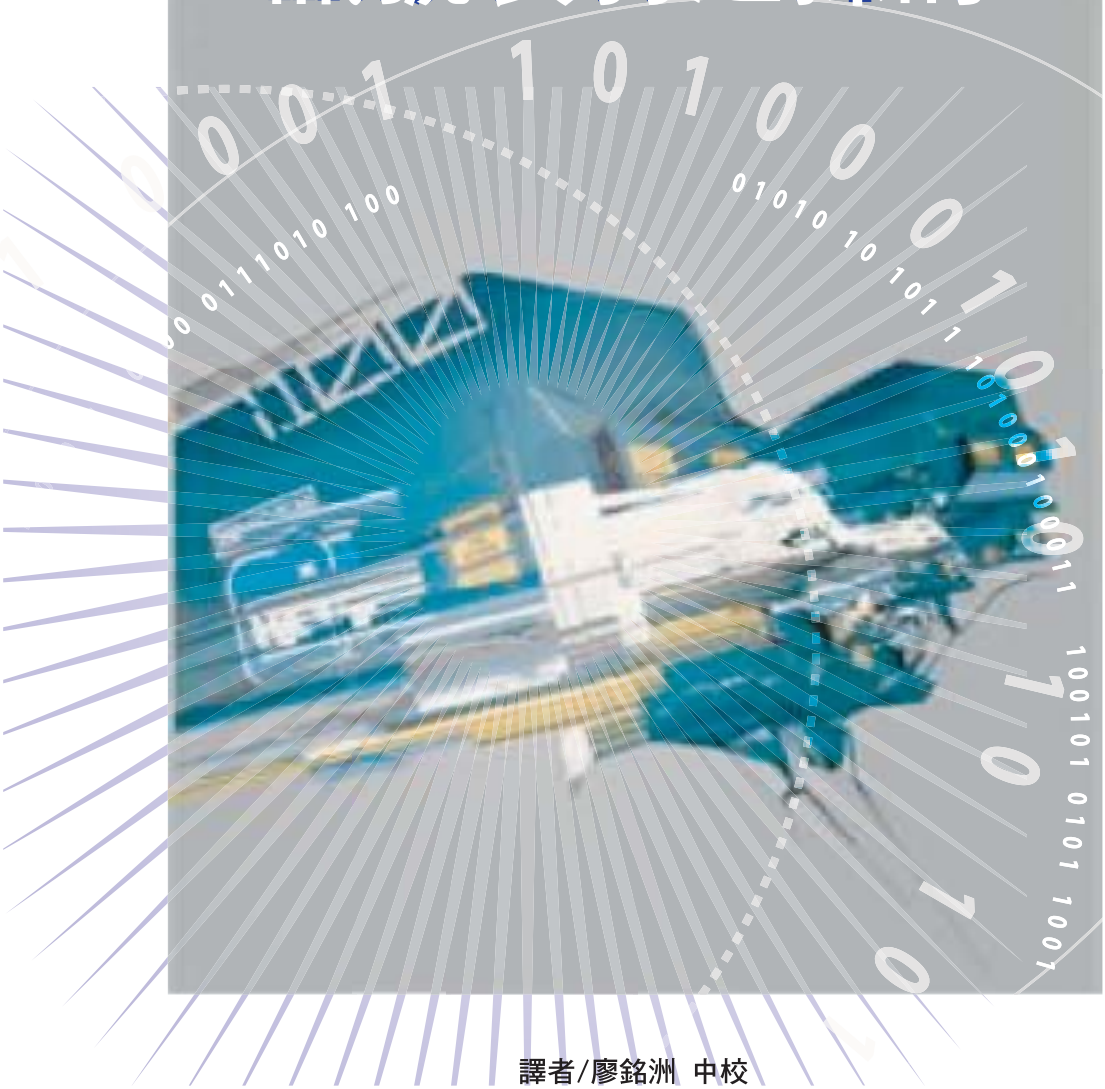
通信網路在城鎮地區訊號衰弱之探討



譯者/廖銘洲 中校

取材/2004年8月電子防護期刊

(Ted McKenna, "Hearing Impaired," The Journal of Electronic Defense, August 2004)

提要

一、城鎮地區複雜的環境，使得軍隊的通信變得更為困難，軍隊為求生存則必須學會監聽而非阻斷民用通信網路。

二、電腦運算能力與應用軟體開發的能力大幅度的成長，加快了戰場變革的步調。也就是說，在電腦科技的觸發之下，擴大了戰場不對稱的現象，使得強者變得更強，弱者顯得更弱。

前言

國軍的防衛作戰構想是以「資電先導、遏制超限、聯合制空、制海，確保地面安全，擊滅犯敵」之指導，建立「小而精、反應快、效率高」之精準打擊戰力，以達成有效嚇阻之目標①。其成功的基石仍在於建構一個安全、穩定而有效率的通資系統爲溝通的平台。

由於台灣地狹人稠，城鄉分野並不明顯，而城鎮地區普遍的特性爲主要街道塞滿車輛、建物比鄰與電力、電纜線密布，這些因素均不利於無線電波的傳遞。除此之外，各式民用通信系統日益蓬勃、資訊網路遍布全島，假以時日民用的通資技術將凌駕軍用通資技術之上。國軍應如何克服城鎮地區複雜的環境對軍用通信網路造成的困擾，以及如何有效地整合民用通信網路技術，爲本文探討的重點。

在過去我們習慣以「套用戰爭規則後，而形成生命威脅的特殊區域」來界定戰場涵蓋的範疇。但就目前發生內戰的海地與獅子山共和國爲例，這兩個國家的平民被迫在人民反抗軍與政府正規維和部隊的戰火夾縫中生存。維和部隊期望能夠不受限地運用各種手段來完成任務，但事與願違，爲了避免引起人民反感，必須盡可能地減少摧毀反抗軍的有生力量。另外，在城鎮地區作戰的過程中，所有的車輛、電力/電纜線、建築物再加上慌亂的居民等，勢必會癱瘓部隊的耳目－通信。

一旦維和部隊進入城鎮地區後立刻會發現由於環境的雜訊與干擾的問題十分嚴重，將導致無線電系統變得相當不可靠而使部隊指揮與管制不易，然而反抗軍卻能僞裝成平民百姓的樣子或是躲在一些令人料想不到的角落，毫不費力地尋找穿著制服的士兵，讓維和部隊成爲非常顯著的目標而吃足了苦頭。

雖然反抗軍所使用的通信設備並未到達軍規的等級，卻與正規部隊使用相同的通信技術，例如行動電話與基地台、衛星、有線電等民用或商用通信網路。因此，維和部隊需同時執行監聽(interception)與人爲干擾(jamming)時相對地提高了任務的困難性。隨著民用通信網路的技術日益發達，再加上城鎮地區惡劣的通信環境，均屬於新型態戰場的一環。如何在城鎮地區滿足部隊通信需求的技巧，是軍隊各級幕僚在擬定作戰計畫之前必須體認與學習的重要課題。另外，從頻率管理與分配的角度而言，爲避免民用與軍用通信系統相互影響，各自擁有自己專屬的通信頻帶。但無法避免的是在無線電傳輸過程中，需使用共同的傳輸媒介—自由空間(Free Space)。首先，考慮城鎮地區的環境對電波傳遞的影響，通常有以下幾點特性：

一具有許多妨礙電波傳播的建築物。

二布滿電力線、導電與導磁物質等電波訊號干擾源。

三行道樹或其它阻擋電波訊號傳遞的物體等。

當無線電波發射後，會以各種不同的角度在上述的物體表面間來回交叉反射，方抵達接收機，這就是大家所熟悉「多重路徑(Multi-path)反射」問題的成因。此時，不同的角度代表電波傳播的路徑長短不一，換言

① 國防部，國防報告書，http://www.mnd.gov.tw/report/defence/chinese/p2.HTM。

之，接收機在不同時間會收到相同訊號，更甚者會在相同時間收到不同時間發射的信號，致使接收機無法辨識原始的訊息。例如，當使用者在使用GSM行動電話，遇到手機收訊不好時，通常會一邊問對方「可以聽得到嗎？」，一邊移動身體來改善訊號品質。檢視當時使用者的環境，通常是位處房屋內、汽車旁或窗戶旁等複雜的環境中，此種狀況在空曠的郊區則絕少發生。雖然軍用無線通信與民用頻帶不同，對複雜環境所衍生的問題與民用系統並無二致。

根據以往的經驗，在複雜的城鎮地區另一個棘手問題爲雜訊(Noise)。本文所指的雜訊是屬於人爲雜訊的部分，主要爲電力線、發電機或汽機車的點火系統等裝置所造成的電磁干擾源。傳統的消除雜訊的手段不外乎加大無線電發射機的發射功率或是改良接收端增加訊號處理的功能兩種。其中以接收端增加訊號處理功能的方式較佳，經由高階的無線電設備，以其內建訊號處理功能，不但可以減低多重路徑反射的影響，自混亂訊號中去蕪存菁檢出需要的訊息以增加訊雜比(Signal-to-noise Ratio)之外，更可以避免因加大發射功率帶來發射機位置暴露的危機或導致更大範圍的干擾問題等。除了傳統的手段之外，亦使用較高的頻率來增加電波訊號的穿透性。

許多通信器材的製造商察覺到軍隊在城鎮地區遭遇到雜訊與干擾的難題，紛紛推出新式的通信設備來搶佔市場。例如：Harris公司(RF-5000的製造商)在今年年初推出一款UHF頻帶、手持式、視線(Line-of-sight)的通信機，主要利用較高的頻率對環境產生較高穿透能力的概念加以設計而成②。由於頻率升高，發射機的天線尺寸相對地縮小，功率承載自然降低，因而必須犧牲掉部分的傳輸距離。雖然通信距離不足的部分，可藉由增設中繼站來加以彌補。電梯中與大樓的天台等處仍是此類設備的通信死角，這是不容否認的事實。

除了選用較高頻的通信設備之外，還可利用新型的軍用通信網路(Military Communications Network)技術來矯正或減少干擾。正如同美國陸軍計劃以戰術資訊網路(Warfighter Information Network-Tactical)作爲作戰部隊的通信平台，並藉由較具彈性的資料接力(Relaying data)或其它相關的技術來達到溝通的目的，使成員之間均能保持密切的連繫。早期的通信架構限制較多，只要是使用不同程式的通信裝備、無線電頻率不同、分屬不同的無線電網或電台之間有障礙物阻隔時，彼此之間就無法連繫。改善的方法爲建構一個與網際網路運作協定相容的無線電網路系統，使欲傳遞的訊息經由最靠近的電台往次一個電台傳遞，直到訊息送達目的地爲止。目前美軍廣泛運用網路來傳輸資料，如報告敵我軍位置或是其它類型的數據資料交換等應用，新型的軍用通信網路系統即可與現行傳輸資料的網路互相結合，促使語音與數據資料交換益形便捷。但依舊也會有新的限制與瓶頸產生。例如，勢必要開發新的頻寬分配管理軟體，才能在極有限的無線電頻寬下，滿足成員在語音與數據資料傳輸上的需求。

一、戰場監控

通信網路除了支援軍隊之指揮與管制

② http://www.rfcomm.harris.com/products/tactical-radio-communications/default.asp#1.

外，仍需進一步地提供監聽敵軍通話內容的能力。當軍隊的通信作爲提昇至監聽的層次時，所面臨的挑戰已不僅止於處理電波干擾或雜訊等問題了，這也意味著無論我軍使用哪一個通信頻帶(目前軍用通信系統的頻率與民用頻率並不相同)，都要深入瞭解民用通信網路的各種技術，才有能力對敵軍所使用之民用通信網路進行有效的滲透。因此，在規劃建構新一代的軍用無線通信網路時，必須考慮系統是否具備下列兩個方面的能力：

㈠軍用無線通信系統需使用更高的頻帶，使電波更具穿透力與抗干擾能力。

㈡軍用無線通信系統之接收機頻率的範圍需能涵蓋民用頻帶，以利有效監聽。

據此，洛克威爾公司電子化戰場部門的程式經理包布朗指出：「軍用無線通信系統使用的頻率若不能提昇至2GHz以上，未來將會遺漏90%的訊息量。」尤其當民用通信網路蓬勃發展並使用各種不同的頻率與時間分配管理技術之際，設計的概念早已與十年前傳統軍用系統大不相同。新式軍用通信設備必須增加軍用頻段以外頻率的接收能力；同時新式軍用通信設備也特別需要加入更多新式的演算法；系統操作者在使用系統之前，更是需要經過嚴密而完整的操作訓練。

回顧過去十年通信技術的發展歷程時發現：美軍早期的通信技術確實保持在領先的地位，自從美軍釋放部分通信技術至今，民用通信系統的製造商反而成了最大的受益者。美軍雖然不斷地從事通信技術的改良，也新增不少自行開發出來的加密技術，例如JTRS(Joint Tactical Radio System)軟體無線電系統允許使用不同頻率與不同程式的無線電機均可加入系統中，讓操作者輕易就可與其它操作者通信。民用通信系統的製造商在通信領域的發展，至少在跳頻、展頻、加密與網路等部分的技術超越軍方，這也造成了爾後軍方在監聽訊息時的困難度。

新的通信技術也讓依賴民用通信網路的敵人帶來好處，例如加密與跳頻技術整合後，使部隊要追蹤敵人的訊息來源變得更爲棘手；除此之外，將行動電話手機內晶片的程式改寫，即可重製成另一支或多支不同門號的手機。這像極了希臘神話裡面的九頭蛇，攔截或監聽其中一支特定電話號碼的訊息，仍然漏掉其它的蛇頭之間的對話。那麼從頸部將所有的蛇頭都砍下來，仔細想一想，透過人爲干擾的手段阻斷相關電話的訊號，並不是一個容易實現的辦法。如此說來，軍隊完全陷於兩難的境地：軍隊一方面想要保護通信網路避免被炸彈或其它原因致使通信網路毀損，另一方面也不想讓敵人的通信網路暢行無阻，而採取小規模的干擾或是阻擋也會招致民怨。若要做到滴水不漏的過濾則無異等於將整個通信網路關閉。根據媒體報導在2004年3月11日發生於西班牙首都馬德里的炸彈爆炸事件③之後，經過了一連串的調查才發現，透過手機的遙控也可以用來引爆炸彈。此消息震驚了所有負責城鎮地區安全的美軍幕僚們，無不希望這是媒體虛構的劇情而非眞實的事件。

當部隊用盡一切手段來阻撓敵軍的通信時，一個相當重要的關鍵是：人爲干擾總是比監聽所需要的技術來的簡單許多。雖然民用通訊設備製造商不願意確切的說明要具備

③ http://www.wordiq.com/definition/March_11,_2004_Madrid_attacks.

怎樣的技術才能監聽或干擾他們產品的訊號。製造商確實擁有相關的技術是無庸置疑的。然而敵人所使用的通信工具有相當的多元性，從行動手機、衛星電話、有線電電話到網路電話(Voice-over-Internet Protocol, VoIP)等。其中尤以網路電話最具彈性，只要是網際網路的連線可及之處皆可使用。敵軍就像是個狡猾的駭客隱藏在網路中，也有可能是個隨時移動的無線網路用戶，透過追蹤網路位址(IP Address)來定位，實屬不易。話雖如此，通資專家仍然嘗試著開發出讓網路用戶暴露位置的相關技術，一旦敵軍使用網際網路通信時，便可鎖定敵軍的位置，這將是通資專家們的一大挑戰。

二、戰場滲透

由於城鎮地區中人口密度較高，因而會產生較多的通信鏈路，執行電監與干擾任務時，也就必須增加相對應數量的設備或是加快電監與干擾設備的運算速度。這提供一個令人注意的指標，就是「比起以往傳統戰場情報蒐集的任一項目，個人資料情報的蒐集變得相對地重要」。舉例來說，美軍在協助哥倫比亞政府追蹤一個惡名昭彰的毒梟時，就是依賴個人資料情報的獲得，使通信的監聽與攔截變得更爲容易。無論這個毒梟走到哪裡，負責追蹤毒梟通信訊號的電監小組，爲了能夠攔截並監聽訊號，就要跟著移動到與毒梟手機連線的基地台附近。但問題在於毒梟和我們一樣都明瞭，目前所使用的手機有被監聽之虞，會不斷地更換手機，以避免訊號被追蹤。因此，毒梟目前的位置、使用哪一個號碼，這是電監小組在變換監聽地點之前亟需獲得的情報。若要電監小組在數以萬計的電波訊號中搜索、過濾並監聽通話內容，無疑是大海撈針。電監小組永遠需要相關的電話號碼表、基地台的位置或掌握類似的線索，才有可能利用電監設備來追蹤毒梟的位置。

爲避免透過手機遙控的爆炸裝置(Improvised Explosive Devices, IEDs)威脅地面人員行動的安全，進行數百公尺以內之小範圍的干擾，是一個比較合理可行的作法。舉例來說，靠近伊拉克北部地區手機遙控的爆炸裝置幾乎隨處可見。已有許多廠商提供伊拉克部隊具干擾通信訊號功能的新產品，使地面的軍事行動避免受到手機遙控爆炸裝置的威脅。EDO公司生產的通信干擾裝置，也曾提供美軍部隊在伊拉克的戰場上使用；Thales公司也在去年推出一款新型的通信裝備，除了可以當成通信訊號的計頻器使用之外，也可用以進行訊號的監聽，達成戰場監控的目的。當然手機遙控爆炸裝置的問題，並非是伊拉克部隊的專利；根據媒體報導，巴基斯坦的總統也曾遭受手機遙控爆炸裝置的威脅，而在干擾器的保護下安然無恙；印度的邊境防衛隊(Border Security Forces)也需處理相同的問題，促使邊境防衛隊自行開發出有效範圍超過100公尺以上的干擾器，來保護本身的安全。

目前，若有非特定人士或機關在非軍事用途的情況下，藉由民用通信網路的技術，針對民用通信網路監聽或干擾，並不至於令人感到意外。舉例來說，無線電計程車所使用的無線電屬公共的頻段，無需申請執照與付費。接著就像是電影裡面常見的情節，幾個中央情報局(Central Intelligence Agency, CIA)幹員或警察經常利用一些看起來並不顯眼的箱型車或是貨櫃車改裝成行動基地台，

裡面裝滿了各式的監聽與通信設備，停在目標區附近的路邊針對手機、有線電話、無線電計程車使用之無線電波等進行監聽，藉以監控嫌犯的行動。若部隊要在城鎮地區執行監聽任務，得學會此技巧，也該使用一些看起來並不怎麼起眼的民用車輛來僞裝大量的監聽設備。

論及戰場型態的轉變，已進入所謂「不對稱戰場」的時代。若有全副武裝士兵開著迷彩塗料的軍車，大剌剌地進入城鎮地區，所有民眾立刻行注目禮或者像是國慶閱兵一般沿街鼓掌歡迎。部隊的監聽行動應盡可能地避免引起敵人的注意，那就要效法展頻通信的技法：把訊號埋在雜訊中。其中訊號意指監聽行動，而雜訊則代表城鎮地區環境特徵。所以，參與城鎮作戰的成員就應該將通信器材與監聽設備等裝載在民用的車輛中，使之看起來與民眾每天的生活的裝扮相同，才算得上是最好的僞裝。

拜民用通信網路加密技術日益茁壯之賜，使得監聽任務變得無比艱難，而這一場加密技術的競賽將是永無止境的繼續下去。雖然軍方與民間通信專家均擁有解密的能力，但這個技術並不是想像中那麼簡單，通信內容加密的過程是經過繁複的處理步驟，同時也結合大量的運算，往往等到解密完成卻早已過了時效。在民用通信的領域，通信系統製造商爲了確保客戶之間的通信安全，無不投入大量的人力與資金，期能開發出更安全的加密技術，以避免因使用過時或容易破解的加密技術而被市場淘汰。敵人選擇民用通信網路爲溝通的媒介，意外地撿到通信保密的好處。軍方喜歡直接使用干擾的手段來妨礙敵人的通信，最主要的原因是部隊沒有太多可用的時間進行大量的運算與繁複的處理步驟，來處理這些加過密的訊息。

縱使「資源」再多還是永遠不夠用，必須視事情的輕重緩急做到合理有效的分配。如果從戰略層面來看，可以按照主觀的意願將通信訊號任意地加解密或從事破解敵人加密技術的工作，時間並不是主要的限制因素；但是如果是從戰術層面來看，操作手在建立通信網路的步驟中，執行三角定位、身份辨識與確保通信鏈路品質爲第一優先，其次爲監聽，最後才是解開敵人的通信內容。因此在電子戰的戰場，無論是戰略或戰術層面，均需仰賴電腦的輔助不斷地計算、計算、再計算。也就是說，決定電子戰能力優劣的主要因素在於誰使用的電腦速度比較快、計算能力比較強。

三解決之道

在大部分區域衛星絕對可以提供良好的通信品質與影像的傳輸。意即透過衛星與無人飛行載具的協助，確實可以改善城鎮地區雜亂電波的問題。若再增加一些新的技術，衛星網路也將會擁有追蹤移動目標的能力。不過單就目前的技術而言，尤其當戰況緊急又遇上無線電網無法正常運作的情況下，衛星系統算是最受青睞的通信工具，地面部隊指揮官可以透過衛星系統，呼叫位處地球背面的總部請求火力支援，同時傳回當前的影像。

目前，許多國家的情報部門已經擁有優異的監聽技術，包括美國、英國、澳洲等國家之國家安全局不僅有能力監聽有線電話、海底電纜、行動電話基地台等通信系統，當然也包括監聽衛星通信的能力。他們何以能夠輕易地從各式通信系統中截獲所需要的訊

息？應全部歸功於電腦運算能力的提昇與軟體技術的發達，僅需在相關的應用軟體中輸入關鍵字，例如姓名或身分證字號等類似字元，電腦系統就可以呼叫資料庫中與關鍵字連結的個人資料，藉以篩檢通信內容中與個人資料相同的字元，並自動追蹤紀錄相關連線的通話內容。雖然這種功能對部隊在城鎮地區之軍事行動而言並沒有迫切的需要，但是在敵軍愈來愈偏好使用民用通信網路的當下，若能藉由監聽的技術來追蹤特定人士的行蹤，則會展現相當大的助益。

衛星與無人飛行載具除了提供通信方面的用途之外，其主要的貢獻是在全球定位方面扮演著不可或缺的角色。若民眾欲滿足全球定位的需求，方法其實十分地簡單，只要使用者在手機裡面加裝全球定位系統(Global Positioning System, GPS)晶片，或是使用無人飛行載具分別與地面接收站及行動電話基地台連線，並以三角定位的方法計算無人飛行載具與兩個基地台之間的無線電訊號，便可輕易地完成定位。反觀目前軍隊相當地仰賴衛星系統，提供在全球定位、武器導引與建立更多的通信鏈路等應用，如果敵人也懂得運用這些技術，將逐漸地蠶食軍隊在衛星系統的優勢，慢慢地成爲軍方潛藏的弱點。

根據媒體報導，在聯軍拯救伊拉克人民自由(Operation Iraqi Freedom)行動的初期，也就是由美軍帶頭進入伊拉克的領土時，伊拉克軍隊曾經企圖干擾美軍的通信網路。然而，此一作爲並沒有給伊軍帶來絲毫幫助，反而癱瘓了伊軍自己的通信網路。此時，伊軍的通信干擾源也就名正言順地成爲聯軍反輻射飛彈的獵物。從過去幾次的戰役中，我們不難發現，我們所對抗的其實是第四軍種，當敵人使用更精良的通信裝備時，我們就必須相對地提昇通信裝備的性能與數量，使其具備鎖定更多通信鏈路的能力。

結論

通信網路爲軍隊之神經，其範疇包括目標獲得、語音與數據資訊交換、敵我狀態情報的傳輸、連接各式的感測器等應用。像這樣廣泛用途的工具，彰顯了加密技術在通信網路的重要性。但是要加密到何種程度才足以抗衡敵人日益精良的通信網路呢？此問題並沒有固定的標準答案得視情況而定。

隨著戰場型態的轉變，傳統縱向的通信架構，將面臨嚴苛的考驗。除了使用更高頻段來提高通信網路的效能之外，應在傳統通信架構之上增加橫向通信鏈路，形成網狀通信架構；同時也需增加通信系統與資訊網路連結的介面。此時，通信網路需相對地付出操作手與設備倍增、複雜度增加、前置規劃作業費時、需擴充通信中心頻管與網管功能等必要的代價。

譯者簡介

廖銘洲中校，中正理工學院電機系、中正理工學院電研所碩士。曾任排長、連長、教官。現於國防大學中正理工學院國科所攻讀博士。