美國監聽(視)事件對國軍資訊安全維護之啟示

作者/施玟伃少校

國防大學理工學院正 94 年班，理工研究所 101 年班，陸軍通訓中心通資安全正規班 26 期，曾任排長、通信官、資訊官、教官，現任職於陸軍步兵訓練指揮部教官。

提要

一、科技在軍事領域上的發展速度遠超乎我們的想像，戰場情報訊息萬變，世界大國無不想掌握機先，孫子兵法有云「先知者，知敵之情者也」，快速掌握情資，就能有效超前部署，故全球監聽事件應聲崛起，人與人之間不再有秘密，各項活動也都被攤在陽光底下，對國軍而言，如何維護通資安全將是本篇文章的重點。

二、美國自 911 事件後便啟動恐怖份子監聽計畫，在批評的聲浪下，美國政府逐步取得相關法令的授權，進而名正言順的執行監聽情報蒐集。參與計畫者不外乎有名間廠商，因此發生聞名全球的「史諾登洩密事件」，該事件也凸顯了通資安全的重要性。

三、過去數年來，電腦強化監視技術與個人身分識別技術有著顯著的進步，內容涵蓋個人身高、體重、生活習慣、親友資料及處所等，再結合無遠弗屆的監視衛星與高度匿蹤無人飛行載具，[1]未來世界任何風吹草動在監視者眼皮下將無所遁形。

關鍵詞：監聽技術、史諾登事件、監視事件

[1]Eric L. Haney，Brian M. Thomsen，〈論 21 世紀戰爭：超越震撼與威攝〉，《國防部史政編譯室》，99 年 3 月，頁 183-184。

壹、前言

科技在軍事領域上的發展速度，就如同民間企業競爭所需之變革一樣快速，科學進步加上商業與通信全球化，成本低廉的資訊科技是促使軍隊必須轉型的重要根源，而軍事轉型四大必要需求為戰略、科技、威脅與風險管控。[2]然而風險管控最大的威脅莫過於「恐怖主義行動」；恐怖主義，依目的不同，可區分為：鎮壓性、革命性及分離性的恐怖主義，係為達特定政治目的，有系統的對政府、社會或個人使用難以預測的暴力或威脅等手段，而可利用恐怖主義之主體，不限於各種政治組織、民族團體，還包括宗教狂熱者、革命者、追求社會正義者、軍隊及秘密警察。[3]

為因應恐怖主義行動，世界各國紛紛積極制定各種反恐措施，像世界大國美國立了一系列的反恐法案，其中，最具爭議的乃是美國於911恐怖攻擊事件發生後 6 個月內，布希(George W. Bush)總統於 2001 年在國會監督下通過了一項限時法--《2001 年提供阻絕恐怖主義所需適當手段以鞏固美國法案》(簡稱美國愛國者法)，該法案賦予執法機關更多監聽電話通聯、電子郵件及網路行動等個人資訊的權力。這樣倉促的立法過程，無非是要保護美國國家與國民免於遭受恐怖活動攻擊之威脅，但令人擔憂的是，美國為因應恐怖主義，快速立法的程序及限制措施是否有侵害人民基本權利之虞。[4]

貳、無遠弗屆的監聽(視)技術

一、聽瓮

竊聽技術遠在古時候帝王時期就已經開始發展，古代間諜最早發明的竊聽器稱之為「聽瓮」其為一種口小腹大的罐子，(如圖一)將其埋在地下，於甕口蒙上一層薄薄的皮革，間諜在進行偵測時，就貼耳在上面聽取周邊的動靜，為了減少情報的失誤，會選擇培訓盲人執行任務(盲人眼睛不好，但在聽力方面會優於正常人) 「聽瓮」[5]在隧道攻城戰能夠發揮極大功用。清末曾國荃太平天國一戰率領湘軍攻城時，當時的太平軍於城牆腳下埋設聽瓮，藉以偵探城外敵軍動靜，導致湘軍未能一舉攻破，可見「聽瓮」在古代戰爭中還是發揮很大的作用。

[2]Elinor Sloan，〈軍事轉型與當代戰爭〉，《國防部史政編譯室》，99 年 6 月，頁 242。

[3]何秉松，<現代恐怖主義之意義與反恐怖主義的國際實踐>，《國政研究報告憲政(研)》，第 091-034 號。

[4]林婈旻，〈史諾登事件對美國人權影響之研究〉，《中央警察大學公共安全研究所論文》，103 年 5 月，頁 1。

[5]kknews，聽瓮，https://kknews.cc/history/mb9ybb2.html，(檢索日期：109 年 6 月 15 日)。

圖一 聽瓮

資料來源: https://kknews.cc/history/mb9ybb2.html，(檢索日期：109年6月15日)

二、黑室

在古羅馬時代，政界主角廣布專屬自己的間諜網，尤其在凱薩（Gaius Julius Caesar）大帝在位時，常利用「攔截信件」的動作讓自己能夠察覺各種反對他的人與事。中世紀時，在法國大革命期間，革命政府在法國各地成立許多「監視委員會」，該組織被授權可監視、逮捕任何對政權有威脅之貴族及外國人。歐洲各國政府在18世紀也投入部分人力設立「黑室」(Black Chambers)，這種機構通常設置在郵局辦公室內，利用各種技術秘密檢查私人信件。[6]

三、Lamphone（遠端竊聽技術）

以色列內蓋夫本-古里安大學（Ben-Gurion University of the Negev）以及魏茲曼科學研究所（Weizmann Institute of Science）的科學家們發表了一種新的遠端竊聽技術稱之為「lamphone」。他們表示，任何人只要一台筆記本電腦，和一千美元以下的設備（一具望遠鏡和一個約 400 美元的光電感應器），就可以即時聽到 100 公尺外房間的任何聲音，正確的說法是聲音在燈泡玻璃表面上產生的微小振動。科學家們表示，通過蒐集這些在燈泡上振動引起的光學微小變化，情報員就可以清楚的獲得聲音來識別對話內容，甚至連在聽什麼音樂都可以知道，他們還發現，LED 燈泡出現的訊號量約是白熾燈泡的 6.3 倍。[7]

[6]安東尼.卓薩爾，〈國際縱橫：世界各國政府監聽的歷史〉,《BBC 新聞雜誌》，104 年 6 月 28 日。

[7] WIRED，以色列最新間諜技術：「監聽」你家的燈泡，https://www.wired.com，(檢索日期：109 年 6 月 15 日)。

四、可視麥克風

通過望遠鏡用高速攝影機拍房間中的一袋洋芋片或植物，並分析他們的振動頻率後，就能重建室內的對話和音樂，[8]基於影像的技術用途，可視麥克風的應用比 Lamphone 更廣泛一些，惟需要更多軟體進行精密分析，所費時間相對較多，適合用於長期監視對象。

五、手機監聽器

手機監聽僅需使用對講機原理，其原理為製作兩個晶片，分別裝在竊聽者與被竊聽者的手機裡面，[9]就像是家裡的市內電話無線子母機一樣。分述如下：

(一)複製 SIM 卡：竊聽者需得到被監聽者的手機 SIM 卡，複製後開始監聽工作，此方法最為簡單，但也最容易被發現，因為被監聽者發現電話費暴增即可合理懷疑手機被動手腳。

(二)晶片式竊聽器：晶片式竊聽器是目前監聽市場內比較常見的類型，它根據有效距離分為 35 公尺至幾百公里等類型和級別，售價從幾千元至幾十萬元不等。[10]工作方式就跟對講機一樣。

(三)大型的行動電話監聽系統：一般運用在間諜活動中，原理完全不同於其他竊聽器。它是直接從空中攔截行動電話信號，通過解碼可監聽到所有通話內容。這類竊聽器與電腦相連接，不僅讓被監聽人毫無察覺，而且可以儲存上百組電話號碼，並將竊聽內容錄製到電腦硬碟當中。當然如此專業的設備價格也不菲，要價高達幾十萬元。[11]

六、線路中繼監聽

線路中繼竊聽，顧名思義，即是竊聽麥克風由線路連接到一個傳輸中繼，竊聽人員在中繼端收聽或者中繼端經過編碼、加密後以無線電的形式傳輸到竊聽人員端。這種竊聽方式運用在早期戰場戰術竊聽，偵察兵將高靈敏微型麥克風放置在敵指揮所等重要情報點附近，竊聽端則在遠處竊聽對話內容。[12]

七、調頻(FM)發射機竊聽

此方法是使用一個調頻發射機作為聲音訊號的收音端，另一個調頻收音機作為聲音的中繼端，再直接竊聽、錄製或用短波編碼後再發射出去。這個竊聽的方法優點是不受外在天氣或是環境的噪音影響，依然可以清楚的聽到聲音。為

[8] 同註 7。

[9] kknews，手機監聽器的原理是怎麼樣的，如何防止並察覺直接被竊聽了呢？，https://kknews.cc/tech/kvkqlxv.html，(檢索日期：109 年 6 月 15 日)。

[10] 同註 9。

[11] 同註 9。

[12] 同註 9。

了防止其他人在使用收音機時收聽到竊聽的內容，竊聽者一般會把竊聽器的頻率設置在當地調頻廣播的頻率之外。[13]

八、水棲生物感應器

某國國防部撥出 4500 萬美元專款研發「持續性水棲生物感應器」，該研究室利用發光浮游生物和伊氏石斑魚等海洋生物對海底環境改變的強大敏感度及靈活度去觀察水下或海底物體，監視他國核潛艇和水下載具活動。[14]

參、美國監聽計畫

馬克思（Karl Marx）說：現代國家是「管理全體資產階級共同事務的委員會」。而美國就是將其發揚光大的前驅者，美國資本主義在網際網路早期發展階段便已建立主導地位，並由此獲得影響力及利益，加上愛德華·史諾登（(Edward Snowden）的洩密事件，我們才能得知美國監控規模是如此驚人。史諾登在 2013 年時所洩漏的文件顯示，美國對於特定類型的政治合作，會使用數位方式監控本地及外國人，因為這樣的監控作法對美國而言既有效又便宜的。

一、稜鏡(PRISM)計畫

「稜鏡計畫」(PRISM)為美國國家安全局，自2007年起開始實施的機密級電子監聽計畫，該計畫的正式名稱為「US-984XN」，[15]起源自美國911事件後，前總統布希先生責由美國國家安全局實施「恐怖分子監聽計畫」（Terrorist Surveillance Program），並在歐巴馬(Barack Obama)總統時期獲得外國情報監察法院（FISC）合法授權，該計畫能對即時通信和儲存資料進行深度監聽，監聽媒介包含電子郵件、視訊影像、語音交談、相片，網路電話和任何藉由網路傳輸的平台。

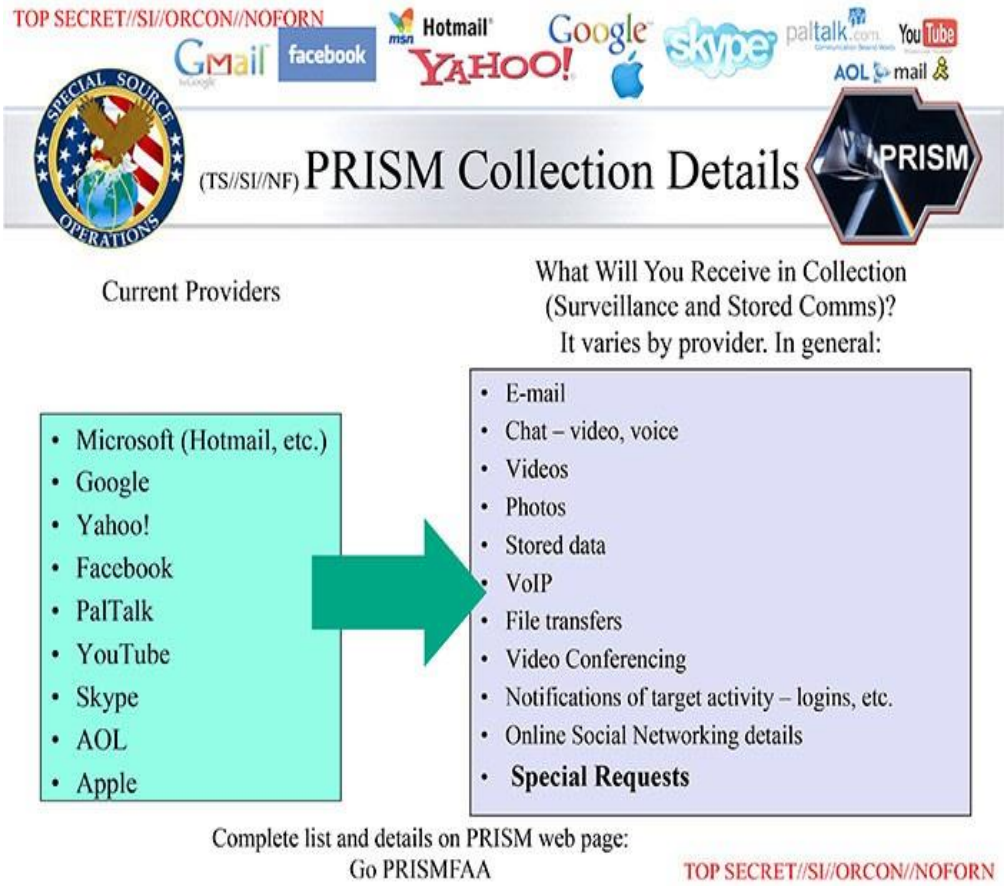
稜鏡計畫起始於2007年1月8日，解密日期為2038年9月1日，其資訊提供者主要有九個主要公司：微軟(Microsoft)、雅虎(Yahoo)、谷歌(Google)、臉書(Facebook)、Paltalk、優兔(YouTube)、Skype、AOL及 Apple，蒐集的資訊包含信箱、影片、照片、網路電話、即時社會網絡資訊及客製化需求等，(如圖二)然而上述公司加入計畫的時間也不同。(如圖三)

---

[13] kknews，竊聽與反竊聽，https://kknews.cc/news/yvpkp4k.html，(檢索日期：109 年 6 月 14 日)。

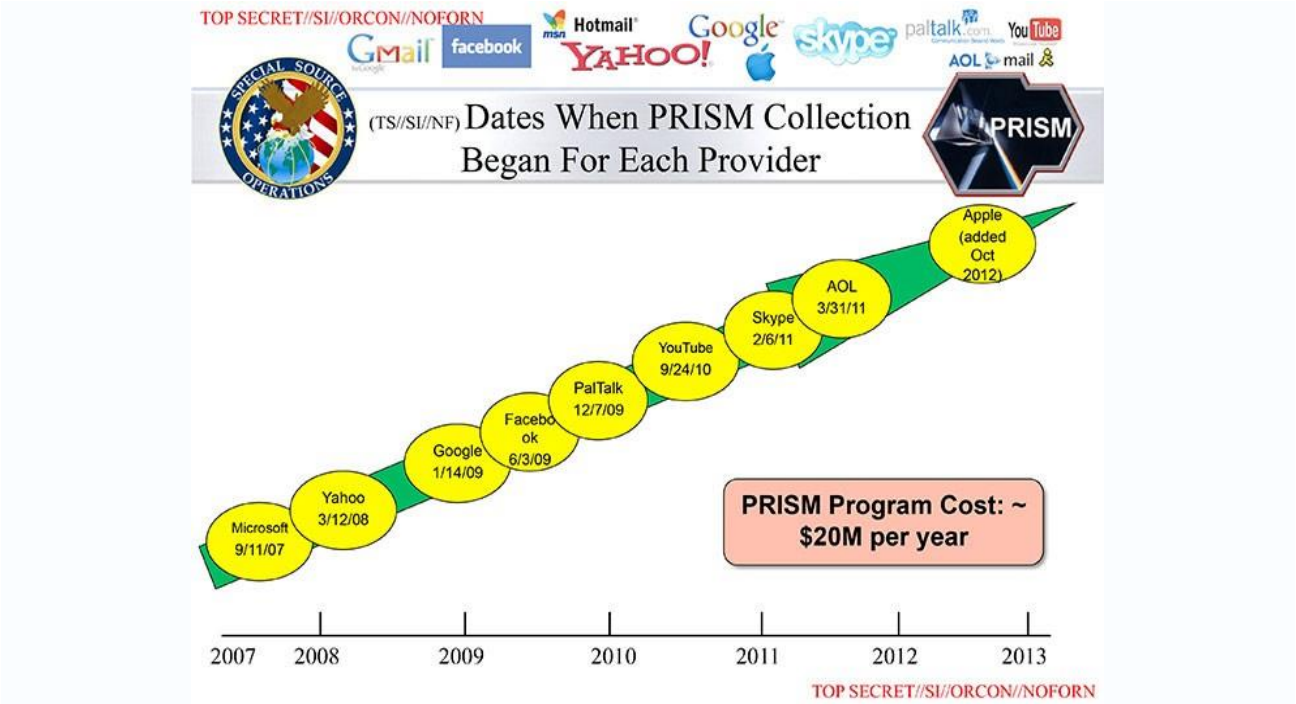
[14] 中國大陸國防部-孫立華、孫龍海，揭密/這些令人防不勝防的間諜技術手段，你中招了嗎，https://mod.gov.cn，(檢索日期：109 年 12 月 23 日)。

[15] Savage, Charlie, Wyatt, Edward; Baker, Peter.,<U.S. says it gathers online data abroad>. 《New York Times》，http://www.closeprotectionworld.com/security-news-north-america/80126-u-s-says-gathers- online-data-abroad.html,，(檢索日期：109 年 9 月 2 日)。



圖二：稜鏡計畫（PRISM） 參與公司與蒐集資料項目

資料來源: The Washington Post；http://www.washingtonpost.com /wp-srv/special/politics/prism-collection-documents/，(檢索日期：109年9月1日)



圖三：稜鏡計畫（PRISM）各公司參與時間表

資料來源: The Washington Post；http://www.washingtonpost.com /wp-srv/special/politics/prism-collection-documents/，(檢索日期：109 年 9 月 1 日)

根據PRISM計畫的秘密簡報檔案顯示，世界各國之間的資料交流，都必經美國的骨幹網路且會被美國攔截，原因在於美國與各洲之間的網路頻寬遠大於各洲之間的頻寬數(如圖四)，為了加速資料的流通性與便利性，往往會選擇經由美國網路來做為傳遞的路由站。[16]

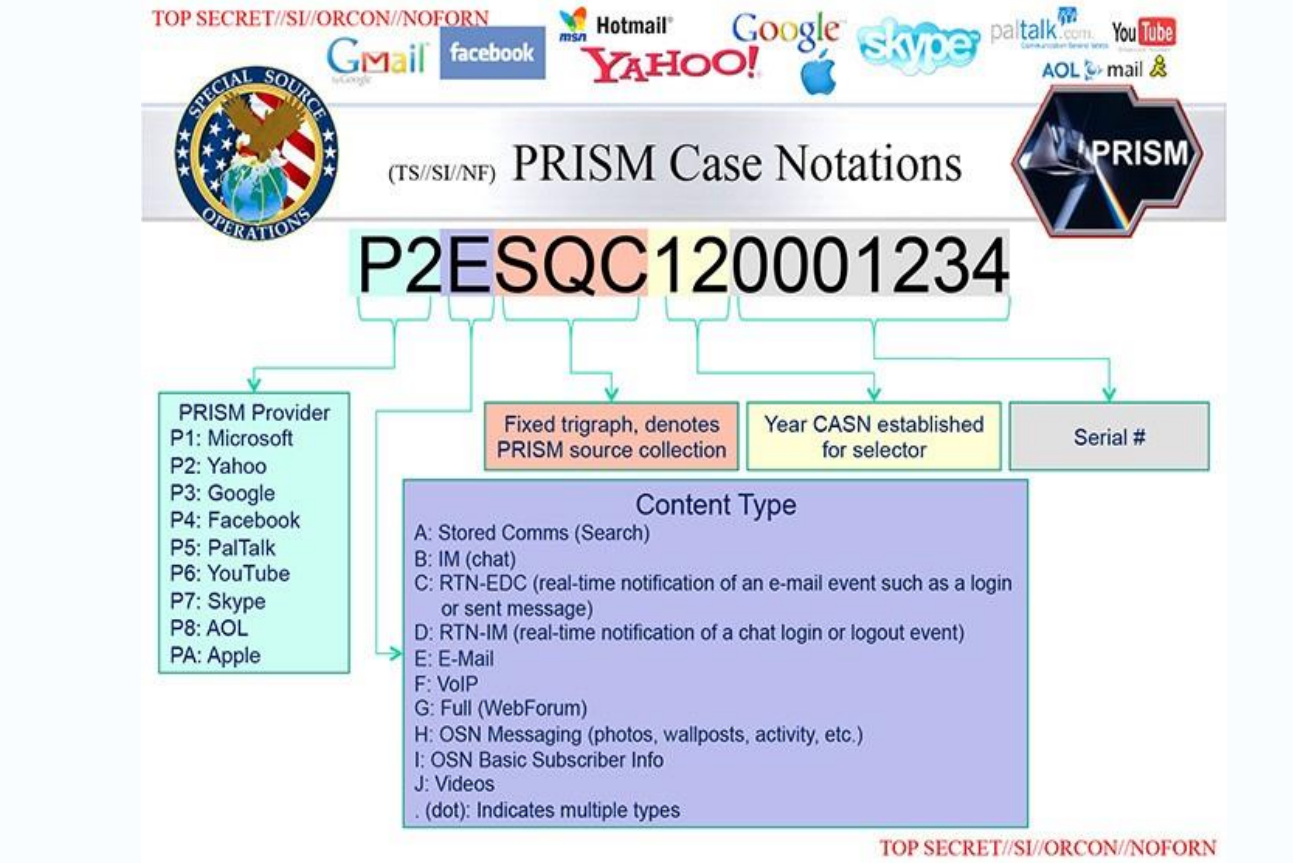
圖四：全球電子通信頻寬脈絡圖

資料來源: The Washington Post；http://www.washingtonpost.com /wp-srv/special/ politics/prism-collection-documents/，(檢索日期：109 年 9 月 1 日)

PRISM情報分析師首先要向「稜鏡」項目發出搜索請求，尋求獲得一個監視目標(需為外國人或是在國外的美國人)及其資訊，由各合作公司根據搜索流程及需求實施監視作業，獲得資訊內容會分送「國家安全局」(National Security Agency，簡稱NSA)與「聯邦調查局」(Federal Bureau of Investigation，簡稱FBI)資料庫進行分類儲存。每個被監視的目標會被標號儲存，標號各有不同的含義，能夠反映出即時監視、儲存資訊的可用狀態。根據這些編號，當一個指定目標登入或發送電子郵件時，國家安全局可以接收到相關即時通知或監視到指定目標的語音。例如：綠色部分：「P」代表哪間公司提供的資料；紫色部分：「A」代表通信資料，「B」代表即時通訊，「C」代表電子郵件即時通知，「D」代表聊天活動即時通知，「E」代表電子郵件，「F」代表網際網路語音通話，「G」代表全文(網路論壇)，「H」代表社交網站資訊，「I」代表社交網站使用者資料，「J」代表影片；[17]紅色部分：固定的字串；黃色部分：專案建立的年份；灰色部分：專案序號(依序排列)。(如圖五)

[16] The Washington Post；http://www.washingtonpost.com /wp-srv/special/ politics/prism-collection-documents/，(檢索日期：109 年 9 月 1 日)。

[17]同註 4，頁 23。



圖五：PRISM專案編號說明

資料來源: The Washington Post；http://www.washingtonpost.com /wp-srv/special/politics/prism-collection-documents/，(檢索日期：109 年 9 月 1 日)

二、X-Keyscore 計畫

愛德華・史諾登提供英國《衛報》另一高度機密等級的監視計畫「X-Keyscore」32 張簡報內容，該文件僅有美、英、加、澳與紐等國（五眼聯盟-情報分享）的授權人員才能觀看。[18]該計畫的主要功能是利用個人會話及郵件進行語言及網路追蹤，簡報內容指出，這是國安局歷年來監控範圍最廣的系統，在全球各地共設置約 700 台伺服器[19]，(如圖六)迄今已協助逮捕超過 300 名恐怖分子。而從簡報中的地圖來看，伺服器設置地點遍及各大洲，除了美國本土以外，也包括俄羅斯、中國大陸與委內瑞拉等敵國。「X-Keyscore」計畫與美國其他已曝光的監控系統不同，可將幾乎所有網路活動編入索引，使資料可供搜尋。[20] X-Keyscore 可以蒐集來自不同類型的資料，然後再進行追蹤調查，且蒐集來的數據可保存 30 天。X-Keyscore有9大功能分述如下：

(一)搜尋目標：主要搜尋使用語言非所在地區的人。例如：在美國使用中文。

(二)搜尋加密資訊：系統可以使用各國的加密軟體對搜尋該國的檔案進行解

[18]The Guardian.,< XKeyscore presentation from 2008 – read in full >.http://www. theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation?INTCMP，(檢索日期：109 年 9 月 2 日)。

[19] Idownload，http://www.idownloadblog.com，(檢索日期：109 年 10 月 21 日)。

[20]同註 4，頁 29。

密，該系統不分析解密後的檔案，而是追溯該檔案曾經瀏覽過的網站。

(三)技術搜尋：人們喜歡利用虛擬個人網路(VPN)作為網路中繼站，X-Keyscore有技術能搜尋這樣的使用者使用網路的紀錄。

(四)蒐集網路對話：網路上的語音、文字對話都會在伺服器或是電腦裡面留有紀錄，X-Keyscore能蒐尋相關紀錄作為情報。

(五)語言追蹤：這項功能更像是「搜尋目標」的延伸，只是這項功能有鎖定特定的地區，並且在搜尋到目標後進行追蹤工作。

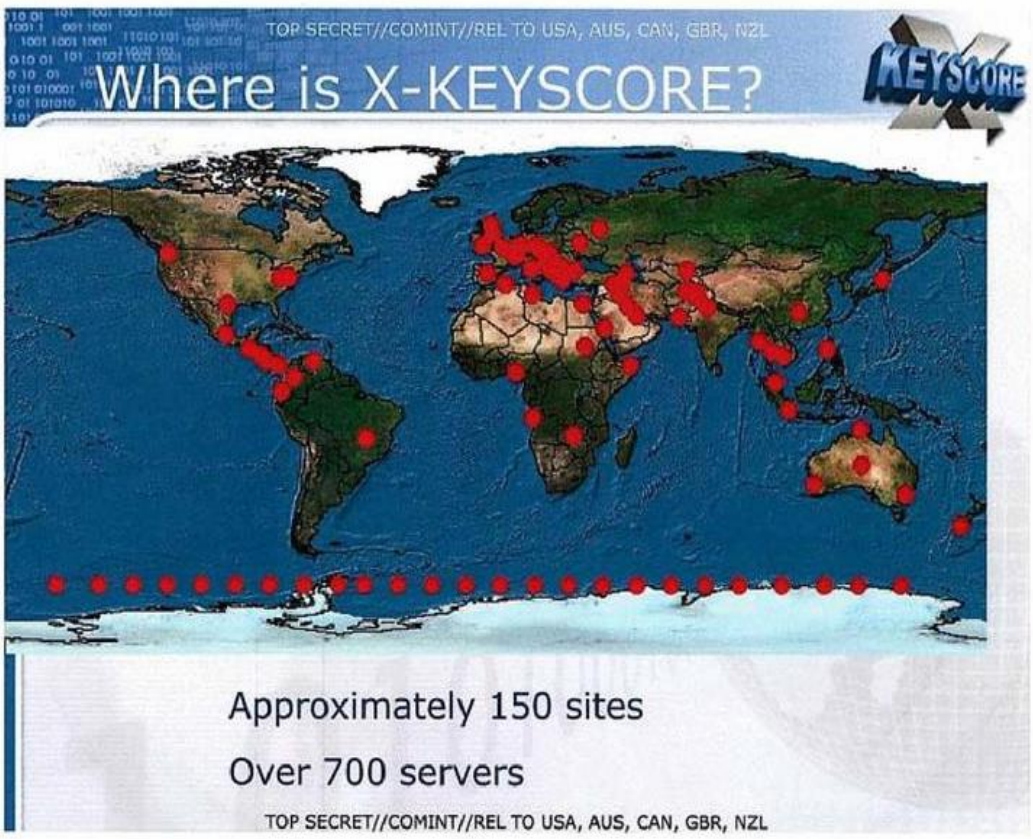
(六)網頁紀錄監控：目標在網路上的活動都會被記錄並進行追蹤監控，例如：使用GOOGLE MAP搜尋某地點，X-Keyscore將會把目標與地點開始進行關聯結構串聯。

(七)搜尋文件檔：以「KEYWORD」搜尋網路上相關的文件資料。

(八)分析指紋資訊：利用美國國安局的指紋資料庫對目標指紋進行比對、分析。

(九)發現新網頁：利用目標的ID搜尋相關新網頁，進而掃描網頁內容查找相關資訊。

X-Keyscore之所以強大，在於搜尋範圍分布全球，9大功能可循環式的串聯搜索，搜尋到的資訊還能被分析再利用，這也是為什麼恐怖份子在短時間內就已遭捕獲300多名。



圖六：X-KEYSCORE 全球分布圖

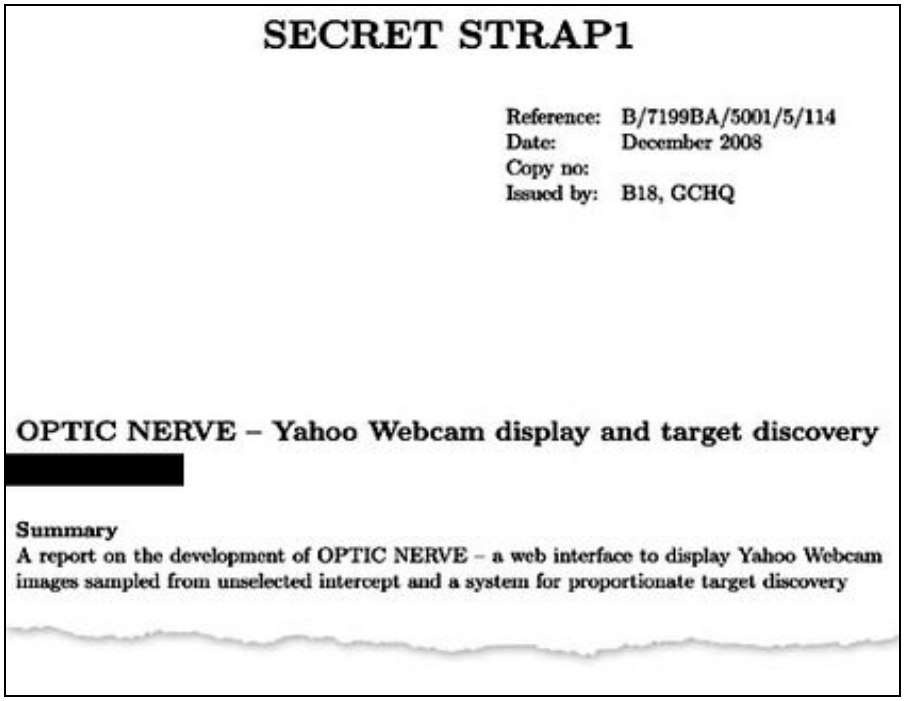
資料來源: Idownload，http://www.idownloadblog.com，(檢索日期：109年10月21日)

三、Fairview

Fairview乃是由美國國家安全局(NSA)實施的一項秘密大規模監聽，運作的對象乃係針對外國移動訂戶的大規模監聽項目。該項目的目標是整批蒐集來自外國公民行動電話的數據。[21]根據史諾登的爆料，NSA僅在 2013 年 1 月蒐集來自巴西用戶的 23 億份數據，NSA可侵入與該公司有聯繫的外國公司系統。利用「Fairview」，NSA能夠直接進入巴西電信系統，蒐集數以百萬的個人、企業、機構的電話錄音與郵件內容。各國依照被蒐集監控情報的多少，被標上不同顏色作為專案儲存。[22]

四、Optic Nerve

美國國家安全局(NSA)協助英國政府通訊總部（GCHQ），利用行動代號Optic Nerve的偵察系統於2008至2010年間，監控攔截雅虎(Yahoo)視訊的畫面(每五分鐘蒐集一次影像)與資料庫，其中甚至包括裸露畫面，且初估有超過 180 萬使用者受到影響。GCHQ還利用此系統來攔截與儲存影像，(如圖七)且讓情報人員自由取用攔截到的影像來分析可疑帳號。這套系統原本是用來試驗臉部辨識的系統，提供情報分析人員比對，並破解情報指涉嫌疑人利用多帳號藏匿的工具。[23]


SECRET STRAP1

Reference: B/7199BA/5001/5/114
Date: December 2008
Copy no:
Issued by: B18, GCHQ

OPTIC NERVE – Yahoo Webcam display and target discovery

[redacted]

Summary
A report on the development of OPTIC NERVE – a web interface to display Yahoo Webcam images sampled from unselected intercept and a system for proportionate target discovery

圖七 OPTIC NERVE簡報

資料來源: Idownload，http://www.idownloadblog.com，(檢索日期：109年10月21日)

[21]EUA espionaram milhões de e-mails e ligações de brasileiros, O Globo, 6 Jul 2013. Retrieved 9 Jul 2013，(檢索日期：109 年 10 月 21 日)。

[22]US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden, South China Morning Post, 23 June 2013. Retrieved 9 Jul 2013，(檢索日期：109 年 10 月 21 日)。

[23]同註 4，頁 34。

表：美國監聽計畫綜合比較表

美國監聽計畫綜合比較表				
監聽事件	參與公司	媒介	監聽主要對象	特色
PRISM	Microsoft等9個公司	網路	非美國人 在他國的美國人	監控時間最久
X-Keyscore		網路	全球	監控範圍最廣
Fairview		通信系統	巴西	
Optic Nerve	YAHOO	視訊鏡頭	英國	監聽時間最短

資料來源：作者自行整理

國家和政府的網路監控行為，已經藉由立法排除人權與隱私權來成為公權力展現的一部分，無論遭遇多強烈反對，各國亦可能持續進行且日後可能更強化這方面的科技研發，使國際競爭更激烈，人民隱私權更難確保。[24]自 911 恐怖攻擊事件發生後，有許多報告顯示美國國家安全局的活動嚴重侵犯人權，而政府卻一再掩飾及保留評估它的合法性，使得美國政府不斷的蒐集和儲存所有美國人的訊息。對於史諾登的揭露，顯現美國國安局計畫是一個巨大的謊言，挑戰法律邊緣，及實質違反人民隱私權。[25]

肆、美國監聽事件省思

情報是決策的基礎及成功的關鍵，沒有情報的決策就是盲目的，而情報的取得端賴監控技術的發揚，[26]孫子兵法也說「謀定而後動」，20 世紀 70 年代以後，情報和能源、科技被稱為現代社會經濟發展的三大支柱，[27]因此，情報的重要性已是千古不變的道理，從清朝時期的監聽技術--聽瓮到現在的科技監控，不難發現我們時時刻刻活在科技監控的範圍內。對美國這樣的世界大國而言，情報體系在國家安全的角色與功能，以及情資整合在國安決策與反恐應變等危機處理皆有著重要的地位，至於如何跨越相關部門各自為政之藩籬，建構有效之情資整合、分享與應變機制，提供預警情報和情勢判斷，協助政府有效進行危機管理，消弭危機於無形；或進行危機處理，遏止事態升高擴散；或有效善後復原，避免損害蔓延，則尚待深入探究。[28]

[24]同註 4，頁 36。
[25]同註 4，頁 92。
[26]黃榮條，〈建構跨部門情報資訊整合應變平台之研究〉，《中央警察大學公共安全研究所碩士論文》，105 年 12 月，頁 25。
[27]李修安、王思安，〈情報學〉，《一品文化出版社》，105 年，頁 41-43。
[28]同註 25，頁 23-24。

美國的監聽事件之所以揚名全球，源自於美國政府在冷戰結束後精簡預算，導致國防事業高度外包後，使情報作業面臨困境，為求快速重建情報作戰的能力，政府選擇與民間企業緊密合作。外包制(outsourcing)已經成為全球化時代的一種普遍現象，一般營利公司的目標就是在面對競爭割喉戰時也能符合成本效益，並獲得更廉價的勞動力和其他更便宜的競爭工具，最終演變成外包制的一個大規模的經濟效益，[29]而外包商在其能力、經濟效益等商業考量下，很多時候會將部份工作發包給承包商來進行，這也是肇生史諾登事件的主因，承包人員沒有固定的公司，單憑個人能力承接工作，因而人員的忠誠度與歸屬感相對而言較低，所以，倘若國軍的外包模式沒有改變，不難想像史諾登事件有可能在我國發生。

冷戰結束後，美國面對多元威脅劇增，因此必須擁有更多情報來源、提高情報蒐整效率，並從中過濾、發掘潛在危險，礙於訊息量過於龐大，必須仰賴專業承包商的服務，對於國家安全而言，承包商雖強化情蒐能力，但也相對增加洩密的風險，故如何管制承包商這個雙面刃將會是軍事單位必須面對的重要課題。

伍、國軍資訊安全防護策略

資訊洩漏的原因有八成來自人為威脅，這與監聽事件洩密的主因不謀而合。在各種利益的驅使下，不論是政府或是民間，都會利用監聽方式取得敵方情資，加上科技的日新月異，人們使用網路的頻率相對提高，人與人之間的秘密不再是秘密，任何網路上的活動都在監視者眼皮底下一覽無遺，使用者除了養成良好的網路使用習慣以外，更應該對個人資料加以保護，史諾登在接受美國紐約客雜誌《The New Yorker》訪談裡面建議我們做到以下幾點將可以保護個人隱私。

一、使用加密工具：立即停止使用 Dropbox，因為它並沒有提供加密服務，如果要考慮其他的替代產品，SpiderOak 是個交換、傳輸檔案的好選擇。

二、不要使用會侵害隱私的服務：Facebook、Google 這兩個大家最常用的網路服務，其實對你的隱私可能有莫大的危害，不要用這兩個社交媒體傳送文字訊息。[30]

簡而言之，凡走過必留下痕跡，所有網路上的文字、語音及影像都在無形中被管理者存取，大部分的使用者對「資訊安全」觀念的薄弱，抑或是基於便

[29]謝祥棟，〈美國情報機構承包制之研究以史諾登事件為例〉，《國立中正大學戰略暨國際事務研究所碩士論文》，104 年 3 月，頁 22。

[30] T 客邦，如何保護隱私?史諾登建議你不要用 Dropbox、Facebook、Google，http://techbang.com/posts/20389-how-to-protect-your-privacy-see-shi-nuodeng-3-recommendations，(檢索日期：109 年 10 月 27 日)。

利性的思維下，忘卻了資訊安全的重要而疏於戒備，殊不知這些網路平台、媒介都極有可能在政府及其他的壓力之下，將目標資料交付出去，因此，資訊安全的地位就顯得重要許多。

「資訊安全」定義為「維持資訊的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)」，取字母開頭，亦稱為資訊安全的 CIA。[31]一開始的資訊安全導向都是正面的，管理者對於資訊的保存也是有意義的，但如果今天這個資訊是會造成國家安全及軍事機密危害，那所謂的資訊安全就不再是資訊安全了。以 2020 年美國總統大選為例，民主黨候選人拜登的兒子杭特在選舉前一個月出現疑似電郵外洩導致拜登的支持度降低，被洩漏的郵件顯示，拜登家族很有可能長期與中共聯絡，藉由資訊交換獲取金錢，當然，這樣的消息被拜登否決了，拜登接受媒體訪談時提到，美國目前最大的威脅是俄羅斯，最大的競爭者是中共，這兩個國家很有可能就是提供假消息的來源。不論這個消息的正確與否，我們可以知道連世界大國的候選人在選舉期間，其家人的電腦都能夠被有心人是竊取相關資料，更遑論身為百姓的我們呢！

國軍為了保護資訊安全做了很多防範措施，例如，網路實體隔離、採購限制非中共產出品、個人通訊設備安裝 MDM 及軍用電腦安裝相關監控軟體等，無非是希望藉由層層把關守護資訊安全。但是，網路的縫隙在於資訊技術的強大與否，培養優秀的資訊專業人才、教育國軍人員資訊安全觀念、強化使用者保密習慣才是有效防範資訊洩密的最好辦法。

陸、結語

國家安全的概念及其內涵的發展趨勢，大致上已由軍事和戰略安全為主導的高階議題，擴及以經濟與社會為焦點的低階議題，並走向綜合性安全的方向。因此，必須運用軍事與外交手段及其他所有國家資源，有效整合運用，發揮整體功效，方能維護國家安全與增進國家利益。[32]而維護國家安全最有效的方式就是軍事作戰，然而，隨著科技的演變，軍事作戰的方式也逐漸轉型，作戰的方式不再是傳統的船堅砲彈，而是趨向無形的戰場—網路，情資的蒐整來自網路，資料來源來自網路，駭客的入侵也來自網路，而史諾登所揭露的美國監聽事件更顯示，良好的網路使用習慣將可避免許多私人甚至於公務資訊被攤在陽光底下。「網路」給了資料偷窺者無限的監視空間，因此，提升網路管理作為才能消弭資訊外洩於無形。

---

[31]增井敏克，〈圖解資訊安全與個資保護/網路時代人人要懂得自保術〉，《碁峰資訊股份有限公司》，108 年 9 月，頁 22。

[32]劉燕薇，〈我國國家安全決策之運作〉，《國立政治大學外交學系戰略與國際事務碩士在職專班 碩士論文》，91 年 1 月，頁 49。

秘密通訊自由與隱私權是基本人權中重要的一環，亦是憲法所保障之基本權利，更是思想自由與人性尊嚴的具體表現。然而，通訊科技日益發達，通訊往往被利用為犯罪工具，進而可能侵害個人權益、社會秩序甚至國家安全。因此，為保障人民基本權利，同時確保國家與社會安全，根本之道在於落實通訊監察相關法制之執行，除了全面禁止違法通訊監察外，對於合法的監察亦應嚴加規範，[33]另外，需要加強執行間聽者的道德與法律素養，才能符合憲法兼顧保障人民權利以及國家法益之本旨。

[33]同註 4，頁 100-101。

參考文獻

1、Eric L. Haney，Brian M. Thomsen，〈論21世紀戰爭：超越震撼與威攝〉，《國防部史政編譯室》，2010年3月。

2、Elinor Sloan，〈軍事轉型與當代戰爭〉，《國防部史政編譯室》，2010年6月。

3、何秉松，<現代恐怖主義之意義與反恐怖主義的國際實踐>，《國政研究報告憲政(研)》，第091-034號。

4、林婺旻，〈史諾登事件對美國人權影響之研究〉，《中央警察大學公共安全研究所論文》，民國103年5月。

5、安東尼.卓薩爾，〈國際縱橫：世界各國政府監聽的歷史〉，《BBC新聞雜誌》，2015年6月28日。

6、WIRED，以色列最新間諜技術：「監聽」你家的燈泡，https://www.wired.com，(檢索日期：109年6月15日)。

7、kknews，手機監聽器的原理是怎麼樣的，如何防止並察覺直接被竊聽了呢？，https://kknews.cc/tech/kvkqlxv.html，(檢索日期：109年6月15日)。

8、kknews，竊聽與反竊聽，https://kknews.cc/news/yvpkp4k.html，(檢索日期：109年6月14日)。

9、中國大陸國防部-孫立華、孫龍海，揭密/這些令人防不勝防的間諜技術手段，你中招了嗎，https://mod.gov.cn，(檢索日期：109年12月23日)。

10、Savage, Charlie, Wyatt, Edward; Baker, Peter.,<U.S. says it gathers online data abroad>. 《New York Times》，http://www.closeprotectionworld.com/security-news-north-america/80126-u-s-says-gathers- online-data-abroad.html,，(檢索日期：109年9月2日)。

11、The Washington Post；http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/，(檢索日期：109年9月1日)

12、The Guardian.,< XKeyscore presentation from 2008 – read in full >.http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation?INTCMP，(檢索日期：109 年 9 月 2 日)。

13、Idownload，http://www.idownloadblog.com，(檢索日期：109年10月21日)。

14、EUA espionaram milhões de e-mails e ligações de brasileiros, O Globo, 6 Jul 2013. Retrieved 9 Jul 2013，(檢索日期：109年10月21日)。

15、US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden, South China Morning Post, 23 June 2013. Retrieved 9 Jul 2013，(檢索日期：109年10月21日)。

16、黃榮條，〈建構跨部門情報資訊整合應變平台之研究〉，《中央警察大學公共安全研究所碩士論文》，民國105年12月。

17、李修安、王思安，〈情報學〉，《一品文化出版社》，2014年。

18、謝祥棟，〈美國情報機構承包制之研究以史諾登事件為例〉，《國立中正大學戰略暨國際事務研究所碩士論文》，2015年3月。

19、T 客邦，如何保護隱私?史諾登建議你不要用 Dropbox、Facebook、Google，http://techbang.com/posts/20389 (檢索日期：109 年 10 月 27 日)。