10.6326/NDJ.2014.29(5).6

全球隱密監控與國家間反應：以「梯陣」、「稜鏡」間諜網絡為例

Global Covert Surveillance and International Responses: Examples of "Echelon" and "Prism" Spy Networks

吳胤瓛 (Yin-Huan Wu)

中山醫學大學附設醫院法務管理師

提　　要

本文揭櫫全球隱密監控的「間諜網絡」課題，論證主導全球情資監控的美國作爲超強獨霸國家動用按特殊關係簽署秘密安全協定，由美、英、加、澳、紐「五眼」(Five Eyes)聯合運籌迄今之「梯陣」(Echelon)暨情蒐渠道如「稜鏡」(PRISM)、大道(MAINWAY)、船塢(MARINA)、核子(NUCLEON)計畫偕同英「顳顬」(Tempora)計畫等間諜網絡，在實踐國土內外與全球安全上的網絡作戰論述、考量佈局、形勢及國家利益思維。除了闡釋間諜網絡爭議不斷之內涵與發展歷程外，更納入歐洲聯盟及世界各國對此問題之國際間互動及反應之辨析。研究發現：評析國家利益及利益鬥爭實是也總是全球戰略安全之至上核心，基於形勢，霸權壟斷此間諜網絡工具技術集權不墜且更趨嚴密。敵對中共的網絡諜戰將成我面臨駭資曝險及國家安全最大威脅，亟需統整軍情、國安、政戰單位之資訊編制並以國家層級指揮；強化關鍵基礎建設；杜絕敵國電資工程入侵；構建自主獨立電訊與資安產業並納入國防戰略；整體資訊化指管通資情監偵殺系統(C^4ISK)反制；厚植應變網軍侵襲、無證竊聽與數據挖掘之抵禦戰力。

關鍵詞：全球安全、間諜網絡、梯陣、五眼、網絡諜戰

Abstract

The purpose of this study is to discuss the issue of spy network with focus on global covert surveillance, and to examine the secret security agreement dominated by the United States to conduct global surveillance. The agreement was signed by the United States (NSA), United Kingdom (GCHQ), Canada (CSEC/CSE), Australia (ASD), and New Zealand (GCSB), also known as the "five eyes". They form the so called "Echelon" intelligence gathering channel which includes: "Prism", "Mainway", "Marina", "Nucleon", accompanied by the British "Tempora" plan and spy networks. In addition to criticize the controversial behavior of using spy monitor satellites to intercept electronic transmission and communications, this article is more interested in EU and other countries in the world to examine the international

interaction on this issue. It has found that the core of global security strategy is always focused on national interests. Accordingly, the hegemonic states will continue to monopoly the spy network.

We must be committed to maintain the confidentiality of electronic information in order to prevent various kinds of cyber invasions from China. Therefore, the information security industry needs to be included in the national defense strategy and the C^4ISK systems needs to be integrated in order to beef up the capabilities to counter enemy's cyber attacks.

Keywords: Global Security, Spy Network, Echelon, Five Eyes, Cyber Espionage

壹、前　　言

網際網絡，不僅僅是一個虛擬場域，更是國家利益和國家安全的實在聚合體。美國國防部於2011年7月發佈「網路作戰戰略」，除明確要求五角大廈將網路視同作戰領域，並對來自其他國家的網路駭客攻擊，認定為已構成戰爭行為，將比照陸、海、空三軍，從被動防禦轉為主動攻擊，以因應日益升高的網路安全威脅，同時計畫與民間企業以及其他美國盟邦共同發展網路作戰能量。[1]

資訊戰，已是繼陸戰、海戰、空戰、太空作戰之後的第五種戰爭。資訊戰可分為兩種態樣：網際攻防及電訊截收。在網軍網絡戰中一般體現於四方面：駭客攻擊、病毒傳播、信道干擾、節點破壞癱瘓等。而無線電技術偵察又稱為信號偵察，是軍事偵察的重要手段，使用無線電技術設備，截收敵方發射的各種無線電信號從中獲取情報的措施；被稱為除了陸、海、空、天之外的第五空間之偵察。

各國願意高價購買更多、更好的零時差漏洞，導致間諜機構正催生利潤豐厚、危險、不受監管的網路軍備競賽，一個蓬勃開發的灰暗市場。競技場上的資訊開發商可將他們的商品出售給出價最高者－遑論是駭客犯罪集團、恐怖組織或金援恐怖分子的國家。[2]諷刺的是，創造零時差漏洞市場，已使世界進入網路戰爭時代。而更諷刺的是，美國政府是現今最大的零時差漏洞弱點買家。[3]

「資訊戰」（網際及電訊）結合「間諜戰」（滲透、反間、監控）後的「網絡諜

1 曾復生，〈美「中」網路間諜戰最新情勢研析〉，《國家政策研究基金會》，2014年6月9日，<http://www.npf.org.tw/post/2/13698〉（檢索日期：2014年6月9日）

2 James Bamford,“NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar”, *WIRED.com*, June, 12, 2013, <http://www.wired.com/2013/06/general-keith-alexander-cyberwar/>（檢索日期：2014年6月21日）

3 美國政府的行為，將會導致網路安全業界的劇變，從防禦為主轉變為攻擊至上。當販賣弱點的利潤遠超過於公布弱點所獲得的名聲時，發現的弱點將不再被公布，而是轉變為誰能將所發現之弱點，隱藏最長時間，以便在販賣時獲得最大的利益。零時差弱點將變成虛擬世界的核子武器，那個國家掌握最多弱點，便會在發動網路戰爭時，取得最大優勢。Joseph Menn“Special Report: U.S. cyberwar strategy stokes fear of blowback”, Reuters, May 10, 2013, <http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510>（檢索日期：2014年6月21日）

戰」(Cyber Espionage)更可說是繼起演進的第六種戰爭態樣，不僅有龐大組織，同時也是以最大規模運用間諜心術的佈建。「網絡諜戰」：即以全球為戰場，透過佈建龐大組織系統，無遠弗屆攻擊暨阻絕，全面隱密監控且截獲關鍵情報，主要憑藉網軍侵襲、無證竊聽與數據挖掘等技術，藉此操縱且奪取網路空間控制權；不對稱侵略、壓制及威懾與其競爭之國家、企業乃至個人，以期鞏固網絡霸權獲致最大數據掌控地位，更進一步依此壟斷政治上與經濟上之霸權。「網絡諜戰」能力，是建立「不對稱性戰略優勢」的重要環節，而其中的內涵包括「制信息權」和「制電磁權」，並以「電子對抗」、「通信對抗」，以及「網路對抗」為主要作戰形式。[4]此外，將整體的「網絡諜戰」能量，隱藏在作戰部隊和非官方的民間公司組織中，並透過電腦網路的連結可以在世界上各個角落，直接或間接地攻擊目標，進行網路作戰潛伏而不易被察覺。

考察現勢，更加佐證網路戰爭之多變動態與實務發展。

在2014年6月14、18及19日，中共網軍全面出動以大規模的駭客分散式阻斷服務攻擊(DDoS)癱瘓香港大學民意網，導致香港「占領中環」運動全民公投的投票時間被迫延長一週，支持香港普選的壹傳媒網站同樣被駭，連帶影響在臺壹傳媒及蘋果日報的運作，測得臺灣蘋果日報遭駭，6月23日DDoS高峰異常數據流量每秒動輒超過245萬次系統查詢。[5]同日（19日）臺港蘋果日報轉由Facebook平臺對外發聲後，源自中共的網絡攻擊旋以社群網站臉書(Facebook)北卡羅來納州資料中心為攻擊目標，導致臉書全球當機斷訊。香港D100電臺透過網站觀測到中國對美國連射三波數位導彈。攻擊來源為中國，被攻擊最多的目標則為美國(11644)、香港(408)。第一波來源為南寧、第2波杭州、第3波從鄭州發射，當這三波數位導彈頻繁落地後，美國數據猛然飆高突破1萬2千大關，與稍早前香港遭攻擊的數據相差足足30倍。[6]港大民研指出，PoP Vote投票系統由Amazon AWS、CloudFlare、UDomain通域所提供。紀錄顯示，AWS的DNS在20小時內超過100億查詢、CloudFlare、UDomain分別為75Gb、10Gb的DDoS攻擊。大多來自香港當地的互聯網服務供應商，因攻擊流量太過龐大，導致三家服務商都暫停服務，模擬投票系統停擺。

以美國為例，國家安全局(NSA, National Security Agency，下亦簡稱NSA)作為世人印象中世界最神秘的情報機構，由於太過神

4 同註1。網際網路空間至少有7個關鍵戰略高地，包括作業系統、搜尋引擎、通信裝備基礎設施、雲端運算、治理論壇、密碼體系，以及網際網路協定第六版(Internet Protocol Version 6, IPv6)等。（檢索日期：2014年6月23日）

5 http://www.appledaily.com.tw/realtimenews/article/new/20140623/421307/1/網站續遭駭《蘋果》：應是中國網軍所為。

6〈臉書掛點前，中國3波數位「導彈」襲美〉，《蘋果日報》，2014年6月19日，<http://map.ipviking.com/http://www.google.com/url?url=http://www.appledaily.com.tw/realtimenews/article/new/20140619/419474/&rct=j&frm=1&q=&esrc=s&sa=U&ei=S5irU6myGYmLkwWZ6IHIBA&ved=0CBQQFjAA&usg=AFQjCNE2D7Mq4s-H2UrQEiLc1asSYPpC6w>（檢索日期：2014年6月19日）

秘，甚至不為美國其他部門熟悉，而曾被稱為「壓根不存在單位」(No Such Agency)。在預算合計超過千億美元，人員總數在50萬以上的美國情治機構中獨樹一幟，密級最高、耗資僅次中央情報局(CIA)，然人員總數最多、規模最大。[7] 甫卸職退休的Keith B. Alexander四星上將，曾被稱作是世界上最大的情報部門美國國家安全局(NSA)局長、美國中央安全局(CSS)局長和首任美國網戰司令部(United States Cyber Command, USCYBERCOM)司令等「大帝」統轄。[8]

美國已建置觸角遍及全球各地的情資偵蒐間諜網絡，基本構成要件包括新型間諜衛星、通訊訊號截收站、雷達系統以及監聽站。情報偵蒐用以截收各項通訊內容的平臺涵括：海面下的潛艦、地面的天線系統，以及運行於地表上空軌道上的人造衛星，更以多處美軍主要海外基地，遂行情報偵蒐任務。

國安局，及其神秘的梯陣(Echelon)，始終是不獲官方承認但事實上由美國領導的全球間諜網絡，美、英、加、澳、紐發展成為「特殊關係國家」與「複雜相互依賴國家」而廣佈全球實施監聽和傳播之電子通訊操縱建構。梯陣之存在，基於冷戰思維，但縱使時至今日運籌仍方興未艾。在前蘇聯解體之後，Echelon間諜網絡不僅沒有停止運作，反而以控制恐怖主義及組織犯罪為由增強其全球範圍內的情報收集能力；然而，政治、商業、外交方面的訊息皆同樣通過新的通訊技術被監控。

梯陣(Echelon)系統由五眼(Five Eyes)構成，由美國國家安全局、英國政府通訊總部、加拿大政府通訊安全局、澳大利亞國防通訊局和紐西蘭政府通訊安全局等(the U.S.-National Security Agency(NSA), the British-The Government Communications Headquarters Headquarters (GCHQ), the Canadian-The

7 美國國家安全局的前身是1949年5月20日經參謀長聯席會議決定的，由國防部成立的「軍隊安全局」(Armed Forces Security Agency, AFSA)，負責綜合協調下屬部門的情報工作，包括「陸軍安全局」、「海軍安全組」和「空軍安全服務部」，當時沒有多大權力。1951年12月10日中央情報局局長給國家安全委員會主席寫了一份備忘錄，建議成立一個綜合的通訊情報部門，建議被採納並開始調研，1952年6月13日調研報告《Brownell Committee Report》(Herbert Brownell主持)完成，建議在AFSA基礎上成立NSA，工作範圍超出軍隊內部。6月杜魯門總統簽署文件，規定了NSA的工作範圍，1952年11月4日正式成立，將國家安全委員會情報組的9人轉為NSA的領導機構。這個文件在一代人的時間內一直保密。"Edited by Jeffrey T. Richelson assisted by Michael Evans," The National Security Agency: Declassified-Companion Page to the Bulletin of the Atomic ScientistsJanuary/February 2000 Issue, *National Security Archive Electronic Briefing Book No. 24* January 13, 000, <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/>（檢索日期：2014年4月21日）

8 亞歷山大(Keith B. Alexander)四星上將接替Michael Hayden，是設在馬里蘭州米德堡(Fort George G. Meade)美國網絡司令部司令(U.S. Cyber Command, USCYBERCOM)，美國國家安全局(National Security Agency, NSA)局長和中央安全局(Central Security Service, CSS)局長。任期2004-2014年間作為美國網絡司令部司令，他負責按照美國戰略司令部(U.S. Strategic Command)的要求規劃、協調及實施網絡作戰和防護美國國防部的計算機網絡。作為美國國家安全局局長和中央安全局局長，他負責美國國防部的機構，該機構承擔國家外國情報、作戰支援和美國國家安全訊息系統保護的責任。此崗位由Michael S. Rogers繼任。因傳媒報導吹哨者斯諾登揭弊案而黯然於數月後卸職退休。

Communications Security Establishment Canada (CSEC/CSE), the Australia-Australian Signals Directorate (ASD) and New Zealand-Government Communications Security Bureau (GCSB))，自二戰起按特殊關係簽署秘密安全協定聯合運籌迄今。

經美國媒體[9]、歐洲公民自由、司法與內政事務委員會(LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens)調查報告、歐洲聯盟歐洲議會決議報告(2001 EU Parliament Report: Echelon Global Private and Commercial Communications Interception System. European Commission, Temporary Committee on the ECHELON Interception System. July 11, 2001)[10]及美國中央情報局前局長James Woolsey及Jewel v. NSA案等透露證實才終於揭露於世。前揭五眼聯盟憑藉特殊關係國家的基本條件，就是同文、同種、相似的文化、文明、歷史、意識形態與同盟經驗。美、英、加、澳、紐五國即是以英語、盎格魯薩克遜民族為主的國家，享有相似文化、文明與歷史，均屬民主體制。自第一次世界大戰以來，五國幾乎在每一場戰爭中協作具有共同聯繫脈絡。二戰以來，更是堅不可摧的結盟國家。在美紐重締盟約後，紐西蘭負起維持南太平洋和平與穩定任務，參與美國在本區主導的空海整體戰(Air-Sea Battle)聯合作戰。而文件上標誌「FVEY」，即是五眼(Five Eyes)五國共享情報資源之意。

國際間對此之反饋是，歐盟調查委員曾建議歐盟要避免衛星竊聽極為困難，應建立歐洲加密系統以防止資訊、情報外洩。無從逆料的，此事揭露之後才不過3個月，紐約旋發生了911事件。嗣後許多歐盟國家，非但遲滯採取對策，無感威脅，有些還加入情資共享或協助美國一系列監控活動。

911前為梯陣，911後則為稜鏡（梯陣的美國版），但本質不變。2001年911恐怖襲擊事件令美國認識到最大的敵人不是某個國家，而是防不勝防的恐怖主義，於是全球推行反恐戰略。而美國國防部的網路作戰論述則是保衛美國免於遭到網路第一線攻擊，並利用網路科技前線前沿攻擊敵人。網絡透明化乃肇始於美國針對反恐而提出的電子監控。

因面對國會巨大政治壓力，司法部長Alberto Gonzales和美國情報事務主管空軍中將Michael Hayden首度向眾議院情報委員會簡報國家安全局(NSA)監聽行動的運作細節方吐露證實該計畫存在，據《紐約時報》2005年12月16日報導，[11] Gonzales先前曾涉嫌作

9 James Risen and Eric Lichtblaub, "Bush Lets U.S. Spy on Callers Without Courts", New York Times, December 16, 2005, <http://www.nytimes.com/2005/12/16/politics/16program.html?_r=0>（檢索日期：2014年4月24日）

10 EUROPEAN UNION, "2001 EU Parliament Report: Echelon Global Private and Commercial Communications Interception System" July 11, 2001, <http://publicintelligence.net/2001-eu-parliament-report-echelon-global-private-and-commercial-communications-interception-system/> <http://info.publicintelligence.net/ECHELONreport.pdf>（檢索日期：2014年4月25日）

11 James Risen and Eric Lichtblaub, "Bush Lets U.S. Spy on Callers Without Courts", *New York Times*, December 16, 2005, <http://www.nytimes.com/2005/12/16/politics/16program.html?_r=0>
Calame, Byron., "Eavesdropping and the Election: An Answer on the Question of Timing", *The New York Times*, August 13, 2006.; "Transcript of briefing on NSA surveillance by Alberto Gonzales and Michael Hayden", December 19, 2005, <http://www.politechbot.com/2005/12/20/transcript-of-briefing>（檢索日期：2014年4月28日）

偽證誤導國會，試圖虛與逶迤。

而美國中情局前雇員斯諾登(Edward Joseph Snowden)在香港和俄羅斯匿居時，先後拋出主要監控美國國內服務器和電話的「稜鏡」(PRISM)項目、英國「顳顬」(Tempora)秘密監視項目和美國最大範圍收集網絡數據的「密鑰」(Xkeyscore)項目內DNI Presenter工具，能入侵用戶所保留郵件內容與聊天記錄並披露美國侵入世界第二大電信網絡及設備集團中國華為技術公司(Huawei)、監聽歐洲國際峰會場合、竊聽38國駐美機構等行為震驚世界。

美國除斯氏所言的「稜鏡」(PRISM)計畫之外，[12] 尚有大道(MAINWAY)、船塢(MARINA)、核子(NUCLEON)等情蒐監控計畫。美國國家安全局還直接銜接各大科技公司的服務器收集訊息，除了推特(Twitter)拒絕之外，包括：微軟、雅虎、Google、Facebook、PalTalk、AOL、Skype、YouTube和蘋果等九家涉及的服務商均選擇配合政府，雲端存儲服務商Dropbox在不久後也加入。PRISM所收集的數據中，雅虎、Google和微軟更占98%。[13]

本文研究範圍限定在間諜網絡之所奠定的高新科技的間諜衛星、電子通訊傳輸的攔截監聽系統上，而排除間諜船艦、間諜飛機、海底電纜、傳統人力的間諜活動(espionage)及電腦竊聽等設備；亦有限度地排除有關網軍網絡戰之討論。美國情治單位則集中於美國國家安全局。

貳、爭議不斷的間諜網絡內涵及發展歷程

美國的世界霸權地位繫於對外戰略運籌之全球佈局，實際上已改變冷戰時期「同時在兩個戰區作戰」的計畫，代之以在若干擇定前線上爭取制空權和制太空權的較繁複計畫並大幅依賴情報資訊截獲的高科技戰[14] 且與此相對應地，國際關係與戰略研究學界，對於大規模的國與國戰爭衝突是否為普遍現象，其威脅性是否仍足以構成建軍之前提，亦有商榷。[15]

12 Jill Lawrence, “Why PRISM is Different and Scarier Than Other NSA Spying-The latest surveillance program in the news is the most intrusive, and investigating who leaked it will be a stiff test of administration restraint.”, *National Journal*, June 7, 2013, <http://www.nationaljournal.com/nationalsecurity/why-prism-is-different-and-scarier-than-other-nsa-spying-20130607>（檢索日期：2014年4月30日）

13 Barton Gellman and Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program”, *Washington Post*, March, 29, 2014, <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>（檢索日期：2014年6月12日）

14 Stephen G. Brooks and William C. Wohlmfoith, “American Primacy in Perspective”, Foreign Affairs, Vol.81, No. 4, July/Aug 2002, pp. 20-33；電子文獻參閱<http://belfercenter.hks.harvard.edu/files/american_primacy_in_perspective.pdf>及Immanuel Wallerstein, “The Eagle Has Crash Landed”, *Foreign Affairs*, Vol.81, No. 4, July/Aug, 2002, pp. 60-68一文。另參閱Robert Kagan & William Kristol著，楊紫函等譯，《當前威脅：美國外交與國防政策的危機與契機》(Present Dangers: Crisis and Opportunity in American Foreign and Defense Policy)》（臺北：國防部史政編譯室，2002年2月）。John Arquilla and David Ronfeldt著，楊永生譯，《網路及網路戰》(Networks and. Netwars: The Future of Terror, Crime, And Militancy)（臺北：國防部史政編譯室，2003年1月）。

情報或資訊傳輸的網際安全概念於焉建立。2002年小布希總統發佈第16號國家安全總統令(NSPD, National Security Presidential Directive)，組建美軍歷史上也是世界上第一支網路駭客部隊—網路戰聯合職能司令部；明確地採取「由守轉攻」的姿態。在鞏固防禦體制基礎上，將重點轉移到進攻上，這也是2002年9月發表的美國國家安全保障戰略(Bush Doctrine)的反映；[16] 代表美國軍事戰略之重大轉變，由以往之嚇阻戰略轉化為軍事預防戰略及單方（一國主義）行動，文中對於「軍事力之使用」多所著墨。2008年初小布希總統賦予國防部更大的網絡戰反制權表態，允許美軍主動發起網絡攻擊。要求美軍具備進入任何遠距離公開或封閉的電腦網絡的能力，然後潛伏保持完全隱蔽並悄悄竊取信息，最終達到摧毀對方系統、破壞對方指揮控制，甚至控制對方的商務、政務等民用網絡。2009年6月23日，由美國國防部長Robert Gates成立，2010年5月21日正式運行的美國網戰司令部(USCYBERCOM)是美國戰略司令部(United States Strategic Command)下級聯合司令部，由四種軍種聯合組成：陸軍網戰司令部(Army Forces Cyber Command)、海軍網戰司令部(Fleet Cyber Command/United States Tenth Fleet)、空軍第24空軍(24th Air Force)、海軍陸戰隊的網絡空間司令部(Marine Corps Cyberspace Command)等即擁有對本轄部隊的獨立指揮權，網戰部轄下軍事力量，包括海軍第10艦隊、空軍第24軍和陸軍第2軍團。[17]

囊括中央情報局(CIA)、國防情報局(DIA)、國家安全局（NSA，掌管全球電子竊聽）、聯邦調查局(FBI)、與國家偵察局(National Reconnaissance Office，負責太空攝影偵察）的情治機構，僅2013會計年度就耗資526億美元。[18]

國家情報總監(Director of National

15 如Michael Mandelbaum(約翰霍普金斯大學高等國際研究所教授)即指出：國際體系中的首要強權耗費數年時間，竭盡所有資源與武器以求獲致大幅改變地緣政治面貌的主要戰爭已然過時。Michael Mandelbaum, Winter 1998-99,*"Is Major Obsolete?"*, *Survival*, Vol.40, No.4, pp. 20-38。相關資料可參閱Steven Metz著，國防部史政編譯局譯，《美國戰略：美國四年期國防總檢的議題與方案》(American Strategy: Issues and Alternatives for the Quadrennial Defense Review)（臺北：國防部史政編譯室，2002年4月），p. 51與以色列軍史學家Martin Van Creveld, *The Rise and Decline of the State*, Cambridge University Press, pp. 337-354。渠認為武器擴散將使傳統的國與國戰爭顯得無舉足輕重。超強之間的戰爭將被具備核武能力的區域強權間之戰爭所取代。

16 The National Security Strategy, <http://www.whitehouse.gov/nsc/nss.html>（檢索日期：2014年6月24日）

17〈揭開美國網軍面紗：純銅包裹建築防信號外泄〉，《京報網—北京晚報》，2013年6月30日，<http://news.xinhuanet.com/info/2013-06/23/c_132478458.htm>；〈陸軍網絡司令部(ARCYBER)〉，《知遠戰略與防務研究所論壇》，2011年1月10日，<http://forum.defence.org.cn/archiver/?tid-35291.html>；崔雯，〈揭秘各國網軍：美國規模最大　英國網絡罪犯被徵召〉，《鳳凰網》，2013年6月23日，<http://news.ifeng.com/shendu/nfrwzk/detail_2013_06/30/26963747_0.shtml>（檢索日期：2014年4月23日）。網絡司令部的任務：「USCYBERCOM策劃，協調，整合，同步並進行活動：領導國防部訊息網絡的行動和防衛；做好準備，並在指示下，執行全面的軍事網絡空間行動，以確保美國和盟友在網絡空間上的活動自由，並阻止敵方的相同行動。」

18 趙國材，〈人類普遍價值的最大諷刺：斯諾登閉口噤聲若寒蟬〉，《海峽評論》，第274期，2013年10月，頁9-12。

Intelligence, DNI)[19] James Clapper闡述2014年10月1日開始的2015年會計年度預算案，提供給情治單位美國國防部長Chuck Hagel說明2016年前網戰司令部(United States Cyber Command, USCYBERCOM)網攻資訊人員編制超過6,000人，[20] 可知縱算在國防部預算全面縮減情況下，網絡攻擊武器仍是少數持續一路增幅投資的項目，另外兩項則是無人機和特種部隊。[21]

惟如同Daniel Ellsberg（70年代向《紐約時報》爆料，使美國在越戰中暴行曝光的軍方分析員）和Bradley Manning（向維基解密洩密，面對最高監禁154年的刑罰）；包商Booz Allen Hamliton也是美國中情局前僱員斯諾登2013年6月在香港向傳媒《華盛頓郵報》、英國《衛報》[22] 披露「稜鏡」(PRISM)計畫洩密所造成之監聽醜聞，導致網軍發展遭逢重大頓挫，美國參謀首長聯席會議(Joint Chiefs of Staff, CJCS)主席Martin Dempsey四星上將即表示，斯氏洩漏情資造成之嚴重傷害，美國恐需長達2年時間以及可能要耗費數十億美元才能彌補漏洞予以復甦，因洩密情資絕大部分都與軍事有關，其中包括美國軍力、軍事行動、戰略和技術等機密。

一、「梯陣」間諜網絡

1943年5月17日，美、英兩國之間就通訊情報合作締結「BRUSA」（英／美協定）。而1947年，以美國的國家安全局(National Security Agency, NSA)為中心，在英、加、澳、紐的諜報機關參與之下，締結「UKUSA」協約，監聽對象包括前蘇聯暨歐陸各國間密碼破譯及超高頻、微波通訊等。[23] 自網路普及化應用以來，美英全球情報系統UKUSA屢為國際重要話題且備受爭議。[24] 自1970年代，隨著透過人工衛星中繼站的國際電話服務普及，不限蘇聯通訊，均成監聽對象。這是因為對UKUSA的參與國而言，蘇聯並非唯一警戒對象。日本經濟實力急速增強再度成為「潛在敵國」。1981年，美國開始透過雷達監聽日本政府與各地大使

19 國家情報總監直接受到美國總統的指揮、管理與控制。這是根據2004年情報改革和防恐法案(Intelligence Reform and Terrorism Prevention Act of 2004)而設立的，負責下列工作：⑴為美國總統、美國國家安全會議與美國國土安全會議(Homeland Security Council)在關係到國家安全的情報事務上的主要諮詢對象；⑵統領旗下包括16個組織的美國情報體系；⑶統籌指導美國國家情報計畫(National Intelligence Program)。

20 Ellen Nakashima,“U.S. cyber warfare force to grow significantly, defense secretary says”, *Washington Post*, March, 29, 2014, <http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html>（檢索日期：2014年4月25日）

21 田思怡編譯，〈美向陸簡報網軍數盼投桃報李〉，《聯合新聞網》，2014年4月8日，<http://udn.com/NEWS/WORLD/WOR6/8598666.shtml?ch=rss_international#ixzz2zgyUQG2r>（檢索日期：2014年4月23日）

22 <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>（檢索日期：2014年4月25日）

23“NSA Echelon System THE NATIONAL SECURITY AGENCYAND GLOBAL ELECTRONIC SURVEILLANCE”, <http://www.darkgovernment.com/news/nsa-echelon-system/>（檢索日期：2014年4月27日）

24 James Bamford,“Loud and Clear-The most secret of secret agencies operates under outdated laws”, *The Washington Post*, November 14, 1999, <http://www.washingtonpost.com/wp-srv/WPcap/1999-11/14/019r-111499-idx.html>。

館間通訊。當時，美日之間貿易摩擦嚴重，美認為藉由監聽可蒐集日本海外市場傾銷證據。[25]

對UKUSA及嗣後的ECHELON之追蹤研究及公開報導始於英國自由報人Duncan Campbell揭露，亦經歐洲議會「監聽技術2000(Interception Capabilities 2000)」官方文件之確認而除去其神祕面紗。該文件為歐洲議會的「科學與技術評估甄選委員會(Science and Technology Options Assessment Panel; STOA)」委託調查監聽技術的發展現況，以及其衍生的個人資料濫用風險之成果，其1999年四份報告中提出結論認為，近乎所有的現代通訊技術都有可能被截收並篡改。在這份報告中，首次得以窺見「商用通訊衛星監聽系統」間諜情報網(Secret surveillance system: ECHELON)。依照該份文件的研究，UKUSA此一自1947年即已建立所謂通訊情報(Communications Intelligence; Comint)或訊號情報(Signal Intelligence; SIGINT)作戰系統，其中對於網際通訊的分析甚至已達惴懼驚憚地步。

間諜網絡中，美以涉及「外國勢力活動」為由，針對非美國本土的外國人進行情報監控蒐集。澳洲情報機構負責蒐集東南亞和中國南部地區的通訊信號，該行動導致從斐濟、東加、索羅門群島，到中國大陸的情報以及印度和波蘭在南極活動，均無一倖免。加拿大情報機構負責原蘇聯北部地區，紐西蘭負責西太平洋地區，英國負責歐洲、非洲和俄羅斯的歐洲部分，美國負責監視美國、亞洲、俄羅斯的亞洲部分和中國北方地區。後來美國相繼在德國、日本和南韓建立軍事基地，監控活動也隨之擴大到這些地區。美在日本青森縣的三澤基地內，便交集「Echelon」監聽系統。[26]

澳洲是梯陣太平洋地區重要環節，位於西岸的Geraldton基地是其中監聽核心，主要負責偵察印度洋及太平洋上空軌道運行的國際通訊衛星，截取包括中國在內亞太各國的政、經、軍情報。此外，澳洲腹地沙漠神秘的「聯合太空防務研究基地」松峽基地(Pine Gap)素有「澳洲51區」之稱[27]、Norfolk Island無線電接收站，可全方位監測東亞及南亞地區軍事目標。

1997年香港回歸前，門禁森嚴的「小西灣」衛星監聽站代號叫做「天竺葵」，墨爾本的叫AUJ360，衛星中繼線叫「三趾鷗」。澳大利亞20世紀80年代發行的防務文件就稱「三趾鷗」是設在香港、針對中國通訊攔截

25 Tanaka Sakai，〈世界中の通訊を盗聴する巨大システム〉，《tanakanews》，2000年3月2日，<http://tanakanews.com/a0302echelon.htm>；田中宇，〈竊聽全世界通訊的巨大系統〉，《geocities.jp》，2000年7月1日，<http://www.geocities.jp/tanakanewscn/000701.htm>（檢索日期：2014年4月23日）

26 アメリカの國家安全保障(NSA)が主導する情報機関エシュロン(Echelon)の盗聴が國際問題化している中で、金正日黨書記・北朝鮮労働党総秘書の國際電話の通話内容を、西側のある情報機関が探り出していたことが明るみになった。進一步文獻可參閱：http://www.infovlad.net/underground/asia/japan/dossier/echelon/echelon_nkorea01.html；http://www.interq.or.jp/gold/network/estate/news/000815.html「米國のNSAと英國らがスパイネットワーク「Echelon」を使い國際的なスパイ活動が発覚、現在も盗聴されている」等。

27 <http://www.bibliotecapleyades.net/esp_sociopol_pinegap.htm#top>; <http://antg.cand.com.vn/vi-VN/hosomat/2006/4/81380.cand>（檢索日期：2014年4月27日）。前澳大利亞總理Edward Gough Whitlam在1975年威脅要關閉松峽基地後不久，在美方的敦促之下就被迫辭職。

之工程。澳大利亞對中國進行刺探的主要目標是：中國的先進核武器和太空試驗活動以及中國在西沙群島(Paracel Islands)的軍事活動，也監視蘇聯在東亞的海軍調遣，從海參崴(Владивосток; Vladivostok)和堪察加的海軍基地到越南的金蘭灣。

美國在南韓的監聽部隊主要是駐韓美軍第501情報團，正式名稱為第501軍事情報群，駐紮於美國第8集團軍龍山基地附近的普光洞(보광동)。它誕生於1950年10月13日，當時稱為501通訊偵察團，是駐韓美軍情報機構總代表。利用陸基天線群、海上偵察艦隊、空中偵察機以及衛星等手段，監控北韓所有無線和有線通訊內容，號稱北韓半島所有部隊的調動都在第501團的監控之下。第501團早在1975年就開始對南韓總統府青瓦臺實施竊聽。[28]

早在二次大戰末美國國安局也曾竊聽盟邦電訊，包含截獲中華民國政府機密計畫與相關駐外使節通訊，如：法國投降後德國卵翼下附庸的法蘭西國(l'État français)，即維琪政府(Régime de Vichy, 1940-1944)當時派駐越南總督(1940-1945年)讓・德古(Jean Decoux)傳至駐北平公使瑪哲理(Jacquin de Margerie)電報、刺探中國外長宋子文動向、駐蘇大使傅秉常致電中國駐美大使魏道明電報、日本駐南京大使谷正之電報、及蘇聯外長莫洛托夫邀蒙古領導人霍爾洛・喬巴山(Хорлоогийн

表1　梯陣間諜網絡中美國佈建全球監控衛星之經緯度及監聽站位置

印度洋上監控衛星	INTELSAT 604(60° E), 602(62° E), 804(64° E), 704(66° E) EXPRESS 6A(80° E) INMARSAT Indian Ocean area	Geraldton, Australia Pine Gap, Australia Morwenstow, England Menwith Hill, England
	INTELSAT APR1(83°), APR-2(110, 5°)	Geraldton, Australia Pine Gap, Australia Misawa, Japan
太平洋上監控衛星	INTELSAT 802(174°), 702(176°), 701(180°) GORIZONT 41(130° E), 42(142° E), LM-1(75° E) INMARSAT Pacific area	Waihopai, New Zealand Geraldton, Australia Pine Gap, Australia Misawa, Japan Yakima, USA - only Intelsat and Inmarsat
大西洋上監控衛星	INTELSAT 805(304, 5°), 706(307°), 709(310°) 601(325, 5°), 801(328°), 511(330, 5°), 605(332, 5°), 603(335, 5°), 705(342°) EXPRESS 2(14° W), 3A(11° W) INMARSAT Atlantic area	Sugar Grove, USA Sabana Seca, Puerto Rico Morwenstow, England Menwith Hill, England
	INTELSAT 707(359°)	Morwenstow, England Menwith Hill, England

資料來源：2001 EU Parliament Report: Echelon Global Private and Commercial Communications Interception System, <http://publicintelligence.net/2001-eu-parliament-report-echelon-global-private-and-commercial-communications-interception-system/>

28〈美龐大情報監控系統曝光　能監聽國家領導人通訊〉，《中國網軍事》，2013年6月14日，<http://big5.china.com.cn/gate/big5/military.china.com.cn/2013-06/14/content_29123220_2.htm>（檢索日期：2014年4月25日）

Чойбалсан, Horloogiyn Choybalsan)訪俄等秘辛。[29] 華府「政策研究所」(Institute of Policy Studies, IPS)於1993年依據1966年通過之「資訊流通法案」(The Freedom of Information Act, FOIA)要求國安局解密公開1945年1月至8月的秘密檔案遭到拒絕，興訟3年，國安局敗訴而奉命將900頁密檔影本交給「政策研究所」。

冷戰後，基於英美特殊關係[30] 並協同簽署「SIGINT通訊技術情報協定」(Signals Intelligence)的挪威、丹麥、德國、土耳其等第三邊國家以全球設置4,120座監聽所的龐大規模，用電子攔截系統進行數據庫比對分析，長期暗中侵犯一般民眾通訊隱私與企業機密。[31]

美國間諜網絡中電子偵察衛星延伸至世界每一個角落精密監控，[32] 刺探對象涵蓋具敵意國家以及盟邦。美國在境外佈建的情蒐偵察間諜網絡，鎖定的目標並非純為外國政府及其軍方，而是同時涵蓋國際恐怖組織、販毒集團、軍火走私集團，甚至還從事探查他國經濟活動機密情資的商業間諜工作。分佈在世界各地的監聽站再把電磁波信號傳送到美國情報體系耗資15億美金建在猶他州(NSA Data Center in Bluffdale, Utah)的堯位元組級數據存儲設施上。

另者國家安全局最早披露的消息之一即是1967年的中東六日戰爭中，美國情報偵察船「自由號」在迦薩海域遭以色列故意襲擊，一因美國竊聽以色列許多軍事機密如以色列要向敘利亞戈蘭高地進攻的計畫。[33] 1968年，美國海軍佈置在日本海，監視北韓和蘇聯的間諜船USS PUEBLO被北韓軍隊捕獲，其船員被羈押1年之久。而這又與美國基於對外戰略而機動性規劃地分階段集中於世界衝突點：東北亞、南海、中東、東歐、西亞與中南美洲的海外駐軍基地部署有關。

美國運用這項「SIGINT」(Signals Intelligence)關鍵技術，操作、導引精準武器系統攻擊敵軍位於地下碉堡的指揮部、通訊設施以及軍事總部所在的建築群。「SIGINT」的設置，近可參照中共建立在緬甸SIGINT（信號情報）和ELINT（電子情報）之監測站：在緬甸實兌(Sittwe)、漢依(Hianggyi)、皎漂

29 林博文，《歷史的暗流：近代中美關係秘辛》（臺北：元尊出版，1999年），頁121～138。

30 有關Echelon的彙整可參考<http://www.jca.apc.org/privacy/echelon_link.html>。

31 亞諾，〈窺探美國權威情報機構：美國國家安全局〉<http://www.globalview.cn/ReadNews.asp?NewsID=22797>（檢索日期：2014年5月14日）

32 自1962年5月發射世界上第一顆電子偵察衛星以來，美國使用的電子偵察衛星分為通訊情報和電子情報兩大類。美國先後發展、使用了四代電子偵察衛星。第一代為低地軌道衛星；冷戰結束後，隨著世界政治格局的變化和衛星技術的進步，早期發展的第二代至第四代主要以同步軌道為主，少數採用大橢圓軌道。第二代電子偵察衛星包括「峽谷」(Canyon)、「流紋岩」(Rhyolite)；第三代有「小屋」(Chalet)、「旋渦」(Vortex)、「獵戶座」(Orion)、「大酒瓶」(Magnam)、折疊椅(Jumpseat)；第四代有「水星」(Mercury)、「顧問」(Mentor)、「喇叭」(Trumpet)、「命運三女神」(TriPlrt)。美國現在正在發展第五代入侵者(Intruder)，該衛星是美國「集成化過頂信號偵察體系」(IOSA)的組成部分，美國還在研製具有一定隱身特徵的徘徊者(Plowler)靜止軌道電子偵察衛星和「奧林匹亞」(SB-WASS)低軌道電子偵察衛星奧林匹亞(SB-WASS)。前者用於偵察、定位戰略目標，後者用於海軍、安全局等部門的電子偵察一體化計畫。

33 張殿清，《情報與反情報》（臺北：時英出版，2001年），頁289-292。

(Kyaukpyu)、丹老(Mergui)、阿洽布(Akyab)和紮迪基(Zadetkyi Kyun)及伊洛瓦底江出海口大可可(Great Coco)島等基地現代化，支持中國在孟加拉灣的潛艇活動，同時也可監管印度在Andaman和Nicobar群島的海軍活動監控以及曾在1998年進行核武試爆的東印度奧里薩(Orissa)，這是對印度各樣戰略資產，如導彈發射場、機場之偵蒐。[34] 曾遭中共扣留的美軍EP-3白羊座二型偵察機即是所謂的通訊技術情報機。美國情報部門未能於1998年偵知印度進行地下核武試爆動向，國會旋於1999年時授權軍方改造新型海狼級攻擊潛艦，使其具備截收海底光纖電纜傳輸信號能力。[35] 美國空軍太空指揮部(U.S Air Force Space Command, AFSPC)指在1991年海灣戰爭期間，美國和北約的軍事衛星承擔85%的通訊量，商業衛星僅占15%；而在7年後的2008年科索沃戰爭中，這個比例則倒置。[36] 網絡經濟泡沫的破滅，商業衛星過剩的通訊能力正好補足了五角大廈對頻寬的巨大需求缺口。

間諜情報網(ECHELON)偵查系統曾攔截諸如法國的湯姆生軍事工業(Thomson S.A.)與空中巴士工業集團(Airbus Industrie)的商業機密，並提供給美國國內的競者廠家，以取代其簽約的機會。諸如美國雷神(Raytheo)集團在巴西亞馬遜森林監測設備採購中贏得1,300多萬美金合同。[37]

1995年美國曾藉梯陣間諜情報網，揭露歐洲空中客車公司為贏得與沙烏地阿拉伯航空公司的合同，向沙國政府官員提供賄賂，於是國家安全局(NSA)立即將此事通知美國官員，促使美國波音和麥道公司也加入競標中，最終獲得價值60億美元的契約。另外，美國政府還利用Echelon截獲有關日本汽車廢氣排放標準的資訊、法國1993年參加關貿總協定時的商業秘密以及1997年召開的亞太經濟合作會議的重要資訊。德國《明鏡》週刊報導，1990年，美國家安全局截獲了日本衛星製造商NEC與印度尼西亞方面的談判情

34 載述於Rahul Ray-Choudhury,“Trends in Naval Power in South Asia and the Indian Ocean”, 1996,*Security & Political Risk Analysis (SAPRA)* India think tank.

35〈美布天羅地網　偵搜全球情報〉，《中國工程技術訊息網》，<http://www.cetin.net.cn/cetin2/servlet/cetin/action/HtmlDocumentAction;jsessionid=9B9BF774D76B580649A06F2757FDCCC9?baseid=1&docno=6009>; <http://www.subcontinent.com/sapra/bulletin/96jan/si960101.html.>

36〈數據量超過衛星傳輸能力　美“數字戰”吃緊〉，《人民網》，2003年3月29日，<http://www.people.com.cn/BIG5/guoji/22/86/20030329/957385.html>（檢索日期：2014年4月26日）

37 2000年2月24日、2月25日《人民日報》刊載〈歐盟揭露美國電子間諜網〉〈歐盟指責美國對歐洲國家使用商業間諜衛星〉<http://www.people.com.cn/BIG5/channel5/569/20000308/14112.html>指法國報章《巴黎人報》稱，聯合間諜網早於1947年已成立，旨在蒐集東歐國家的情報。隨著冷戰結束，聯合間諜網偵查標的暗中地轉移為歐陸國家。然而有別冷戰時發展出來的電子間諜系統，間諜網是專門用來刺探非軍方機構情報，如各國的政府部門、社會團體和商業機構。英美兩國多年來已把120枚用以監察前共產國家通訊衛星的間諜裝置，逐漸進行調校。迄今已有40枚被重新調校，對準屬於西歐國家的衛星；間諜情報網還特別以法國（代號FRD）和義大利（代號ITD）的外交人員作為監控目標物。《江南時報》（2000年02月21日第3版），<http://www.ben.com.cn/WLZB/20020709/BIG5/WLZB%5E383%5E7%5E09R1301.htm>（檢索日期：2014年5月11日）

報，當時的美國總統老布希利用這份情報進行干預，最後迫使印尼將這份價值2億美元的合同在NEC和美國電話電報公司之間一分為二。歐盟則稱，1994年，美國情報部門截獲巴西政府官員與法國湯姆遜公司的電話通訊，結果最後與巴西方面簽訂雷達銷售合同的是美國雷神公司。

在2000年4月13日美國眾議院情報委員會曾傳喚CIA局長George Tenet暨國家安全局長Michael Hayden出席預算聽證會，要求就ECHELON偵查系統作出證詞；但有關人證皆諱莫如深。眾議院情報委員會依據House of Representatives amended a bill (H.R. 1555)法授權調查並提出Sec. 307. Report On Legal Standards Applied For Electronic Surveillance。[38]

歐洲議會的科學與技術選項評估委員會(STOA)的工作文件指出，美國試圖以防治犯罪的理由說服歐盟國家，共同採用其「金鑰附帶還原(key escrow、key recovery)」

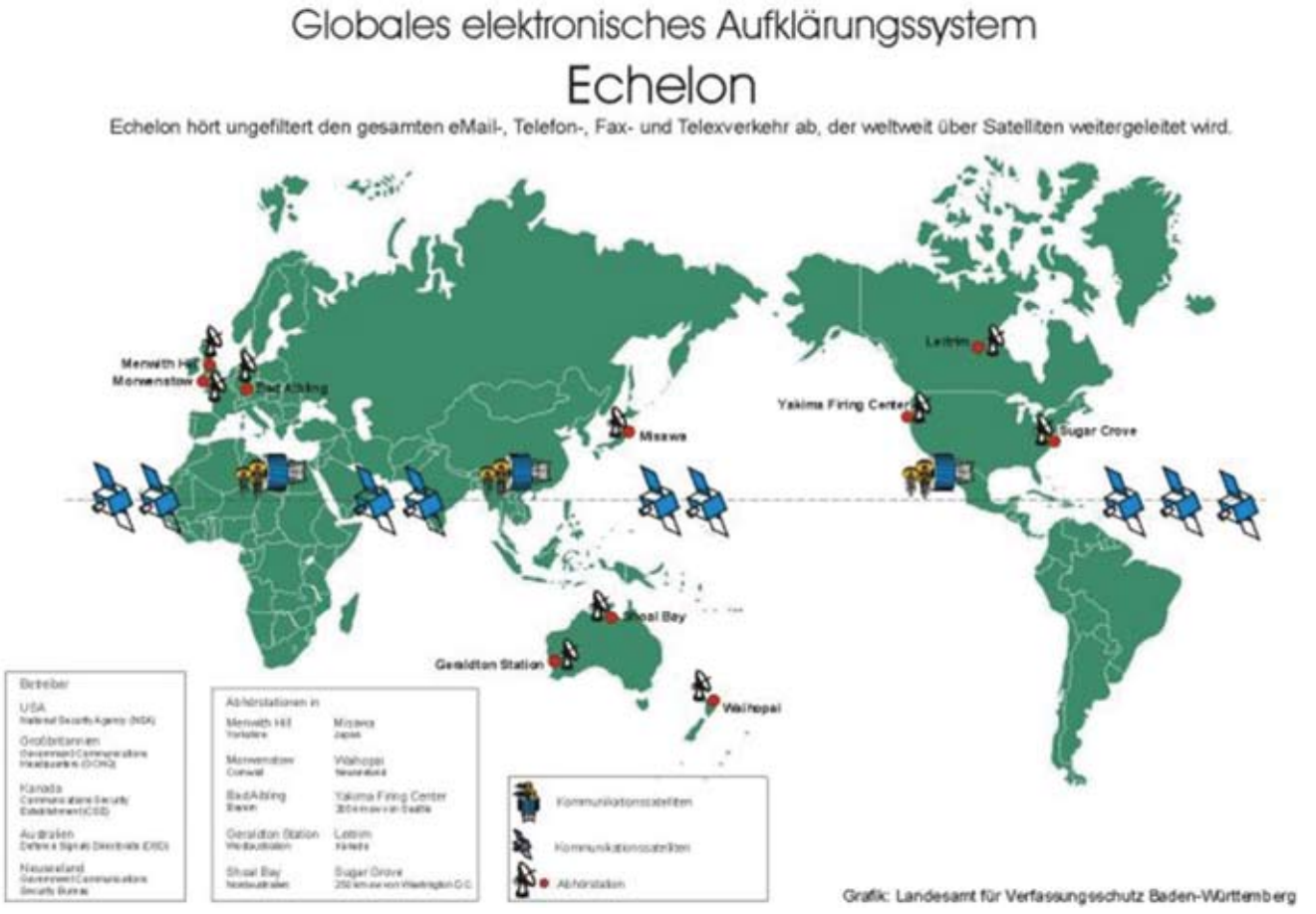

圖1　梯陣間諜網絡係一龐大隱匿之全球電子偵察系統(ECHELON Globales elektronisches Aufklärungssystem: ECHELON)

資料來源：<http://www.fas.org/irp/program/process/echelon-m.jpg>

38 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", *FAS*, February 2000, <http://www.fas.org/irp/nsa/standards.html>（檢索日期：2014年5月8日）

政策，即對任何編密系統保有「後門(back-door)」的存取能力，且美國政府試圖誤導歐盟(EU)與經合會(OECD)各國，隱藏該政策的真正意圖。同時，美國政府也不間斷地持續以防治犯罪的理由，作為該政策的動機。在Windows 95 OSR-2(含)之後的所有Windows版本亦皆內藏NSAKEY，使得美國國安局可以在任何未具特別防範措施的Windows電腦裏，輕易植入未經授權的安全服務程式模組，有效地侵害整個作業系統。[39]

美國中央情報局前局長James Woolsey在2013年3月17日接受《華爾街日報》採訪時稱Echelon成為經濟諜戰的工具，是因為某些外國人不遵守美國的《反海外腐敗法》而行賄。[40] Echelon的偵查對象之一就是這些充當掮客的第三方非美國公司—即使這

圖2　第六眼，以色列耶路撒冷最高點橄欖山北峰Mount Scopus(מִי פּוֹצֵ ה רֵ ה)斯科普斯山情報站
(Secret NSA satellite base on Jerusalem's Mt. Scopus)

資料來源：Richard Silverstein, "Secret NSA Satellite Facility Located at IDF Base in Occupied East Jerusalem", *Tikun Olam-תלונ זוקית*, February 10, 2014 <http://www.richardsilverstein.com/2014/02/10/secret-nsa-satellite-facility-located-in-jerusalem/>

39 不只這樣，電腦安全專家尚一直關切Windows作業系統標準的一個安全功能檔—ADVAPI.DLL檔截取國家機密、商業資訊及與個人隱私的問題。這個檔案控制包括微軟密碼法應用程式介面(MS-CAPI, Microsoft CryptographicAPI)的安全功能，其本來是用來認證經微軟簽名的程式模組，使其可以主動在Windows電腦上獲得執行的權限。<http://ckhung0.blogspot.tw/2013/07/nsakey.html> <http://web.archive.org/web/20000617163417/http://www.cryptonym.com/hottopics/msft-nsa/msft-nsa.html>（檢索日期：2014年4月25日）

40 "The NSA, the FCPA and Parallels of History", *TRACE*, June 21, 2013, <http://traceblog.org/2013/06/21/the-nsa-the-fcpa-and-parallels-of-history/>（檢索日期：2014年4月27日）FCPA為美國國內法，其效力的發揮實際上建立

些非美國公司不是《反海外腐敗法》(FCPA enforcement, Foreign corrupt practice act of 1977)的直接執法對象，但它們亦可能作為共謀犯和從犯受到該法查處而大幅延伸控管管轄及執法裁罰領域。[41]

美國領導Echelon，與英、澳、加、紐的五眼聯盟情報機構聯合操縱。而隱匿之第「六眼」實際上處以色列：由以色列情報及特殊使命局(מידיקפתלו ויעידומל דסומה מידחוימ，HaMossad leModi□in uleTafkidim Meyu□adim; The Institute for Intelligence and Special Operations)，又譯「情報特務局」，俗稱「摩薩德」(דסומה; the Mossad)、耶路撒冷中心所羅門聖殿(שדקמה תיב; Beyt Ha'Mikdash)情報站暨耶路撒冷猶太教及基督教宗教聖地，希伯來大學校園所在地橄欖山之最高點北峰之斯科普斯山之情報站（希伯來語：מיפוצה רה; 阿拉伯語：فراش المبج; 英語：Mount Scopus）等構成。[42]

二、「稜鏡」間諜網絡

1952年，杜魯門以總統令方式成立NSA，但該總統令至今仍屬機密。美國政府直到1957年才不得不承認NSA的存在。NSA原來的任務是收集美國信號情報(SIGINT)和維護通訊安全，到雷根總統時期，其基本任務增加訊息系統安全及安全工作培訓。1986年的一項法律，讓NSA承擔支持國防部作戰的任務，這項額外的任務，連同2008年的《外國情報監督法(FISA)修正案》，為NSA擴權大開方便之門。原本，1978年版《外國情報監督法案(FISA)》對蒐集電子情報有嚴格規定，包括創建一個特殊的法庭來處理NSA對與美國敵對的人員進行電子監控的請求。但修正案從根本上增大執法機構的監聽權限，並減少了FISA法庭在國際案件中的義務，規定它們只須審閱監聽申請的一般形式程序，而無須了解置喙案件的詳細情況。更為強大的是，前揭所述關於美國於1948年在全球範圍內建立代號為梯陣監聽網絡：偵蒐這世界上每一段對話以及每一種行為的內容。

2007年，美國國會在白宮的強大壓力下，通過《保護美國法案》，將FISA中無線電國際監聽無須授權的規定擴展到所有通訊

在屬人管轄基礎之上。FCPA的國際化的一個主要途徑是通過國際組織形成多邊公約，成果體現在：1996年3月29日OAS通過的《美洲間反腐敗公約》、1997年11月21日OECD通過的《反對在國際商事交易中向外國官員行賄公約》以及2003年12月9日UN通過的《聯合國反腐敗公約》。根據OECD的公約，美國又對FCPA進行了修訂，從1998年起，該法對於在美國境內向國外政府官員行賄的外國公司和個人也適用。FCPA國際化的另一個補充途徑是，當FCPA多邊化受挫時，美國可以利用1974年貿易法第301條款對那些認同賄賂為正常業務模式或未有效阻止本國公司利用賄賂獲取合同的國家進行制裁。當然，美國這種單邊主義做法在WTO體系下會受到嚴重的質疑。但早在柯林頓執政時期，國會已經認定賄賂和腐敗屬第301條款中貿易壁壘之範疇，因此，並不能完全排除這種可能性。

41 Henry Chen, "Threat Assessment: PRISM AND FCPA Enforcement", July 2, 2013, <http://www.fcpablog.com/blog/2013/7/2/threat-assessment-prism-and-fcpa-enforcement.html#>（檢索日期：2014年5月5日）

42 Richard Silverstein, "NSA Maintains Secret "Five Eyes" Satellite Facility in Israel", February 9, 2014, <http://www.richardsilverstein.com/2014/02/09/nsa-maintains-satellite-facility-in-israel/>; Richard Silverstein, "Secret NSA Satellite Facility Located at IDF Base in Occupied East Jerusalem", February 10, 2014, *liveleak*, <http://www.liveleak.com/view?i=a3f_1392383537>（檢索日期：2014年5月2日）

方式。在美國國家情報總監和司法部長共同簽署證書的情況下，即使沒有FISA法庭的命令，NSA也可以對在美國之外的人進行情報監聽。這一臨時授權在2008年2月16日到期，但美國會於2008年7月FISA修正案中重新授權，並在2012年9月再次延長5年。這樣，始於小布希時期的稜鏡計畫，被歐巴馬政府全盤接收並上綱擴張。監聽架構沒有那位歐巴馬之前的美國總統如此有系統地展開追蹤。

國際上，如歐盟沒有意識到出於政治目的的大範圍監控居然是可能的。直到2011年年中，包括歐盟委員會、各國的立法機構以及歐盟議會在內，沒有人了解美國的2008年外國情報監視法修正法案（代號為FISAAA 1881a）為何物，而此時，美國對外情報監控條款卻已生效3年。FISAAA結合距今13年的《愛國者法案》，有效地允許未經授權的監視包括存儲於雲端中的數據，凌駕大國之間，且2012年又被歐巴馬總統延展5年。[43]

一般人將絕大部分注意力繼續集中在2001年的《愛國者法案》，但1881a節的監控威力其實最猛烈，它瞄準的是「雲」，使得美國基本上能在美國電子情資網路雲端可以觸及的範圍內，截獲外國人的電子資訊數據而進行純粹的政治監察。

倘按斯諾登2013年6月向《華盛頓郵報》、英國《衛報》[44]披露「稜鏡」(PRISM)計畫之醜聞檔案探察，可謂超乎揣議。[45] 不啻證實美國政府確實設有完整網路監控系統能截取任何資訊，NSA違反國際習慣法上外交特權與豁免竊聽多達38國駐美大使館、多國駐聯合國代表團及駐美機構，並對中國及全球各敏感熱點進行常態網路監控外，而且揭露最早成立於2009年，至2011年開始全面正式運作名為「MYSTIC」和「RETRO」回溯的監聽系統，竟能攔截和錄製數十億筆電話語音內容，並且能夠逐步用最新的內容置換最早內容，數據至多可保存30天。MYSTIC架構中，甚至可監控和存儲某整個外國100%的電話內容，提供五個國家的廣泛原始數據存取和保存，且美方還計畫再增加一國。[46] 遑論美國繼2012年SOPA《線上盜版防制法案》(Stop Online Piracy Act)後，2013年再祭出侵襲閾度更大的《網路情報分享及保護法》(CISPA，Cyber Intelligence Sharing and Protection Act)試圖賦予企業與政府截取個人更多隱私。

一時之間，世界政要對美跨境監聽人人自危。斯氏文件說，從2012年12月10日至2013年1月8日，NSA在30天中對法國公民的

43〈雲計算與法律迷霧〉，《企業網D1Net》，2013年2月20日，<http://www.d1net.com/cloud/news/204285.html>（檢索日期：2014年4月26日）

44 <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>（檢索日期：2014年4月25日）

45 “Plaintiffs' Federal Rule Of Evidence Section 1006 Summary Of Voluminous Evidence Filed In Support Of Their Motion For Partial Summary Judgment”, *EFF*, <https://www.eff.org/files/filenode/Jewel%20Conformed%20Summary%20of%20Evidence.pdf>; “Jewel v. NSA Case No. 08-CV-4373-JSW 53”, <https://www.eff.org/nsa-spying/timeline>, *Electronic Frontier Foundation*.（檢索日期：2014年4月25日）

46 Douglas Ernst, “Snowden: NSA program MYSTIC culls 100 percent of phone records from foreign country”, *The Washington Post*, March 18, 2014, <http://www.washingtontimes.com/news/2014/mar/18/snowden-nsa-program-mystic-culls-100-percent-phone/>（檢索日期：2014年4月27日）

7,030萬個電話通話進行了大規模錄音監控。為此，法國總統François Hollande連夜致電歐巴馬嚴厲譴責。義大利總理Enrico Letta在會晤訪問歐洲的美國務卿John Forbes Kerry時，也要求美國解釋監控義大利公民問題。當晚，德國總理Angela Merkel更致電歐巴馬質問NSA是否在監聽她的手機。

為加強全球反恐，美國秘密進行恐怖分子監聽計畫(Terrorist Surveillance Program)。4年後《紐約時報》曝光這個秘密監聽計畫，引起軒然大波。[47] 公眾赫然發現該計畫的主要內容即授權NSA監聽或攔截：⑴美國公民與其他國家之間來往的電話或電子郵件；⑵政府有「合理理由」相信與恐怖襲擊有關的某人發出或接收的電話或電子郵件。人們認為該計畫擴大警察監聽權力，無須搜查證就可以進行監聽。

美國在2001年的911恐怖攻擊事件後，公眾輿論聚焦於國家安全議題，2001年當時沒有經過聽證會，沒有任何會議討論和斟酌，就交付表決，法案遂以壓倒性優勢通過。共和黨的布希政府於同年10月26日批准通過《愛國者法》(Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001)，[48] 制定當時於參眾兩院都獲得高票支持，賦予執法和情報機構廣泛權力。愛國者法的通過標誌著「無證監聽」正式合法。美聯邦參議院又於2011年12月11日以93比7票，通過新年度6,600億美元的國防預算案，其中之條文包括批准對涉嫌恐怖分子，包括美國公民在內，可以不必提出起訴，便施以無限期拘留。[49]

《愛國者法》第206條規定應當在1978年的《FISA》基礎上增大監視力度；第201條規定當局有權截取與恐怖主義相關通訊。第207條和第225條規定依照《FISA》的規定對外國勢力代理人的非美國人士進行監視；第214和215條擴大聯邦執法部門監測權力，將國際恐怖主義和外國情報活動納入其監視範圍；第216條規定允許使用捕獲裝置和跟蹤裝置等監視恐怖主義活動使得《通訊監視法》的規定不但適用於可以用來截取電腦網絡對話來源，且可以截取內容；第218條放寬聯邦執法部門根據《FISA》獲得監視證的標準，用「重要目的」取代《愛國者法》規定的「主要目的」；此外《綜合控制犯罪和街道安全法》第三編規定總統有權為獲得外國情報信息授予沒有法庭令狀的偵查行為合法偵查權，這一點也為美國領導人以反恐的名義將《愛國者法》變成自己的政治工具賦予法律根據。

另外網上無國界，《2007年保護美國法案》的出現賦予美國情報部門當然納入如hotmail、MSN等平臺上聚集外國用戶之特權：在不需要獲得外國情報監視法庭(Foreign Surveillance Intelligence Court)的令狀下即可攔截經由美國領土內的電訊設施轉接的「外國—外國」電訊；攔截和記錄「被合理認為處在美國領土以外的」相關人員電訊；監聽列為調查對象之接聽電話者跨國電話。毋

47 同註3。

48 HR 3162 RDS, 107th CONGRESS, 1st Session, IN THE SENATE OF THE UNITEDSTATES, October 24, 2001. Citations: Public Law: 107-56, U.S. Statutesat Large: 115 Stat. 272 (2001).

49 張文貞、葉俊榮、王必芳，《緊急狀態法制之探討行政院研究「RDEC-095-18委託研究報告」》（臺北：行政院研究發展考核委員會，2005年10月），頁17-23。

庸置疑，該法案使美國政府監視範圍無遠弗屆，由此，美國政府能夠「合法」監視訊息的範圍已經遠遠逾越美國疆界。

布希總統任內，司法部長James Comey與司法部領導官員原於2004年3月12日請辭，因為他們認為電子監視的命令違法。事實上在2004年司法部長John Ashcroft生病，Comey代理部長，拒絕重新授權不需法庭令狀即進行監聽。白宮法律顧問Alberto Gonzales和白宮幕僚長Andrew Card企圖利用Ashcroft病弱要他簽字，Comey聞訊旋即趕到醫院病房攔阻。[50]

布希曾為挽留終止原意是秘密收集外國情報卻已跨入國內領域的恒星風(Stellar Wind)電子監控計畫。諷刺的是，歐巴馬在競選總統期間曾經批評，但就在他出任美國總統後，這些電子監控項目席捲重來。而且，「恒星風」甚至由一變四。作為超強獨霸國家，美動用情蒐四大渠道：「稜鏡」(PRISM)、大道(MAINWAY)、船塢(MARINA)、核子(NUCLEON)計畫。前兩項「大道」計畫、「船塢」計畫，目的是在蒐集電話及網路的「元數據」；後兩項「核子」計畫、「稜鏡」計畫，則是截取電話及網路溝通的訊息內容。

美國司法部副部長James Cole曾宣稱「對美國公民通話記錄的大規模收集並不受憲法第四修正案關於不合理搜查和逮捕條款的保護。」[51] 不過電郵元數據有所不同。英國《衛報》披露在2009年3月NSA監察長極機密報告中曾闡明這一網絡元數據收集之目的，[52] 目的被稱作「數據挖掘」，而NSA則稱作「關係鏈分析」。NSA分析目標人物的二度關係網絡。換句話說，目標人物的連絡人的連絡人都會被關注。在911事件之前，元數據「關係鏈分析」在NSA內部是被禁止的。[53] 但現NSA收集範圍全面拓展至整個現代電訊，並且取得異乎尋常的高速發展，同

50 Dan Eggen and Paul Kane,“Gonzales Hospital Episode Detailed”, *The Washington Post*, May 16, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500864.html>;“George Bush PERSONALLY Sent Card and Gonzales to Thug Up Ashcroft”, *emptywheel*, July 10, 2009, <http://emptywheel.firedoglake.com/2009/07/10/george-bush-personally-sent-card-and-gonzales-to-thug-up-ashcroft/>（檢索日期：2014年5月6日）

51〈《衛報》詳解美國國安局元數據收集項目〉，《鉅亨網》，2013, 6/28, <http://news.cnyes.com/content/20130628/kh8k8k9hnml9i_2.shtml>（檢索日期：2014年4月27日）

52“NSA inspector general report on email and internet data collection under Stellar Wind-full document Top-secret draft report from 2009 by the NSA's inspector general shows development of‘collection of bulk internet metadata’ under program launched under Bush”, THE GUARDIAN., 27 June 2013, <http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection>（檢索日期：2014年4月29日）

53 Glenn Greenwald and Spencer Ackerman,“NSA collected US email records in bulk for more than two years under Obama Secret program launched by Bush continued‘until 2011’ Fisa court renewed collection order every 90 daysCurrent NSA programs still mine US internet metadata”, *The Guardian*, 27 June 2013, <http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama>（檢索日期：2014年4月29日）
NSA獲得更大權力，在2007年11月27日的一份法律備忘錄中由美國助理司法部長Kenneth Wainstein發給上司，時任司法部長Michael Mukasey當時上任僅幾週。這份備忘錄的目的是告知穆凱西，五角大廈認為這些電子郵件元數據收集項目限制了NSA可以分析的電子郵件的範圍限制是過多的，而NSA希望獲得進一步授權，深入到美國公民的電子郵件記錄中進行關係鏈分析。這一程序將明確，NSA可以分析與美國公民或美

時，美國與情報和監視相關的法規和監視行為已從針對具體嫌疑人，轉向系統化龐大規模訊息偵蒐。事實上騰訊聊天軟件QQ和中國移動的即時通訊飛信赫然也在NSA的監視範圍之列。NSA自2010年起開始最主要特色在於能選擇性進行監聽TURBINE的大規模監聽計畫，自動整合被侵入對象特徵，減少監聽範圍並通過中間人攻擊偽造臉譜(Facebook)網站入侵用戶電腦。

參、國際上對此「梯陣」、「稜鏡」間諜網絡問題之國家反應

梯陣竊聽案爆發後，參議院情報委員會主席Dianne Feinstein即由力挺監控計畫，驟變強調不知道NSA監控外國領袖，要求全面檢討監控計畫，此間發展閃爍其辭，態度上善變游移。

一、主要盟邦

加拿大：加拿大則參與監控巴西石油公司(Petrobras)與礦能部等事件。

但2014年4月，加拿大國稅部因為「心淌血」(Heartbleed)安全漏洞暫停網上報稅，全球三分二網站廣泛使用的OpenSSL加密軟件，揭發漏洞後，引起全球關注及恐慌，美國國家安全局(NSA)早在兩年已經知道加拿大國稅部出現保安漏洞，但一直秘而不宣，反而將計就計利用這個漏洞發動攻擊，竊取密碼和機密情報。[54] 美方嚴詞否認對前揭OpenSSL漏洞有任何知悉。[55]

英國：歐盟看似咄咄逼人的態度，讓英國保守黨人士極為憤怒，認德、法正發起試圖破壞英美特殊關係的運動：歐盟試圖對英美進行政治迫害。他們強烈要求英政府譴責歐盟內操縱這次調查的國家。英國政府亦擬《電子商業法案(Electronic Commerce Bill)》賦予執法權力。為偵查犯罪，故第三者有交出使用者編密金鑰予執法部門的義務。

英國衛報揭露，根據斯諾登檔案，英國國家通訊情報局從海底光纜中截獲往來英國的所有電郵、電話和密碼。英國和美國情報機關聯手在2009年英國主辦G20期間與美國聯手竊聽與會者的電話，設置假網咖擷取電子通訊，每臺電腦均安裝木馬程式，竊錄帳密，秘密監控與會領袖代表，連友邦南非也不放過。[56]

在2007顳顬計畫兩年後的2010年，英國在五眼聯盟中重新取得優勢地位，並聲稱在這五個成員中擁有最大的網路接入量。如今，英國提供數量龐大的元數據，稱已遠遠超過美國國家安全局。

二、美洲國家

巴西：美NSA曾監控巴西女總統Dilma

國國內人士相關的通訊元數據。2007年，美國國防部長Robert Gates簽署關於網路元數據的補充程序，包括如何處理關係上美國公民的數據。

54 Sebastian Anthony, "The NSA knew about and exploited the Heartbleed bug for 'at least two years", April 14, 2014, *Extremetech*, <http://www.extremetech.com/extreme/180435-the-nsa-knew-about-and-exploited-the-heartbleed-bug-for-at-least-two-years>（檢索日期：2014年4月28日）

55 "NSA denies Heartbleed bug awareness", *BTT*, 14th April 2014, <http://bttcomms.com/blog/support/nsa-denies-heartbleed-bug-awareness>（檢索日期：2014年4月27日）

56 Verge Staff, "Everything you need to know about PRISM", *the verge*, July 17, 2013, <http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet> <http://www.nationaljournal.com/nationalsecurity/why-prism-is-different-and-scarier-than-other-nsa-spying-20130607>

Vana Rousseff，而因美未公開致歉，羅塞芙擬取消原訂2013年10月23日訪美行程暨撤銷對美Brazilian Folha de S. Paulo daily reported F-18先進超級大黃蜂(F-18 Super Hornet)戰鬥機高達40億美金之軍購案、無線推遲與美方討論原油和生物燃料技術合作等舉措抵制。[57]

墨西哥：同樣地，美亦監控墨西哥Enrique Peña Nieto，[58] 旋遭墨西哥外長召見美國駐墨大使譴責其窺竊電郵情資。

三、亞洲國家

韓國：通過截取從釜山通往亞洲其他地區的海底通訊網傳輸的情報，說明進行地區竊聽。為此，韓國的國家情報院與澳大利亞的安全情報局(ASIO)有著30多年的緊密協作。作為世界上最重要的通訊樞紐之一。

新加坡也從70年代開始成為「五眼」的眼線。澳大利亞情報機構國防信號局與新加坡情報機構展開合作，共同竊聽SEA-ME-WE-3電纜國際電信通道。該電纜始於日本，經新、吉布地、埃及、直布羅陀海峽通往德北部，由國有運營商新加坡電信鋪設。

四、歐洲各國

歐盟：歐洲聯盟於2002年10月23日歐洲議會召開聽證會(參照Verbatim report of proceedings SITTING OF WEDNESDAY, 23 OCTOBER 2002)並作出表決且提出提案Motions for resolutions-Echelon (*B5-0528/2002, B5-0562/2002, B5-0564/2002, B5*-0565/2002)並終於在2002年11月7日完成07/11/2002 T5-0530/2002決議。

早在2000年2月，歐洲議會公民自由與權利委員會即通過「監視技術的發展暨濫用經濟資訊的風險」決議，義大利、丹麥國會展開調查。而民間網路業者更發動傳訊超載阻斷以抵制間諜情報網的監控。然基於共同安全防衛政策建軍防務與經濟上同美國合作的需要，[59] 歐盟的抵制譴責，實際上無能為力、成效有限。[60] 按前揭歐洲聯盟07/11/2002 T5-0530/2002決議文內容闡述：「歐洲議會通過對梯陣的決議，遺憾的是理事會和委員會未能充分踐行臨時委員會提出的建議。進一步的措施是必要的，以保護公民和企業對通訊的截取的濫用和非法使用以保障通訊的私密性，並引入對商業間諜和競爭情報的濫用管制措施。成員國應被要求在它們之間進行合作，訊息與共同安全與防務政策方面增加效益的目的的交換。議會堅持認為，應採取措施以提供所有歐洲公民提供涉及隱私的保護同等的法律保障，同時嚴格尊重歐盟Acquis Communautaire即目前歐盟依照的法律，包括歐盟所有的權利和義務與《歐盟立法、條約和裁決彙編》(the accumulated legislation, legal acts, and court decisions which constitute the body of European Union law)所揭示的的合法權利，並考慮到歐盟基本權利憲章。特別是與美國的溝通和對間諜措施攔截

57 "Brazil's President Dilma Rousseff cancel US visit if she doesn't receive public apologies for cyber spying", *ITAR-TASS*, September 05 2013, <http://www.itar-tass.com/en/c32/865244.html>（檢索日期：2014年4月26日）

58 Yossi Melman, "The NSA affair and the dogmatic notion of privatization", October 28th 2013, *i24news*, <http://www.i24news.tv/en/opinion/131027-the-nsa-affair-and-the-dogmatic-notion-of-privatization>（檢索日期：2014年4月21日）

59 <http://cpunks.files.wordpress.com/2013/09/echelon.pdf>（檢索日期：2014年4月29日）

60 <http://www.europarl.europa.eu/portal/en/search?q=echelon>（檢索日期：2014年5月6日）

的濫用應該有國際協定。關於歐洲未來的公約要求制定保證成員國將致力於禁止，或不積極參與（直接或根據第三方）的間諜活動的建議。最後，關於建立協調的歐洲情報活動和引進這些活動的民主審議進展甚微，建議必須很快在這一領域會談」。

因此歐洲議會「梯陣」系統調查臨時委員會副主席Elly Plooij-Van Gorsel在2001年7月宣佈解散會議中乃表示：「瑞典Göteborg高峰會剛開過，會中再次強調與美國關係的重要性。」「布希給我們帶來了『梯陣』系統的麻煩，但是歐美關係依然問題重重。我們無法阻止美國窺探我們的秘密。」

瑞典：情報機構國防無線電局(FORSVARETS RADIOANSTALT, FRA)不但幫助美國國安局監視俄羅斯政府機構和官員(NSA Sweden FRA XKeyscore Plan-Cryptome)，[61] 對俄羅斯民間目標也很關注，包括監視俄羅斯國家石油財團(Gazprom)能源公司；瑞典是五眼聯盟在歐洲的最大合作者，因為其可以直接侵入波羅的海電纜。

法國：法國司法部長Elisabeth Guigou曾聲籲說：當年這個網路是用來監測來自蘇聯和東歐國家的情報，但現在看來，它已被用於蒐集經濟情報並監測競爭對手。巴黎檢察官Jean-Pierre Dintilhac據歐洲議員Thierry Jean-Pierre則向歐洲議會提出訴訟要求，他表示，具備對國家基本利益造成直接危害的能力，也將危及通訊的隱私。2000年7月5日歐洲議會通過投票決定，成立臨時調查委員會，並將邀請歐洲相關國家的代表共同研究對付Echelon的措施。[62] 法國巴黎檢察院則授權情報反間諜機構「本土警戒局」(La Direction de la Surveillance du territoire (DST))進行預備性偵辦。[63]

德國：Echelon系統為美、加、英、紐、澳等國監聽廣電及電子郵件通訊的全球性監聽設施網路；其在德國境內的設備位於慕尼克附近的Bad Aibling。Jelle van Buuren，撰文*Dutch Government Says Echelon Exists*, Heise Telepolis, Jan. 20, 2001 (http://www.heise.de/tp/)與*Hearing On Echelon In Dutch Parliament*, Heise Telepolis, Jan. 23, 2001 (http://www.heise.de/tp/)深入報導此監聽攔截系統。

在調查「梯陣」偵聽系統的歐洲議會臨時委員會，[64] 德國綠黨成員Ilka SCHRÖDER懷疑歐洲建立自己名為「ENFOPOL」系統，其中包括諸如信用卡資訊和IP埠等敏感領域對歐盟的所有人進行徹底的即時監控。她認為，所有秘密機構本質上都是不可信的，應被解散。她反對「梯陣」調查委員會試圖通過某種法律漏洞將這個五眼攜手合作的衛星

61 <http://cryptome.org/2013/12/nsa-se-fra-xkeyscore.pdf>（檢索日期：2014年4月25日）

62 Steve James, "Revelations about Echelon spy network intensify US-European tensions", *World Socialist Web Site*, <https://www.wsws.org/en/articles/2000/04/spy-a12.html>
"French Prosecutor Begins Probe of United States' 'Echelon' Spy System", July 05, 2000 From Reuters, *Los Angeles Times*, <http://articles.latimes.com/2000/jul/05/news/mn-47859>（檢索日期：2014年4月29日）

63 "Le curieux silence des Français sur Echelon", <http://strategique.free.fr/archives/textes/ech/archives_ech_01.htm>（檢索日期：2014年4月29日）

64 EU Parliament: Decision of 5 July 2000 setting up a temporary committee on the ECHELON interception system, <http://www.fipr.org/rip/EPcommitteeECHELON%20July2000.htm>（檢索日期：2014年4月29日）

偵聽系統引入，甚或以世貿組織為藉口。「這不是個法律問題。秘密機構已經屢次侵犯法律，不能僅靠立法了事。任何民主的控制都使秘密機構更加合法化。」德國議員Erika Mann在歐洲議會調查臨時委員會上重申觀點。她說：「應該投入必要的資金到解密技術上，這和加密技術同樣重要。」[65]

針對懷疑美國公司通過竊聽法蘭克福網路交換中心DeCIX這一事宜，德國檢察長已被證實要調查其中潛在的間諜活動。

丹麥：丹麥國防部長Hans Hækkerup在國會承認丹麥軍情局FE(Intelligence Agency of the Danish Armed Forces)納入全球電子監測系統之中。Bo Elkjær and Kenan Seeberg則撰GÅDEN OM ECHELON一書探討間諜監測暨資訊攔截問題。丹麥為第三邊國家，因此丹麥國會[66]對此並不採嚴格譴責立場。

比利時：發佈報告書Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé“Echelon”[67]自2011年起，美國情報機構就對比利時電信公司進行駭客入侵，2013年7月，比利時電信公司發現其內網設備存在「安全後門」，電信網路數據被「不明身分的第三方」不定期向外洩露。懷疑美國情報機構所為。比利時電信將此提交比利時聯邦檢察院，檢察院已證實，竊取比利時電信網路數據所使用的技術表明存在美國的高度介入行為，入侵的駭客擁有強大的金融資源和後勤支持，並使用了特殊的惡意軟件和高超的密碼技術。

駭客入侵比利時電信網路的目的主要是竊取戰略訊息，駭客主要攻擊對象是連接歐洲與中東的亞歐三號海底光纜。2013年9月16日，比利時首相Elio Di Rupo、內政大臣Joëlle Milquet和司法大臣Annemie Turtelboom)發表聯合聲明，對比利時電信公司可能遭美國情報機構入侵一事做出明確而強硬回應，一經確認是網路間諜襲擊，比利時政府會予以強烈譴責並採取相應措施。

西班牙：美國試圖要使西班牙納入全球監聽系統網絡以分享。(Isambard Wilkinson, *US wins Spain's favour with offer to share spy network material*, Sydney Morning Herald, June 18,2001(http://www.smh.com.au/news/0106/18/text/world11.html).)

義大利：在調查「梯陣」(Echelon)偵聽系統的歐洲議會臨時委員會，義大利成員Maurizio Turco聲稱：「事實上，歐洲之所以這麼做是為了轉移人們的注意力，而同時自己設立一套這樣的偵聽系統。」委員會主席Carlos Coelho對此言不屑一顧。最終，委員會延遲對長達113頁的「梯陣」偵聽系統最終報告的討論。該報告由德國成員Gerhard Schmid負責。是否向美國就「梯陣」偵聽系統提出正式抗議的投票被推遲到2001年7月3日進行。

對於監聽竊資案，2013年7月義總統Giorgio Napolitano和外交部長Emma Bonino均表示美應合理回應。國防部長Mario Mauro則稱傳聞屬實將影響義、美關係，然之後義

65 Steve Kettmann,“Does Europe Covet Own Echelon?”, *WIRED*, 2001. 6. 20. <http://archive.wired.com/politics/law/news/2001/06/44689>（檢索日期：2014年4月29日）

66 丹麥ECHELON-SURVEILLANCE-CRYPTOGRAPHY-INTELLIGENCE網站<http://www.datashopper.dk/~boo/index.html>; <http://www.folketinget.dk/>

67 <http://www.datashopper.dk/~boo/EchelonBelgium.pdf>

美關係漸歸常態。

瑞士：Digital Allmend、Swiss Pirates和瑞士混亂電腦俱樂部(Swiss Chaos Computer Club)都是Digitale Gesellschaft基金會成員，該基金會還想要檢察署以非法收集訊息和入侵電腦系統（分別為《刑法典》第143條和143條之2）為由進行調查。瑞士隱私基金會Digitale Gesellschaft力爭對違反瑞士法律的外國情報機構提起法律訴訟。同時，美國法官2013年7月9日裁決電子前沿基金會(EFF)針對NSA的訴訟能繼續進行。歐盟在華盛頓提起稜鏡門事件，而巴西已對美國在巴西進行間諜活動展開調查。瑞士隱私基金會在2013年7月7日寫給瑞士聯邦檢察署的信中指出非法情報機構疑觸犯瑞士聯邦法律。基金會在給聯邦檢察長的信中指出，根據近來媒體對「稜鏡」和「顳顬」(Tempora)之類的監控行動，有充分的理由質疑《瑞士刑法典》中有關政治、經濟和軍事間諜活動的第271、272和273條受到他國侵犯。

肆、我國切身面臨之威脅：網絡諜戰及情資監控

當前我國家安全不啻曝露在全球、且在對岸隱密監控的風險環境中。敵對中國的威脅無比明確、嚴重且急迫。

現我國電信事業主管機關國家通訊傳播委員會(NCC)針對網路資安問題，並無情報與使用的政策工具。但中共具資訊戰力，已建立如解放軍電子科技學院、總參謀部第三分部與資訊戰模擬中心等機構，且當前解放軍四大總部、七大軍區均設有網軍部隊。中國網軍大本營為中國人民解放軍61398、61486部隊，後者又被稱為「推桿熊貓」(Putter Panda)駭客小組，前述兩者皆隸屬上海共軍總參謀部三部（技術偵察部）；而中國信息大學作為訓練基地，也是中國發動網攻之要角。共軍「非接觸先敵攻擊」參演部隊曾加入北京軍區第38集團軍數字化合成營。[68] 中國大陸自1985年起，就開始發展「網電一體戰」的能量。共軍已經組建一支超過10萬人的網路部隊，而其目標是在2020年建立全球第一支「信息化武裝部隊」。

中國將網路戰發展成整合軍事、情報、研發等部門，已從理論走向實務，企圖直擊美國通訊網路基礎建設，掌握發動攻擊入口，進一步癱瘓後勤，攻擊供應鏈，包括運輸、物流、金融業者等。共軍曾對美國、我國重要基礎設施，包括電網、金融、空管、傳媒進行過網絡攻擊、植入木馬程式及截取情資，此無異發動侵略戰爭。

我國安局從受攻擊對象分析發現，已由政府機關、駐外館處，擴展到民間智庫、電信業者與委外廠商等。資安問題涉及層面甚廣，包括金融、電信、通訊、陸海空交通等，因此，更必須立法加強國家關鍵基礎設施及其供應鏈風險反制。

伍、間諜網絡引發之爭議癥結、反思及國安曝險防範—代結語

國家安全議題因重視制敵機先，已提升至平時預警監測、訊息篩濾與符碼攔截的全球間諜情報網絡為主（以SIGINT為代表），

68〈我軍6月下旬將舉行首次新型作戰力量聯合演練　數字化合成營首次公開亮相〉，《新華網》，2013年5月28日，<http://news.xinhuanet.com/mil/2013-05/28/c_124777402.htm>（檢索日期：2014年5月14日）

大幅依賴情報資訊截獲的高科技轉移，911後因反恐襲目的更顯盛行，惟安全與自由間平衡與否？如何取捨？全球安全之隱蔽操縱，涵蓋涉及「外國勢力活動」之全球政商領域並疊覆民眾隱私侵犯虞慮等忌諱地帶，動輒得咎，業引發諸多爭議如㈠美國最高法院拒絕複審無證監聽案、㈡國家安全與公民基本權的衝突及㈢國際對峙、外交齟齬。

2001年美國911之後，為保護國家安全，美政府強化監控力度。2005年，總統布希多次授權國家安全局(NSA)，在無令狀的情況下監控美國內人民的電話和電子通訊。以美國民權聯盟(ACLU)為首的社會組織認為無證監聽違反美國憲法，遂於2006年1月提起了ACLU v. NSA案。2006年8月，地區法院判決國家安全局的活動違反了美國憲法第一修正案、第四修正案和《1978年國外情報監聽法》。

然而，2007年9月，第六巡迴上訴法院撤銷該案，理由是由學者、記者和非政府組織構成的原告欠缺訴訟資格，因為他們無證據表明其遭受到國安局監聽。因此，法院並未對國家安全局的監聽行為是否違憲做出實質判斷，當然也未支持其合法性。2007年10月，ACLU再向美國最高法院提起上訴。2008年2月，最高法院拒絕審理該案，理由同樣是原告沒有訴訟資格。[69] 就是形式上將此爭辯擱置、懸宕不決。

2008年8月，美國國會通過《外國情報監督法修正法》(FISA Amendments Act of 2008)授權國家安全局在沒有法院令狀的情況下監聽美國公民。該法改變了以前由總統通過發佈行政命令實施秘密監聽的作法，在法律層面認可其合法性，但其合憲性問題的爭論日趨激烈。在歐巴馬政府任期內，秘密監聽的問題未得到解決。因為在歐巴馬總統競選期間，保證不會如布希政府那樣在無司法令狀的情況下對美國公民進行監聽，但是他卻又支持監聽修正法通過。美國電子前哨基金會(Electronic Frontier Foundation)甚至認為，歐巴馬政府在監聽上立場比上屆的布希政府更顯惡劣。

2009年4月3日，歐巴馬政府針對2008年提起Jewel v. NSA案，向法院提出動議，指出法院對繫爭問題無管轄權，要求法院撤銷訴訟，因為國會未放棄豁免特權，因此，在先進國家如德、美，政府的通訊監聽都具有基本的國會立法作為依據，以符合民主的多數決原則及法律保留原則，爭議的焦點僅是是否符合比例原則。在此種微妙環境下，未形成可用司法先例，法官心證特別是最高法院法官們如何做出司法闡釋值得探究。在期待判例之前，分析立法機關內政黨競爭、利益鬥爭和社會團體的角力，未來更有學術積累、研究方向上之重要意義。[70]

掌控情資網絡者之立場，蓋認為只要裨益於自己的經濟和政治利益，在外國領土上實施網絡監控，合情合理。身處新的和正在湧現的威脅經常藏匿在全球龐大而複雜的現代通訊系統中，美國認為基於安全戰略必

69 Jeralyn,“Supreme Court Refuses Review of NSA Wiretapping Case”, Feb 19, 2008, <http://www.talkleft.com/story/2008/2/19/11029/2163/supremecourt/Supreme-Court-Refuses-Review-of-NSA-Wiretapping-Case>;“Supreme Court Denies Cert in ACLU v. NSA”, <http://www.techlawjournal.com/topstories/2008/20080219.asp>

70 楊會永，〈反恐中的憲法問題：個人訊息保護〉，《法中論壇—中國法學平臺法中論壇》，<http://www.jurachina.cn/forum.php?mod=viewthread&tid=445&page=1>

須在特定情況下蒐集、儲貯及追溯檢索大量的信號情報，以發現並甄別這些威脅。NSA對於某些國家和地區實施的信號情報蒐集活動是為了提升美國國家安全和外交利益，同時保護美國及其盟友的國家安全。但辯論的另一方，則認為對於網絡間諜活動，實際上斷難區分出：所謂捍衛國家的網絡攻擊，和純為經濟利益。網絡攻擊、無證竊聽及數據挖掘，已侵犯基本人權暨通訊隱私及自由。而內幕作業的「境外情報監督法庭」(FISC)，FISC透過機密裁決，創造整套秘密法律，授權國安局蒐集龐大資訊，不僅用以追蹤嫌疑恐怖分子，更可追查懷疑涉及核技術、間諜或網絡攻擊的人士。由11名成員組成的FISC原本只是審批監聽等搜查令，在幾乎不受公眾監管下，常評估指涉憲法的重大問題，建立重要的法庭先例，權力堪比最高法院(Supreme Court)甚凌駕最高法院而成「太上法院」，其裁決足以影響未來情報機構的運作模式，卻不像最高法院般要向公眾交代，也毋須聽取政府以外的意見更屬悖離民主自由原則。

民主自由需要手段捍衛，如果梯陣、稜鏡是手段，那麼是否該義無反顧維繫國家安全？然間諜網絡一旦使用是否就先斲喪民主自由之內涵或根本價值？又或者公民社會的意見反彈與懷疑其實應服膺在國家利益絕對序位下？公眾事務的參與自由，透過網路平權的架構已被重新釋放，然既有法規範卻造成捍格，回歸民主國家法治本質，應該要能造就多數人最大的權益，並且不去剝奪少數人的核心價值與尊嚴，也就是說應該創造維護一個多數人皆可安心追求人生職志，且脫逸常規的少數人也可不被過份壓迫的生存環境，法應與時俱進，進行根本面的基進反思與動態挪移，方能真正符合社會的需求，凡此均值深思。為兼顧人權，網路監視機制應由國安局在司法部門授權下方得行使。

盱衡實際政局，2013年7月共和黨眾議員阿瑪什(Justin Amash)遞交根據美國憲法第四修正案對政府權力進行限制，杜絕政府機構蒐集非法證據之修正案，要求對國安局監聽民眾電子訊息的行動應有限制。但眾議院在經過激烈辯論後仍以217票反對、205票贊同微弱多數否決該議案而批准國安局繼續電話監聽告終。這一結果無異顯示美國一貫基調暨共和黨保守派和民主黨自由派在這同一問題上罕見的一致：強調國家利益至上。

間諜無所不在、推陳出新，竊聽盜資亦然。網諜企圖竊取機密而入侵範圍也從傳統的國防機密，擴展至交通等基礎民間設施。

中國人民銀行、財政部、國家發改委、銀監會、工信部等政府機關，皆在評估中國商業銀行對IBM伺服器的依賴是否威脅國家金融安全的問題，已由《彭博社》2014年5月報導。評估報告提交給由中共國家主席習近平領導的網路安全小組。中共今年（2014年）初成立中央網路安全和信息化領導小組。而今年5月中旬，中國國家機構政府採購中心更發布《關於進行信息類協議供貨強制節能產品補充招標的通知》，要求中央機關採購的電腦產品不准安裝Win 8。中共近日更要求國營企業切斷與麥肯錫、波士頓諮詢公司等美國顧問公司的聯繫。[71]

省思我國對於開放對岸電訊來臺，或中國之華為、中興通訊及引進小米、紅米手機

71〈中美諜戰升級！傳中國要求銀行棄用IBM伺服器〉，《ETtoday新聞雲》，2014年5月28日，<http://www.

有竊密之虞，卻無任何警覺或戒防，反觀美國，美國會眾議院情報委員會2012年10月8日即曾就此作成調查報告；而亞洲國家如韓國官方更採嚴防立場。[72] 如澳洲基於國安考慮，禁止華為投標澳洲國家寬頻網路；美國也曾拒絕華為收購美國3Com公司，之後再度拒絕華為收購美國伺服器技術公司三葉系統等不一而足。國家通訊傳播委員會(NCC)雖於電信法修正案增訂電信網路資安條款做為管控威脅國家資安的電信設備的法源依據；但設備審驗難度高，尤其時常要軟體升級的大型電信網路設備，採一次性資安審驗，將讓業者先用無害版本通關，日後植入「後門程式」，經常性審驗則難以控制成本。應訂《外國及大陸地區投資與國家安全法案》，並強制政府相關單位對可能影響國家安全的外國（包含中國）電信設備、營運與投資案，先至立院舉行聽證會，接受公開檢驗後始得授權。[73]

是以我方因應措施除應包含既往文獻提出之：[74] 一、具備監偵及反偵蒐全軍節點能力；二、研發難以破解加密技術；三、受創迅速反應復甦之整體戰力；四、建置資訊防護罩系統之資通安全環境；五、結合資訊戰與軍中「指揮、管制、通信、資訊、情報、監視和偵查」(Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance)指管通資情監偵之指揮自動化系統(C^4IS)反制；六、建立臺灣自主的資安產業，並成為國防產業一環；七、建立國家國安層級資訊戰指揮體制；八、政府建立安全分級制落實機密保護，成立「外國及大陸地區投資與國家安全委員會」，由包括國家安全局、法務部等政府單位，聯合審核外國（包含中國）電信設備商與營運商是否威脅國家安全，並向通訊傳播委員會提出建議之外，本文建議更須增加：九、制定《關鍵基礎設施安全防護》與《外國投資與國家安全》等立法並周延國會實質審查權及強制踐行全面聽證程序等；十、提升宏揚政戰諜報專業屬性，統整軍情、國安與政戰單位之資訊編制並以國家層級指揮指管通資情監偵殺(Kill)之(C^4ISK)謀略：以科技迅捷性強化諜戰謀略應變性；以科技針對性強化諜戰謀略奇效性；以科技變動性強化諜戰謀略詭詐性；以科技智慧性強化諜戰謀略準確性；十一、杜絕敵國電訊工程進駐，構建自主獨立電訊與資安產業；十二、國家設立網絡諜戰資訊人才養成與專業機構等。

在國安及建軍備戰上反覘，更應覺知當今「資訊戰」（網際及電訊）襲擊結合「間諜戰」滲透、反間、監控等心態與型態，

---

ettoday.net/news/20140528/362104.htm#ixzz35Xwb0p2G>（檢索日期：2014年6月20日）〈大陸中央機關採購電腦禁裝Windows 8〉，《ETtoday新聞雲》，2014年5月20日，<http://www.ettoday.net/news/20140520/359175.htm#ixzz34POuo79r>（檢索日期：2014年6月18日）

72〈朝鮮日報：韓國引進華為設備引發安全爭議〉，《參考消息》，2014年1月13日，<http://finance.cankaoxiaoxi.com/2014/0113/330714.shtml>（檢索日期：2014年6月19日）

73 財團法人臺灣智庫通訊傳播政策小組，《開放中資與國家資通安全—以「華為」為例》（臺北：財團法人臺灣智庫，2013年5月），頁10-12。

74 楊曉欣，〈中共網軍對我資訊安全威脅之探討〉，《清流月刊》，2007年10月號。<http://webarchive.ncl.edu.tw/archive/disk20/19/90/15/67/78/200806273050/20130113/web/sec.gov.tw/CNCJ/CNCJ0602/cncj0602_09611.html>（檢索日期：2014年6月11日）

業已空前蓬勃且演進至第六種戰爭「網絡諜戰」：以全球為戰場，透過佈建龐大組織系統，無遠弗屆攻擊及阻絕，全面隱密監控且截獲關鍵情報，藉此不對稱侵略、壓制及威懾與其競爭之國家、企業乃至個人，以期鞏固網絡霸權且獲致最大數據掌控地位。工業時代戰略戰是核戰爭，資訊時代戰略戰是網絡戰。敵對中共的網絡諜戰將成我面臨駭資曝險及國家安全最大威脅，亟需統整軍情、國安單位之資訊編制並以國家層級指揮；強化關鍵基礎建設；杜絕敵國電資工程入侵；構建自主獨立電訊與資安產業並納入國防戰略；指管通資情監偵殺系統(C^4ISK)整體反制；厚植應變網軍侵襲、無證竊聽與數據挖掘之抵禦戰力。

同時美國所佈局之全球間諜網絡，對歐亞洲較先進開發國家主要採情報監控觀望並截獲商業、軍情先機；而對非洲、加勒比海盆地地區及亞太國家等衝突熱點與資源產地，除了情資監控外，美國尚佐採海外軍事逼迫就範(Compellence)戰略、區域武力建構與較小規模之應變行動(SSCs)和掌控能源的前進部署，大舉遂行網絡霸權及國家意志。不啻如此，表面上是自由市場之活絡生態，美國的情治單位所建構的全球大數據數位匯流情資監控架構，與財閥(Plutocrats)推展集體內線交易，實際上可說是一個陰謀精算的中央集權體制。

（收件：103年5月14日，接受：103年7月23日）

參考文獻

中文部分

專書

行政院科技顧問組，2010。《2010資通安全政策白皮書》。臺北：中華民國行政院。

東鳥，2014。《數據獵殺：一場輸不起的全球網路戰爭》。臺北：上奇時代。

東鳥，2013。《失控的正當性：揭密斯諾登背後的超規模全球監聽計畫》。臺北：上奇時代。

東鳥，2013。《全球最危險的人物：朱利安・阿桑奇維基解密創辦人阿桑奇，改寫全球人民對公權力的信念》。臺北：上奇時代。

林博文，1999。《歷史的暗流：近代中美關係秘辛》。臺北：元尊出版。

金聖榮，2014。《黑客間諜：揭秘斯諾登背後的高科技情報戰》。湖北：人民出版社。

財團法人臺灣智庫通訊傳播政策小組，2013。《關鍵基礎設施安全條例(CIIP)—國家資通安全的第一哩路》。臺北：財團法人臺灣智庫。

財團法人臺灣智庫通訊傳播政策小組，2013。《開放中資與國家資通安全—以「華為」為例》。臺北：財團法人臺灣智庫。

崔龍中，2013。《中情局長秘密檔案》。湖北：華中科技大學出版社。

張殿清，2001。《情報與反情報》。臺北：時英文化。

張文貞、葉俊榮、王必芳等，2005。《緊急狀態法制之探討行政院研究》。臺北：行政院研究發展考核委員會。

彭慧鸞，2011。《網路安全治理的新紀元從美國網際網路國際戰略談起》。臺北：國立政治大學國際關係研究中心。

隋岩，2014。《竊聽風雲：斯諾登與稜鏡計畫》。中國法制出版社。

專書譯著

Anne-Marie Slaughter，馬占斌、田潔譯，2009。《這才是美國：如何在一個危險的世界中堅守我們的價值》。北京：新星出版社。

Bernard Bourdeix著，高楓楓譯，2010。《世界級陰謀》(Le grand livre des conspirations)。江蘇：人民出版社。

Luke Harding著，何星、周仁華、李廣才、花愛萍、孫志明譯，2014。《斯諾登檔案：世界最大洩密事件內幕揭秘》。北京：金城出版社。

Gordon Thomas著，枝椏譯，2005。《以色列情報局》(*MOSSAD*)。臺北：智庫文化。

Robert Kagan & William Kristol著，楊紫函等譯，2002。《當前威脅：美國外交與國防政策的危機與契機》(*Present Dangers: Crisis and Opportunity in American Foreign and Defense Policy*)。臺北：國防部。

John Arquilla and David Ronfeldt著，楊永生譯，2003。《網路及網路戰》(*Networks and. Netwars: The Future of Terror, Crime, And Militancy*)。臺北：國防部。

Steven Metz著，國防部史政編譯局譯，2002。《美國戰略：美國四年期國防總檢的議題與方案》(*American Strategy: Issues and Alternatives for the Quadrennial Defense Review*)。臺北：國防部。

期刊論文

張明偉，2010/12。〈監聽風雲—以通訊監察進行國家情報工作之規範檢討〉，《軍法專刊》，第56卷第6期，頁164-181。

彭錦珍，2004/12。〈資訊時代中共國防現代化之研究—解放軍信息戰發展及其對臺海安全之衝擊〉，《復興崗學報》，第82期，頁187-218。

廖福特，2006/5。〈是共存，非衝突—歐洲理事會如何平衡打擊恐怖主義與人權保障〉，《月旦法學》，第132期，頁39-57。

廖元豪，2006/4。〈多少罪惡假「國家安全」之名而行？—簡介美國反恐措施對人權之侵蝕〉，《月旦法學》，131期，頁38-39。

趙國材，2013/10。〈人類普遍價值的最大諷刺：斯諾登閉口噤聲若寒蟬〉，《海峽評論》，第274期，頁9-12。

蔡庭榕，2003/8。〈論反恐怖主義行動法制與人權保障〉，《刑事法雜誌》，第47卷第4期，頁9-12。

研討會論文

王予芃、陳煇煌，2013/6/1。〈從國家安全觀點探討數位匯流對資訊安全之影響〉，「第九屆知識社群國際研討會(The 9th International Conference on Knowledge Community KC2013)」，臺北：中國文化大學，閩江學院海峽學院，美國托萊多大學亞洲研究學院，頁681-691。

吳胤瓘，2002/12/14-15。〈美國對外戰略的雙軌操縱與歐洲反應—以Echelon間諜情報網及海外駐軍基地部署為例〉，「臺灣政治學會2002年年會暨全球化與臺灣政治」學術研討會。嘉義國立中正大學：臺灣政治學會。頁1-32。

網際網路

丁剛，2000/2/25。〈歐盟揭露美國電子間諜網〉，《人民日報》，<http://www.people.com.cn/BIG5/channel2/18/20000225/7342.html>。

丹尼爾，〈英國國內安全機關MI5的監督機制及相關法律簡介〉，<http://www.mjib-tw.org/Essay/Essay-Detail.aspx?CurrentPage=0&seri=24>2003/11/15。〈社論：慎防中共「網軍」對我發動組織性攻擊〉，《青年日報》，第2版。<http://www.youth.com.tw/db/epaper/es001001/eb0112.htm>。

陳芃君，〈數位英國政策分析〉，《資策會FIND》。<http://www.teema.org.tw/upload/ciaupload/01.pdf>。

田思怡，2014/4/8。〈美向陸簡報網軍數盼投桃報李〉，《聯合新聞網》，<http://udn.com/NEWS/WORLD/WOR6/8598666.shtml?ch=rss_international#ixzz2zgyUQG2r>。

洪智坤，2013/3/28。〈注意：中南海將要監聽你的電話>。《新新聞》，第1308期，<http://www.new7.com.tw/NewsView.

aspx?i=TXT20120328195217412>。

崔雯，2013/6/23。〈揭秘各國網軍：美國規模最大　英國網絡罪犯被徵召〉，《鳳凰網》，<http://news.ifeng.com/shendu/nfrwzk/detail _2013_06/30/26963747_0.shtml>。

黃郁文、林誠夏編撰，2013/06/10。〈從SOPA到CISPA-軟體自由、網路自由與公民自由知多少？〉，《自由軟體鑄造場電子報》第220期，中央研究院資訊科學研究所，<http://www.openfoundry.org/tw/foss-news/8995--sopa-cispa->。

楊曉欣，2007/10。〈中共網軍對我資訊安全威脅之探討〉，《清流月刊》。<http://www.mjib.gov.tw/cgi-bin/mojnbi?/d2/9610/3-1.htm>。

楊會永，2009/4/11。〈反恐中的憲法問題：個人訊息保護〉，《法中論壇—中國法學平臺法中論壇》，<http://www.jurachina.cn/forum.php?mod=viewthread&tid=445&page=1>。

2000/2/24。〈歐盟指責美國對歐洲國家使用商業間諜衛星〉，《人民日報》，<http://www.people.cn/BIG5/channel2/18/20000224/7228.html>。

2001/4/8。〈美布天羅地網　偵搜全球情報〉，《中國工程技術訊息網》，<http://www.cetin.net.cn/cetin2/servlet/cetin/action/HtmlDocumentAction;jsessionid=9B9BF774D76B580649A06F2757FDCCC9?baseid=1&docno=6009>。

2003/3/29。〈數據量超過衛星傳輸能力　美“數字戰”吃緊〉，《人民網》，<http://www.people.com.cn/BIG5/guoji/22/86/20030329/957385.html>。

2011/1/10。〈陸軍網絡司令部(ARCYBER)〉，《知遠戰略與防務研究所論壇》，<http://forum.defence.org.cn/archiver/? tid-35291.html>。

2013/2/20。〈雲計算與法律迷霧〉，《企業網D1Net》，<http://www.d1net.com/cloud/news/204285.html>。

2013/6/14。〈美龐大情報監控系統曝光　能監聽國家領導人通訊〉，《中國網軍事》，<http://big5.china.com.cn/gate/big5/military.china.com.cn/2013-06/14/content_29123220_2.htm>。

2013/6/30/。〈揭開美國網軍面紗：純銅包裹建築防信號外泄〉，《京報網—北京晚報》，<http://news.xinhuanet.com/info/2013-06/23/c_132478458.htm>。

外文部分

官方文件

EUROPEAN UNION, 2001/7/11, “2001 EU Parliament Report: Echelon Global Private and Commercial Communications Interception System”, <http://publicintelligence.net/2001-eu-parliament-report-echelon-global-private-and-commercial-communications-interception-system/> <http://info.publicintelligence.net/ECHELONreport.pdf>

專書

James Bamford, 1983. *The Puzzle Palace: A Report on America's Most Secret Agency*.

Penguin Books Bob Woodward, 1975/10/13, "Messages of Activists Intercepted", *Washington Post*, pp. A1, A14.

Jeffrey T. Richelson, *The U.S. Intelligence Community* (Cambridge: Ballinger, 2nd ed., 1989/Boulder: Westview Press, 3rd ed., 1995; 4th ed., 1999); See also the World Wide Web site of the Federation of American Scientists, <http://fas.org/irp/offdocs/dcid16.htm>

期刊論文

2000/2, "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", *FAS*, <http://www.fas.org/irp/nsa/standards.html>

2013/6/21, "The NSA, the FCPA and Parallels of History", *TRACE*, <http://traceblog.org/2013/06/21/the-nsa-the-fcpa-and-parallels-of-history/>

James Risen and Eric Lichtblaub, 2005/11/16, "Bush Lets U.S. Spy on Callers Without Courts", *New York Times*, <http://www.nytimes.com/2005/12/16/politics/16program.html?_r=0>

Jill Lawrence, 2013/6/7, "Why PRISM is Different and Scarier Than Other NSA Spying-The latest surveillance program in the news is the most intrusive, and investigating who leaked it will be a stiff test of administration restraint.", *National Journal*, <http://www.nationaljournal.com/nationalsecurity/why-prism-is-different-and-scarier-than-other-nsa-spying-20130607>

Jeralyn, 2008/2/19, "Supreme Court Refuses Review of NSA Wiretapping Case", *TALKLEFT*, <http://www.talkleft.com/story/2008/2/19/11029/2163/supremecourt/Supreme-Court-Refuses-Review-of-NSA-Wiretapping-Case>

Stephen G. Brooks and William C. Wohlmfoith, "American Primacy in Perspective", *Foreign Affairs*, Vol.81, No. 4, July/Aug 2002, pp. 20-33 Steve Kettmann, 2001/6/20. "Does Europe Covet Own Echelon?", *WIRED*, <http://archive.wired.com/politics/law/news/2001/06/44689〉

Steve James, 2000/4/12, "Revelations about Echelon spy network intensify US-European tensions", *World Socialist Web Site* <https://www.wsws.org/en/articles/2000/04/spy-a12.html>

Tanaka Sakai, 2000/3/2, "世界中の通訊を盗聴する巨大システム, *TANAKANEWS*, <http://tanakanews.com/a0302echelon.htm>

Verge Staff, 2013/717, "Everything you need to know about?PRISM", *THE VERGE*, <http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>

Yossi Melman, 2013/10/28, "The NSA affair and the dogmatic notion of privatization", *I24NEWS*, <http://www.i24news.tv/en/opinion/131027-the-nsa-affair-and-the-dogmatic-notion-of-privatization>

網際網路

Florian Rötzer，2002/1/16,“Ein europäisches Echelon?”, <http://www.heise.de/tp/deutsch/special/ech/11586/1.html>

Patrick S. Poole, 1998. *ECHELON: America's Secret Global Surveillance Network*. Washingto, D.C.: Free Congress Foundation.

Richard Silverstein, 2014/2/9,“NSA Maintains Secret“Five Eyes”Satellite Facility in Israel”, *RICHARDSILVERSTEIN*, <http://www.richardsilverstein.com/2014/02/09/nsa-maintains-satellite-facility-in-israel/>

Richard Silverstein, 2014/2/10,“Secret NSA Satellite Facility Located at IDF Base in Occupied East Jerusalem”, *LIVELEAK*, <http://www.liveleak.com/view?i=a3f_1392383537>