到具體的法制規範與傳統的道德倫理的約束。

20世紀後期網際網路的演進，數位科技的進步與資訊通信平台的開放，電子郵件跨越了社群距離與實體的障礙；21世紀以來則是各種行動裝置為主體的雲端化的大數據網際網路，使「共同目的、信仰、資源、喜好、需求」等實質條件得以虛擬化，讓該虛擬社群的成員在不同的時間、

20 PaulWilkinson, "Political Terrorism"(London: MacMillan, 1976), pp. 32-35.

21 James Poland, "Understanding Terrorism: Group, Strategies and Responses"(Englewood Cliffs, N.J. : Prentice-Hall, 1988), p. 13.

22 《恐怖主義威脅與美國政府之因應》，(臺北：國防部史政編譯局，民國91年5月)，頁26。

23 係該中心著眼便於執法與掌握預警所作之分類，另有以行為者、實施之目的及思想淵源3種區分類型等，其內容與史密斯和湯瑪士主張概同，故不贅述。

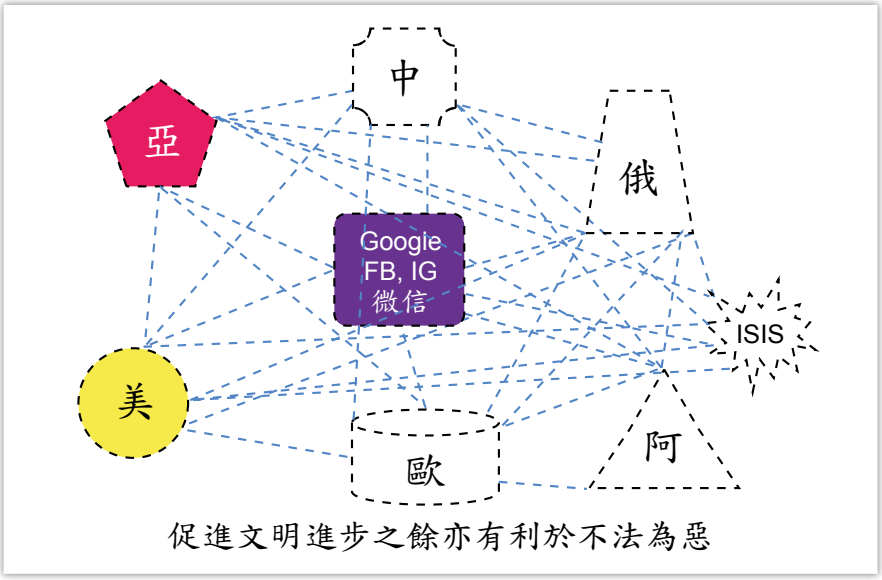
24 張道宜等著，《圖解簡明世界局勢》，頁45～47。

25 資料來源：作者自製。

26 前者如伊斯蘭教國家至今仍行使的氏族與部族的社會制度；後者如「部落格」、「維基百科」的圖文論述與觀點而聚集的「粉絲」(funs)。

地點於虛擬的公共空間聚集、連結，遂行資訊(想法、圖文)溝通或分享，隨時更新，每日以百億則以上計算。社群的涵義便跳脫了傳統的束縛，而有虛擬社群與「鄉民」概念的出現，[27]而且沒有具體的法制規範，道德與倫理觀念薄弱(如圖四)。[28]

圖四　虛擬社群示意圖 ── 任意連結難以約束



資料來源：作者自製。

2012年時，手機用戶已經超過50億，[29]行動裝置的數量仍有增無減，操作日益簡化。規模化的加速，數十億人每日都能夠透過即時反應的網路彼此相連，造成產品與理念的全球化，無限的連結互動之餘，我們等於同時生活在現實與虛擬的世界中，對某些群組而言，後者的地位猶勝於前者。

事實上，當2003年軍事上美軍開始推動「網狀化作戰」(Network Central Warfare NCW)概念的同時，越明年，Facebook、Twitter等社群媒體網站問世，網際網路的社群也逐漸由「部落格」(blog)的主題(如學術交流)型態，轉向「聊天室」(如拓展人脈)的交際型態；[30]至2007年夏，蘋果公司推出iphone智慧型手機以後，行動裝置的功能與便利性更強大，在雲端科技的支持下，進而成為社群成員主要交流工具；[31]2009年美軍成立「網路司令部」之同時，虛擬社群也由「個人專屬網頁」轉向「公共免費平台」。[32]其中蘊涵的能量之大，從2011年中東與北非地區的「阿拉伯之春」運動中，見其一斑。

因為網站的免費開放蘊涵了社群的價值與收益，每次對社群的「打卡」、「按

27　「鄉民」是指「愛湊熱鬧、跟著群眾起鬨」的人。社運人士將鄉民的網路特性用之於街頭政治，鄉民一詞從貶義與自嘲中，多了一層可褒可貶、具爭議性的意思。見維基百科。

28　資料來源：作者自製。

29　吳家恆、藍美貞、楊之瑜、鍾玉玨譯，《數位新時代》，(臺北，遠流出版社，2013年6月1日)，頁7。

30　Facebook、YouTube於2005年，Twitter於2006年，微信、line則至2011年問世。

31　當前手機的運算能力與速度已超過1975年時太空梭上電腦的1000萬倍。記憶體的總容量可以達到TB等級。

32　網路至極大化時，會因為客戶的廣告與線上交易手續費用的收益，產生自然的商業價值而變成免費的平台。如Facebook、Line、Twitter、Instragram(IG)等即是。

讚」、「線上購物」、「網路銀行」，都是某種「認同」與「幣值」，在觸控與滑動螢幕之中，人們的交往可謂「臉書存知己，推特若比鄰」。[33]雖然群組的活動99%的內容都是「垃圾」，但不可否認的是進入並參與虛擬社群，存取網路的認知與社群人脈為己用，已然成為大眾日常生活中，極其重要的一環。

時至今日，線上(online)的虛擬社群，將網際網路的本質從以往的知識圖文交流網(如Google、Yahoo、百度)為主，改變成現在的拓展影像社交網(Facebook、Twitter、Line、YouTube、微信)為重點，[34]在市場利益的驅使下，網路新技術不斷精進，APP的運用一再簡化，在這樣一個社群意識高漲的年代，「鄉民」隱身(宅)在電腦或行動裝置的後面，「一個動作、一個按鍵、一個回覆」，[35]就可以經由免費的網站借助群體的智慧，協助解決自己的問題，這種「萬事問社群」的「不勞而獲」現象，給我們帶來了無比的便利，但是對不同的群組產生不同的同儕效應與排他壓力，[36]也改變了我們在實體社會互動的方式。[37]

「水能載舟，亦能覆舟」。虛擬社群對社會而言：正面的效應是能夠整合社會資源，可以集群體的智慧為我們解決許多疑難雜症；負面的效應則因為「為惡者」可以藏身於暗處或以假名躲避道德的譴責與法律的約束，盜取別人的帳號，從事不法的詐騙、[38]偷竊、攻訐、甚至恐怖攻擊行為，[39]因此，社群網路是個陽光與友善的環境，也是一個充滿危險、詐欺、造假與「霸凌」(bullying)的地方。[40]

未來的社會與人們究竟會不會因為對網路的依賴，造成社群盲目從眾，失去獨立思考的能力，尚猶未可知；然而，在網路「存取」方便之餘，讓人們失去了打下深厚知識根基動力的後遺症候，現在卻已隱約可見。[41]

二、軍事上的傳統與虛擬社群

按照目前資訊科技進步的趨勢觀察，作者認為軍事上傳統社群(硬體裝備與組織制度)，已經跟不上虛擬社群(軟體建設與建軍思想)的腳步了。並且其差距幅度將隨著時間而更形擴大。

就軍事的「函數」而言，因為科技的演進，當代戰爭「空間、時間、戰力」的

33 吳妍儀譯，《雲端大腦時代》，(新北市，野人文化，2015年10月)，頁58～61。原文為「海內存知己，天涯若比鄰」。

34 陳重亨譯，《鍵盤參與時代來了》，(臺北，時報文化，2015年11月)，頁24～28。

35 林力敏譯，《社群人脈學》，(臺北，三采文化，2015年12月4日)，頁18～19。

36 如民國105年總統大選前「黃安與周子瑜事件」對輿論的影響力。

37 吳妍儀譯，《雲端大腦時代》，頁237。虛擬社群裡的人脈連結比實質人際關係來得密切。

38 如警方破獲兩岸詐騙集團以惡意程式使手機變肉機，實施詐財之例。

39 「賓拉登」即利用色情網站的掩護，策畫並發動「911恐怖攻擊」。

40 前者，如駭客盜取虛擬貨幣，挾個人隱私以牟利；後者，如以勒索軟體(ransomware)勒索、網路「人肉搜索」，版主覆蓋等。

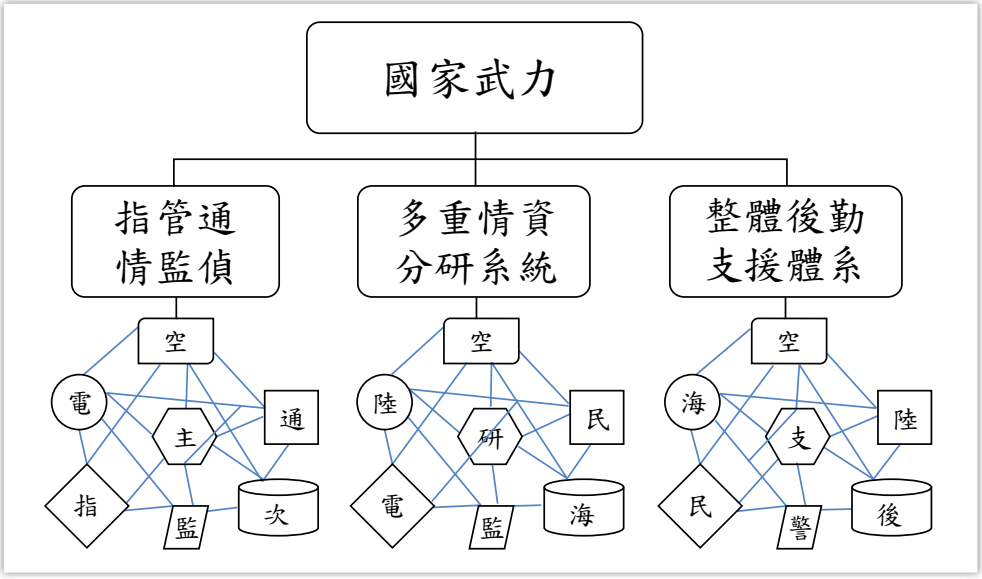
41 學術論文抄襲事件頻傳，即是一例。

發展，已然到了「空間無限擴大，時間急劇壓縮，戰力無遠弗屆」的地步；但是，未來武器系統載台物理性能的提升，已經到達臨界點，很難再有突破性的改進，應該是合理的論斷。因此，我們獲得「運籌帷幄之中，決勝千里之外」能力的相對代價，則是武器的系統日益複雜，裝備的使用期限，急遽縮短，有形戰力的建設甚至到達不堪負荷的地步。[42]

同時，各種武器載台的電子作戰系統，在「摩爾定律」－電腦功能愈來愈強，價格愈來愈便宜－與「梅特卡夫定律」－網路用戶愈來愈多，服務愈來愈廣－的作用下，[43]軍用規格的訂定與獲得，緩不濟急，難抵商用市場競爭的衝擊；商品現貨的規格比軍品規格來得多樣化，軍用網路「節點」的構建與覆蓋，也遠遠不如民間的「基地台」那麼普及。各國軍用的各軍、兵種「社群網路」的狀況(如圖五)，雖然在群組之內多已完成自動化或數位化，然而各個系統依然相對的獨立，連結的程度有限。

這種脫節的情形，在前瞻規劃地面作戰通信與資訊軟硬體的投資時，更形嚴重，往往還沒有部署，便已經落伍，業已成為軍事投資的一項挑戰。可以預期的是如果未來大規模戰爭發生的機率降低，軍事投資持續減少，軍規網路的體制和建設將可能進一步落後於民間發展和市場的競爭，無論未來採取何種作戰型態，民用網路與個人行動裝置在作戰上的份量將愈來愈

圖五　軍隊現行社群 ── 獨立相連



資料來源：作者自製。

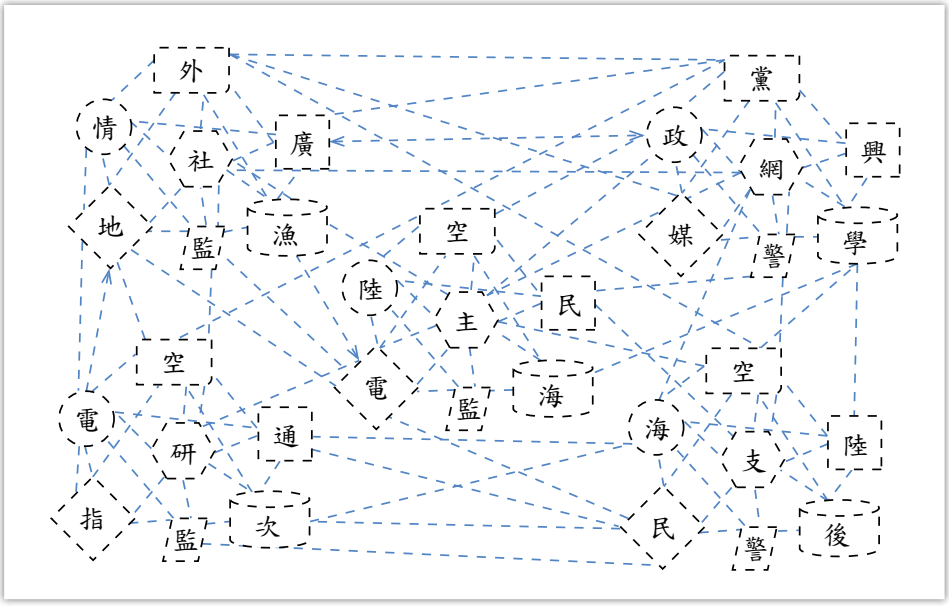
42　加拿大即對美製之F-35戰機價格過高，性能卻只比F-16略強而不滿。

43　前者為1965年，英特爾創辦人之一，摩爾(Gordon Moore)於美國電子學會35週年會中提出晶片會以2^N發展的理論。由60年代的大型主機、70年代的迷你電腦、80年代的個人電腦與工作站、90年代的網際網路與筆記簿、2000年的個人數位助理(PDA)與手機、2010年的智慧型手機、平板電腦發展的經驗，都證實此定律為真。依台積電張忠謀式之觀點認為未來10年仍可適用。後者則在1995年由乙太網路(Ethernet)協定設計者梅特卡夫(Robert Metcalf)提出「網路的效用性(價值)會隨著使用者數量的平方(N^2)成正比」之理論。

重(如圖六)。[44]

美軍預期在未來每位官兵都將成為網路的中繼器，需要連網的裝備可能多達12個。[45]如果這種預期為真，軍隊未來便將會無所不連，演變成如「循環之無端」的社群型態。《韓非子》說：「時移則事異，事異則備變」，因此，未來趨勢若是如此發展，各種虛擬社群網路對地面作戰之影響，[46]便不能不受到應有的重視。

圖六　軍隊未來社群 ── 無所不連



資料來源：作者自製。

三、虛擬社群網路對作戰的影響

古往今來，所有的戰爭都是過去、現在與未來知識與社會結構的綜合體現。戰爭離不開人類的生活型態與社會結構，數位化的社會帶來數位化的威脅，也使戰爭與威脅進入數位化。未來在「網狀化作戰」的建軍思想下，軍事用途的虛擬社群愈來愈普遍，與社會的虛擬社群的連結，也將愈來愈密切。雖然在正規作戰方面目前欠缺有力的戰例可資佐證，但是於恐怖主義與反恐怖主義作戰的領域，雙方都積極利用現有的虛擬社群從事活動；時至今日已是不爭的事實。甚至當前恐怖攻擊泛濫的現象，實來自於斯。

對前者而言；恐怖組織為了要讓恐怖攻擊事件「在不同的地區，同時發起攻擊」，以製造最大實質與心理破壞效果。就必須要有一個綿密組織的社群網絡，透過網際網路，秘密的召募、教育、訓練人員，選定目標、協調、交通與指揮恐怖攻擊全般事宜，[47]有利其將「烏合之眾組成聖戰士」，承擔自殺任務，在必要時還須能

44　2011年在阿富汗作戰之美海軍陸戰隊的AH-1W攻擊直升機駕駛員，捨棄機上內建的導航系統不用，反而用綁在膝上的ipad google地圖為之導航，即是一例。吳家恆、藍美貞、楊之瑜、鍾玉玨譯，《數位新時代》，頁254～256。

45　王文勇譯，《網路戰爭：下一個國安威脅及因應之道》，(臺北，國防部部長辦公室，民國103年9月)，頁95。

46　恐怖攻擊發生後，第一個趕赴現場的往往不是政府權責單位，而是媒體或由網路傳播。

47　英國記者羅素布蘭德(Russell Brand)說：「媒體不會報導革命」；恐怖分子則說：「APP會」。

夠貫徹執行。[48]以往電子郵件傳遞的速度與廣度受限，協調較難，且易被破獲；如今各種APP的「虛擬社群」則可以用「群組加密傳播」的方式，迅速傳遞所要之資訊至某一群組中特定的對象，在閱讀後自動銷毀，[49]其速度與效率均勝於以往，因此，其在恐怖攻擊中「組織、分工與執行」及擔任秘密通信與指揮的角色，有日益加重的趨勢。

這種情形在如英、美這類公民意識警醒，社會治安良好的國家，或中共對網路管制嚴密的社會，都避免不了恐怖分子攻擊的事件；更何況維持治安能力薄弱的政府或混亂的社會。從另外一個角度來看，恐怖分子透過「虛擬社群」掌握了主動，而能夠得以一再得逞；除了造成國際社會的不安與恐懼外，對某些國家而言，恐怖攻擊肆意殺戮的結果，人民生活在亂世，國家則日益衰敗。

以伊拉克為例，ISIS武裝奪得馬利基政權後兩年，其境內傷亡人數之多，令人側目(如表六)，敘利亞更是發生龐大的難民潮，給歐洲各國治安與經濟帶來極大的壓力。[50]

在伊斯蘭教國家，恐怖分子亦得利於美軍留在中亞及中東地區大量流入黑市的廢棄軍火，有了暢通的溝通管道與處處隨手可得的軍火，[51]甚至裝甲車輛，使得恐怖分子可以不顧人民的安危，不必自製爆裂物(IED)，隨時隨地在他們所望的地方發起攻擊。以圖一我國對2015年10月恐怖攻擊統計為例，在33次的攻擊中，ISIS為7次，亦即不到1/4；西北非的「博科聖地組織」(Boko Haram)也有6次，「塔利班」與「基地組織」次數合計則僅有3次，來源不明的卻有14次之多，這樣的結果顯然與一般人想像的有極大的出入。

再以圖二的2015年10月遭受恐怖攻擊之國家及次數統計分析，這些事件之所以能夠「如期如質」得逞的背後，有很大的原因就在於虛擬社群的構連與運用，被用

表六　2014～15年伊拉克受恐怖攻擊死傷人數統計表

年度	死亡	輕重傷	合計	說明
2014	12,282	23,123	35,045	武裝奪權
2015	7,515	14,855	22,370	-12,675
2015年12月	980(506/474)	1,244(867/377)	2,224	(平民／伊軍)

資料來源：〈伊拉克去年暴力衝突，奪7,500人命〉，加拿大明報電子報，2016.01.02。

48　恐怖分子在實施攻擊時，通常會有現場指揮官、「烈士」、自殺炸彈客與督戰人員，如果有人臨陣怯場或猶疑時，後者即將其擊斃，並遙控引爆炸彈客身上的自殺炸彈。見Stanley McChrystal. "Team of Tams"(Penguin Random House Company. N.Y.2015.) pp 13～17.

49　如運用Telegram「閱後付丙」社群軟體。

50　有恐怖分子隨難民混入歐洲，難民的安排給政府造成極大的困擾。

51　ISIS的武器主要來自繳獲的政府軍的輕重裝備，並以社群網路整合其後勤支援問題。見王友龍，《你所不知道的IS》，(臺北，城邦文化，2015年7月)，頁107～114。

之於肆意為惡，淪為奪權牟利的工具。在已知的30次的攻擊中至少有19次是發生在信仰伊斯蘭教的國家(8個)，其餘多在中東、非洲等久經烽火的國家。而且據統計受害最深的5國依序為伊拉克、阿富汗、奈及利亞、巴基斯坦與敘利亞，[52]雖然這些國家每年因武裝暴力而死傷慘重，居民無家可歸，但是除了敘利亞的難民蜂擁至歐洲，造成輿論壓力迫使政府不得不處理之外，其餘都沒有獲得西方媒體的重視，也就相對不為人知，任其為惡。

至於社群運用在反恐怖主義方面；遠者如「2011年5月2日深夜，美國海軍的「海豹部隊」以「海神之矛」(Operation Neptune Spear)代名，執行對「基地組織」首腦賓拉登(Osama bin Laden)百里奔襲的獵殺行動，就是歸功於美軍能從大量的數據資料中，找到了他所在的社群，掌握了他行蹤規律後的縝密計畫與演練，經過白宮的批准與即時視訊督導，「其疾如風，侵略如火」，達成任務迅速脫離。如果沒有大數據與雲端網路的支持，美軍將很難掌握這種「稍縱即逝」的戰機。賓拉登利用色情網站的掩護發起「911恐怖攻擊」，卻也因其所在的社群被美國掌握而被擊斃，可以說他是典型的「成也社群，敗也社群」。[53]

近者如2015年11月13日夜間，法國的「巴黎爆炸案」；在受到攻擊前一個月，警方已接獲來自以色列「法國本土將遭到襲擊」的預警，但卻未對ISIS的宗教宣傳與恐嚇做出適當的因應與準備。事發之後，又喪失先機，後來依據恐怖分子遺留現場的PS4遊戲機，5日之後由PS網路反向偵查語音通信，[54]追出主謀藏身之處，才實施攻堅反制，擊斃首惡阿巴烏德(AbdelhamidAbaaoud)，逮捕其黨羽，[55]方使事件告一段落。

值得注意的是恐怖分子對社群網路的運用，大多透過各種偽裝與掩護，都極盡精簡與迅速之能事，以減少或躲避各國情報與安全部門的攔截與制裁。執行恐怖攻擊時，也能分合自如，而且成功的機率甚高，防不勝防。但是更令人擔憂的是ISIS積極經營社群媒體，血腥鎮壓的手段，[56]說明了他們將虛擬社群網路之運用方式，由暗轉明，由善轉惡，這種利用社群輸出「恐怖革命」的轉變，必然將對未來的無形戰爭－網路安全與攻防－產生了極大的影響。

ISIS對虛擬社群之運用

52 〈全球恐怖活動指數裡的現實〉http://www.thinkingtaiwan.com/content/4869。

53 在突擊直前一名當地居民阿薩(Sohaib Athar)便在「推特」上發出了此一消息，可見網際網路虛擬社群的威力有多大。

54 PS4具有無線通話功能，這種較低階的科技被注意的可能性亦較低，有時比傳統的加密電話、簡訊與郵件更為安全。〈巴黎爆炸前，恐怖分子如何利用科技產品溝通？居然可能是PS4!〉http://www.bnext.com.tw/ext_rss/view/id/1076188.

55 該次突擊中被擊斃之一名女性恐怖分子身上綁著炸彈，自爆身亡。

56 ISIS至少經營4個媒體通路，善於運用twitter、影片與手機APP從事宣傳與招募。王友龍，《你所不知道的IS》，頁123。

我們從每次恐怖攻擊爆炸案件發生後，都不乏有恐怖組織透過媒體自行承認之事實觀察，恐怖分子利用社群從事非法活動其實早已有之，只是以往的動作都沒有像ISIS公然有組織的經營與有系統的宣傳來得大。這些透過特定的管道發布的例證當然有真有假，可以預期的是只要有開放的網路，未來就會有恐怖分子藏身其中，伺機而動，不過，恐怖分子利用社群媒體進行宣傳固然獲得了極大的成效，但同樣的也有「缺失」，例如，ISIS被美國西點軍校反恐中心截獲的「網路安全作業手冊」，[57]便給了各方研擬反制措施產生一定的啟示。[58]

ISIS堪稱為至今最會用運用如Facebook、IG、Twitter、WhatsApp等知名網路社群，以雙重加密的帳號發布消息，運用電腦和手機進行「比特幣」(Bitcoin)融資，[59]實施恐怖行銷與召募的組織。以被其主要利用的Twitter社群網路為例，[60]依據美國的調查在2014年9～12月間，該組織有46,000個使用不同語言的Twitter帳號。[61]2016年初，歐巴馬總統要求：「不希望網路工具和技術被用來幫助及教唆恐怖分子」。[62]美國各大社群網站系統配合國家政策，紛紛刪除與此有關的帳號，以遏止ISIS利用社群網站及加密技術在美國的不法活動，其中Twitter所刪除「煽動對他人傷害」的帳號，即高達125,000個。[63]此舉雖然可以收一時之效，但是卻擋不住他們以新的帳號隱匿身分重新登入；並自行開發手機APP供人下載，[64]採取大量即時發送的策略，意在帳號被停權前，將文宣內容的「推文」散播出去，[65]以爭取外界支持並吸收潛在的「聖戰士」。因此，儘管受到了許多限制，恐怖主義的言論一直未能從Twitter網站絕跡，這也是不爭的事實。[66]

57 美國西點軍校反恐中心從ISIS論壇中截獲一份長達34頁的社群網路教學手冊。http://buzzorange.com/techorange/2015/11/24/isis-security-manuel.

58 如不以有GPS定位之手機上傳影片或影像，以免被追蹤定位。

59 2009年1月3日日本的「中本聰」氏，發明類似電子郵件「電子現金」的「比特幣」問世；以對等網路中種子檔案的網路協定，透過電子貨幣交易渠道，兌換當地的現金或金幣；也可以直接購買物品和服務，是目前使用最為廣的一種電子虛擬貨幣，因還沒有明確的法律規範和保障，恐怖分子可利用此管道進行融資交易。主要資金來源為沙烏地阿拉伯與卡達。柯伯恩著；周詩婷等譯，《伊斯蘭國》，頁100～104。

60 2014年ISIS攻占伊拉克摩蘇爾的前夕，即運用Twitter網站實施宣傳，並報導即時戰況。

61 林仟懿，〈推特改規定禁暴力，IS可能難再利用〉，臺北，中央社，民國105年1月16日。

62 陳韋廷，〈加強網路反恐，歐巴馬求助矽谷〉，臺北，聯合報，民國105年1月10日，A12版。

63 傅莞淇，〈反制社群網站恐怖主義歪風推特刪除逾12萬個「伊斯蘭國」帳號〉，臺北，風傳媒，民國105年2月6日。

64 ISIS開發了「黎明報喜」APP，下載後用戶即會收到ISIS的即時訊息。張穎綺譯，《ISIS大解密》，(新北市，立緒文化，民國104年3月)，頁146～152。

65 同上註。

66 Facebook則在愛爾蘭都柏林有專責部門24小時監測敘利亞與伊拉克境內的帳號。

恐怖分子運用虛擬社群除了宗教、政治宣傳與「實質詐」之外，對國際社會未來危害最大的是將具有暴力傾向的「聖戰士」，隱伏到全世界，伺機而動。在俄羅斯的兩次車臣戰爭時，外來的戰士多半與車臣的淵源較深，人數也不多。[67]據悉2015年初參與ISIS陣營作戰的外籍人士，多達80餘國，人數超過2萬人，[68]姑且不論是否有誇大之虞，這些參戰的恐怖分子將實戰經驗帶回國內之後，會擴散到全世界，並演化成類似「死間」性質的「沉睡細胞」，[69]平時融入當地社會，生活舉止與常人無異，必要時則依據恐怖組織指令或透過社群網路的串聯，發動類似「911恐怖攻擊」或「巴黎連環爆炸案」等事件。[70]根據美國電腦專家烏斯曼尼(Zeeshanul-Hassan Usmani)的估計：美國和歐洲等地約有7萬人「隨時激進化」，對各國而言都是安全上的嚴重威脅的因子，其中又以法國的2.7萬人最為嚴重。[71]

從以上的分析中，現在的社群媒體已經與我們的生活密不可分，更已經被ISIS運用到「正規」作戰方面。虛擬社群運用得當，可以使我們能夠「得道多助」；但是被恐怖分子污染與濫用的結果，不但暴力的本質加劇，甚至有能力登堂入室的進入到我們的影視系統、行動裝置、甚至連到心智未熟的孩童與學生的手機中，直接危害到我們的安危，因此，如何防範社群為惡於未然，已是刻不容緩的工作，這是我們應有的認知。

對虛擬社群的防制與運用

自古以來，對於任何對社會發展有重大影響力的事物，因應之道不外運用「疏堵」兩字而已。雖然恐怖分子並未與伊斯蘭教徒劃上等號，ISIS和其他恐怖組織利用虛擬社群網路的作為，使得各國增加了對他們活動的戒心，則是可以想像得到的後果。茲以美國、中共和以色列為例，分析如下：

在美國方面，主要的手段是「堵」。除了以空中武力攻擊恐怖組織，由總統出面對各大型社群網路與媒體進行道德關說，要求配合國家政策，並獲得善意回應之外；[72]國土安全部門對出入境的審核更趨嚴密，並主張要擴大虛擬社群內容的審查，以大數據對特定的社群進行監控。[73]這種假「國家利益之名」行之的作為，即使略過了法律的層面，頂住了輿論的壓力，但還是難以收效，因為當恐怖分子找到想

67 曾祥穎譯，《車臣戰爭：1994～2000城鎮戰之經驗教訓》，(臺北，國防部部長辦公室，民國95年11月)，頁79～81。外籍人士來自沙烏地阿拉伯、約旦、中共、埃及、馬來西亞與巴勒斯坦。

68 王友龍，《你所不知道的IS》，頁148～150。

69 同註68，頁175～180。

70 巴黎爆炸案中，在巴塔克蘭劇場被擊斃的恐怖分子便具有法國公民身分。

71 〈誰是潛在恐怖分子？大數據告訴你：有錢、青年、少自拍〉，http://www.hk01.com/。

72 Facebook表示在網站上偵測到相關可疑活動，會向執法部門通報。

73 〈擴大審查社群媒體貼文，美國反恐機構：作為簽證審核〉，http://www.ettoday.net/news/20151216。

招募的人，他們便會將對話轉向加密的APP聊天室，只要有心，美國情治部門是很難追蹤這些訊息的。[74]在無法完全杜絕內部潛在威脅發展的狀況下，在「問題不是恐怖攻擊是否會發生，而是何時何地會發生」的預期心理下，因此，加強入境管理與安全檢查，便成為美國的第一道防線，在ISIS未消除前，這種情形應該不致於有太大的改變。

在中共方面，其反恐戰略係採取以「堵」為主，「疏」為輔的「三道防線」部署。[75]前者中共認為西北地區(新疆)與中亞比鄰，為恐怖主義組織滲透的重點地區；因為「民族分裂主義和宗教極端主義是國際恐怖主義的主流理論，後者則為前二者達成其意圖與目的之基本手段」；[76]故爾，中共的「維穩」一直是以防範「疆獨」(或東突厥)的活動為核心。並且中共當局發現至少曾有約300名的「東突」分子從雲南、廣西偷渡出境，經馬來西亞、土耳其至敘利亞，加入ISIS並接受訓練。[77]這些人如再以偷渡的方式潛回國內，必將是「維穩」的一大隱憂，因此，中共認為「『東突』暴力恐怖活動威脅升級」，[78]要求武警「完善以執勤處突和反恐維穩為主體的力量體系，提高以信息化條件下執勤處突能力」，[79]同時，對新疆地區嚴格管制資訊的傳播，[80]強化管理手機相關之電子產品。[81]情報部門則藉法國政府對恐怖攻擊情報掌握不實，以「中國防火長城」(Great Firewall of China)來強化對大陸社群媒體之監控。[82]以Google為例，自進入大陸後，因該公司不願配合中共監督，2010年決定退出中國市場，至2014年5月中共對其全面封鎖，迄今為止並未開放。另外，包括Facebook、Twitter、YouTube等外國社群網站都不能進入中國領土，大陸地區無法直接登入Twitter等網路，必須透過VPN連線，以便接受的檢查，[83]可見其「堵」的手段有多麼的嚴厲。

74 自2011年以來，約有48名美國人躲過當局監控，前往加入伊斯蘭國。〈如何監控境內IS分子美國很頭大〉，2015-12-07 09:56聯合報電子版。

75 蔡裕明，〈中國大陸近期因應恐怖攻擊之政策佈局簡析〉，www.mac.gov.tw/public/Attachment/61716504715.pdf

76 房功利，《新中國鞏固國防的理論與實踐》，(北京，社會科學文獻出版社，2014年11月)，頁274。

77 同註75。

78 《2015年中國的軍事戰略》，〈一、國家安全形勢〉

79 《2015年中國的軍事戰略》，〈四、軍事力量建設發展〉

80 2009年7月5日，新疆烏魯木齊市發生暴亂，中共即分別封鎖Twitter、Facebook等社群網路。2011年中東「茉莉花革命」中國大陸網友企圖以社群網路串聯，中共立即封鎖Google。

81 同註75。

82 防火長城的作用主要是監控國際閘道器上的通訊，對認為不符合中共官方要求的傳輸內容，進行干擾、阻斷、遮蔽。又稱「金盾工程」。

83 中共對關鍵字審查之執行不遺餘力，對內用微信，對外用WeChat.

其次，則是完成相關之立法，並於刑法增修「懲治外國恐怖主義參戰人員」條文，做為執法的依據。第三道防線為利用「上海合作組織」與美國舉行「網路反恐演習」；並與東協、俄羅斯實施聯合打擊恐怖主義演練。[84]

至於「疏」的措施，中共除了教育部門要求各級學校「著力運用微博、微信等社群網路」，「網上網下」宣導愛國主義之外，[85]提出結合民眾實施「人民戰爭，全民反恐」的概念，廣張耳目，[86]檢舉不法，甚至雇用社群工作人員以「獎勵」的方式，做政令宣導或制止敏感的「推文、貼圖」，作為反制恐怖主義之滲透與破壞的手段。[87]

以色列是全球最具反制恐怖攻擊經驗方面的國家。其反恐戰略係採取以「疏」、「堵」併重；早在1948年便制定了「預防恐怖主義條例」，明訂各種規範，建立法源基礎。數十年來面對巴勒斯坦哈瑪斯(Hamas)組織的恐怖攻擊，一直秉持「絕不妥協，速戰速決，以牙還牙」的態度，「定點清除」危害國家安全的個人或組織，所有的報復性攻擊，都稱為反恐怖行動，[88]雖然屢遭國際譴責，依然不改其初衷，也使得國際間不會誤解該國的立場，迫使恐怖分子必須考量實施恐怖攻擊後，以色列無情的報復，這樣「疏導」的作為反而有助於該國國家安全與社會治安之維護。

更重要的是在長期處在恐怖攻擊的威脅下，以色列人民經過戰爭的洗禮與教育，已經做到了「反恐攻擊，人人有責」地步。[89]目前除了以武力堅決反制任何恐怖攻擊外，以色列認為虛擬的社群網路的領域，才是反恐作戰能否制敵機先的關鍵。[90]因此不斷強化網路管控與偵查，運用雲端與大數據技術，對阿拉伯世界虛擬社群圖文視訊資料，實施分析與比對，以提高阻絕恐怖攻擊發生的機率。[91]

就以上3個國家而言，因為國情的不同，對虛擬社群的防制與運用，手段亦各自不同。國家幅員愈大，社會愈開放，禁止虛擬社群用之於為惡就愈困難；美國的監控已多次釀成外交問題，未來應仍將維持其一貫之作法，甚至要求開放「後門」以利其掌握各種社群之動態。中共則盡力將局勢控制在新疆一帶，並極力管制社群媒體，未來國際各大型社群，若不能接受中共官方的審查，進入大陸市

84 同註74。

85 〈陸下令各校用網路宣導愛國主義〉，http://www.cna.com.tw/news/acn/201602090218-1.aspx。

86 北京青年報：繼「朝陽群眾」被指「世界第五大王牌情報組織」後，北京「西城大媽」亦被稱為京城反恐維穩的「王牌情報網」，www.worldjournal.com/3333727/article。

87 章昌文譯，〈網路治國的多面向本質〉，國防譯粹，民國105年2月，頁13。

88 蔡東杰，〈以色列反恐作為，以牙還牙不妥協〉，青年日報，民國98年11月5日，第7版。

89 在當地隨身行李不可亂放是常識，任何一個無人看管的包裹都會即時通報當局處理。

90 〈以色列如何對付大規模的恐怖襲擊－決戰攻擊之前〉，http://www.thinkingtaiwan.com/content/4883。

91 同註90。

場必定須經過極大的考驗，但是相對的也減輕了恐怖分子對中共宣傳的效果。以色列的各種作為堪稱典範，但那是人民在長期烽火之下所產生的共識，願意為安全作出一定的犧牲，也未必見得適用於我國國情。

結論(代建議)

綜合以上所述，我們知道網路戰爭並非是國安與軍隊的專責，而是全民都須面對的事實。恐怖分子組織所在地區雖然網路的設施不如西方社會，不過由於資訊科技的演進，多媒體社群網站的出現，讓恐怖組織有了以小搏大的槓桿，進而成為傳播恐怖主義重要媒介。並將虛擬社群「利他」的善意因其特定因素而用之於「為惡」，也使人們警覺到虛擬社群未來在作戰上能夠產生極大的作用。

以美軍而言，雖然目前美軍僅在中東地區投入少數的特種部隊，協助當地對抗恐怖主義，無法瞭解到美軍對社群的實際運用情形，但是從美軍認為「社群已成為未來公開性情報蒐集、分析及歸納重大事件之關鍵工具，從社群媒體獲取軍事情報是長期預警評估重要的一環」，[92]要求與其他的情報來源同樣的重視。並且除觀念的改變外，採用高薪與津貼的手段留用網路部隊的人才，以因應未來的挑戰。

我軍官兵已習於數位化和智慧化的社會生活環境，從今年臺南地震救災中，官兵對「臉書」的運用情形觀察，我們可便可知我們已經不能脫離虛擬社群的羈絆，並會將這些習性帶到戰場。由於以APP開設社群組成不同的社群網站，非常方便，只要現有的網路體系不被澈底破壞，有太陽能與行動電源，人人都可做為通信的節點，是不爭的事實。因此，可以預期戰時即便建制的體系不被敵方或他方阻塞、制壓或摧毀，各級部隊也會將「臉書」從平時以政令文宣與部隊安全為主的經驗，轉為情報通信與指揮管制的角色，以有利其部隊的掌握與任務之達成，乃是必然的發展。

因此，我們必須認知到：面對這樣虛擬扁平、無所不連與無遠弗屆的社群網路所組成的智慧化社會，無論未來面臨的狀況是什麼，都會有網路的成份夾雜其中，換句話說，我們要從廣義的角度來將虛擬社群看待為網路戰爭中之一環。

面對多樣化的未來，曾文正公主張：「軍旅之事，謹慎為先；戰陣之事，講習為上」。作者以為在戰略與國安的層次，我們可以參考美國、中共與以色列的做法，依據國情擬定適當作為；但是在野略及戰術的層次，則必須各軍、兵種以不同的想定，甚至以不可能的角度從嚴從難，實施推演，以預為籌謀，講求因勢利導，方可因形未來於無窮。

92　黃文啟譯，〈從社群媒體獲取軍事情報〉，國防譯粹，民國105年2月，頁50～55。