監聽風雲－以通訊監察進行國家情報工作之規範檢討*

張　明　偉**

目　次

關鍵字：監聽、反恐、情報、隱私、國家安全。
Keywords：wiretap, anti-terrorism, intelligence, privacy, national security.

* 謹此感謝兩位匿名審查人提供之寶貴意見。
** 張明偉，輔仁大學法學院副教授，美國舊金山金門大學法學博士。

摘 要

本文旨在探討現行通訊監察法制於國安情報監察之適用及衍生之疑義，為能有效杜絕非法監聽，完善通訊監察法制，並滿足國家安全維護之需求，本文主張應制定以國安情報通訊監察為主要目的之專法，用以規範以國家安全維護而非以犯罪偵防為目的之通訊監察，以避免情報工作人員因法制不健全而罹刑章。又為免通訊監察法制間出現積極衝突，本文亦主張應修正現行通訊保障及監察法，使之成為以犯罪偵查為目的之通訊監察專法。

The Wiretapping：Reviewing Intelligence Regulations of Communication Monitoring for the National Security Reason

Chang, Ming-Woei

Abstract

This study discusses problems resulting from current intelligence practice under the Communication Protection and Monitoring Law. To avoid any illegal practice, this study suggests passing a law focused on intelligence collection under the National Security purpose in addition to the Communication Protection and Monitoring Law, with which intelligence agent could comply. Furthermore, this study also suggests amending the Communication Protection and Monitoring Law so that conflicts between these two systems would not become a new problem.

壹、前　言

伴隨著通訊科技的進步發展[1]，人們對於新型通訊設備的依賴也越來越深。在現今幾乎人手一機的時代，無線通訊早已成為人們溝通的主流模式，也因此對於無線通訊進行必要的監察，往往被認為是獲取重要（包含犯罪與非犯罪）資訊最有效的管道（手段）[2]。不過，由於通訊監察（俗稱監聽）[3]影響人民日常生活甚鉅，如未妥善管制，恐將如「全民公敵（ENEMY OF THE STATE）[4]」一片內容般，造成社會大眾之恐懼；而其所衍生抑制言論自由的效果，甚至會影響民主政治的健全發展。

過去於動員戡亂時期，由於國家處於備戰之緊急狀態，在維護國家安全的旗幟下，情治機關常以密錄或郵檢等方式，蒐集或掌控意圖叛亂或異議分子之言行，更常被國際人權團體痛批戕害人權。隨著兩岸情勢的和緩，八零年代後，通訊監察漸轉向以犯罪調查、蒐證為重心。實務上，我國電信監聽業務始於警備總部，後因相關動員戡亂法律因動員戡亂時期終止於 81 年 7 月 31 日失效，基於偵查犯罪及蒐獲不法事證之必要，行政院遂於次日通令調查局，命其依職掌電訊的偵查與監察職責統籌辦理重大犯罪案件通訊監察的執行業務[5]，其後法務部亦曾訂頒「國內犯罪案件通訊監察作業要點」與「檢察機關實施通訊監察應行注意要點」作為各級檢察機關因案執行電話監聽之作業準則。依上開法務部所訂頒行政命令，檢察官得依職權簽發或逕予受理、審查、核准司法警察機關對於犯罪嫌疑人執行通訊監察[6]。為保障人民秘密通訊自由不受非法侵害，並確保國家安全，維持社會秩序[7]，並符合監聽法制化之世界潮流[8]，我國遂於 88 年 7 月 14 日制定公布通訊保障及監察法，藉以法制化通訊監察此一必要之惡。依該法第 2 條規定，除為確保國家安全、維持社會秩序所必要者外，不得進行通訊監察；此外，依該法所實施之通訊監察，亦

1　第一代（1G）手機是指 70 年代發展的類比信號（analog system）手機；第二代（2G）手機是指 80 年代開始發展的數位訊號（digital cellular systems）手機，如 GSM 和 cdmaOne，提供低速率數據業務；2.5G 是指在第二代手機上提供中等速率的數據服務，如 GPRS（Global Packet Radio Service），其傳輸率一般在幾十至一百多 kbps。第三代（3G）手機能將無線通訊與國際互聯網等多媒體通訊結合的新一代流動通訊系統。能夠處理圖像、音樂、視訊形式，提供網頁瀏覽、電話會議、電子商務資訊服務。無線網絡必須能夠支持不同的數據傳輸速度，也就是說在室內、室外和行車的環境中能夠分別支持至少 2Mbps、 384kbps 以及 144kbps 的傳輸速度。由於採用了更高的頻帶和更先進的無線（空中接口）接入技術，3G 標準的流動通訊網絡通訊質量較 2G、 2.5G 網絡有了很大提高，比如軟切換技術使得旅途中高速運動的移動用戶在駛出一個無線小區並進入另一個無線小區時不再出現掉話現象。而更高的頻帶範圍和用戶分級規則使得單位區域內的網絡容量大大提高，同時通話允許量大大增加。3G最大的優點即是高速的數據下載能力。相對於 2.5G（GPRS/CDMA1x）100kbps 左右的速度，3G 隨使用環境的不同約有 300k-2Mbps 左右的水準。 另外有些 3G 系統服務業者會更新為 3.5G 系統（如 HSDPA），此時可有下傳 14Mbps、上傳 5.8Mbps 的速度。See THE INTERNATIONAL COMMUNICATION UNION, About mobile technology and IMT-2000, available at: <http://www.itu.int/osg/spu/imt-2000/technology.html>（last visited: Sep. 3, 2010），另參閱維基百科，3G，<http://zh.wikipedia.org/zh-hk/3G>（最後造訪日：2010 年 9 月 3 日）。

2　據報導，在檢調偵辦高院法官行收賄乙案中，曾任高院法官轉任律師的邱創舜與其妻段美月一開始原否認行賄及侵吞保釋金，也否認扮演司法黃牛，但檢調監聽邱創舜與其妻近三年，邱看到檢方提出的監聽譯文，一時愣住，說不出話來。參閱聯合報記者蘇位榮、熊迺祺，一見監聽譯文 白手套邱創舜呆住，<http://udn.com/NEWS/NATIONAL/NATS9/5783445.shtml>（最後造訪日：2010 年 9 月 3 日）。

3　事實上，在我國法制上，通訊監察此一名詞於 1991 年以前未曾出現，過去大都以竊聽或通訊竊聽稱之。立法院 1999 年 7 月公佈的通訊保障及監察法首次正式使用「通訊監察」之名稱，並對其內涵予以明確的定義。

4　該片劇情簡述如下：律師男主角某日在買禮物時巧遇老友，其友發現某政要殺人的錄影帶而遭追殺，因其友將錄影帶放入律師的購物袋內，遂開始了律師的逃亡旅程，男主角身上無一倖免的被裝上小型竊聽器（皮鞋跟、內褲、手錶、領帶、西裝），甚至信用卡被停掉，此外，FBI 更刻意製造他與初戀情人外遇的假消息，導致男主角被老婆趕出門，並使用衛星全程跟監男主角的一舉一動。

5　參閱李子哲，＜監聽要嚴守法定程序＞，<www.libertytimes.com.tw/2004/new/jan/15/today-o6.htm>（最後造訪日：2010 年 9 月 3 日）。

6　參閱吳榮修，＜人民秘密通訊權的保障與限制＞，<http://www.afa.gov.tw/friendlyprint.asp? tableName=service&CatID=657>（最後造訪日：2010 年 9 月 3 日）。

7　通訊保障及監察法第 1 條參照。

8　參閱李明，《監聽制度研究－在犯罪控制與人權保障之間》，頁 113，法律出版社，2008 年 7 月。

不得逾越所欲達成目的之必要限度，且應以侵害最少之適當方法為之，不過實務上仍存在監聽過於浮濫之批評[9]。

自從 2001 年美國發生九一一恐怖攻擊事件以來，以維護國家安全為目的之情報工作，已成為世界各國預防恐怖攻擊事件再次發生的重要課題。雖然恐怖攻擊事件並非造成國家安全危害的唯一事由，不過當國家機關以維護國家安全為由進行情報蒐集工作（通訊監察）時，不免亦將侵害人民之隱私，此時究應如何調和國家安全與個人隱私保護，以免有所偏廢，即有對以國家安全與情報工作（非刑事犯罪偵查）為通訊監察目的之法制進行通盤研究之必要。換言之，現行通訊保障及監察法是否足以因應各種監察目的（犯罪偵查與非犯罪偵查）的通訊監察需求，並提供各種目的通訊監察之合法性基礎，誠為能否杜絕非法監聽之重要基礎[10]。雖然現行通訊保障及監察法於規範上原僅在提供戒嚴時期由警備總部執行監聽作業之法制依據，不過關於以一般犯罪偵查為目的（針對特定對象實施）之通訊監察是否適合與以國安情報調查為目的之通訊監察一同立法、或是應該分別立法，在法制訂定之初即有爭議。就法理而言，如果認為針對特定對象實施之通訊監察僅適用於犯罪偵查工作，則與犯罪偵查無關之國安情報蒐集，即不應在通訊保障及監察法中予以規範；相對來說，如認通訊保障及監察法之規範效力及於與犯罪無關之國安情報蒐集，則以合理可疑（Probable Cause）為審查應否進行通訊監察之標準，似亦應適用於與國家安全工作有關但與犯罪偵查無關之通訊監察。鑑於現行通訊保障及監察法本身並未嚴格區分以犯罪偵查為目的之通訊監察與以國安情報蒐集為目的之通訊監察，因此關於以國家安全情報蒐集為目的之通訊監察是否具備充分完足之法制基礎，並足供情報工作人員執法之依據，觀之通訊保障及監察法僅第 7 條提供與國家安全情報工作有直接相關之規範，不免令人疑惑。為能釐清情報通訊監察之相關疑義，本文將以現行通訊保障及監察法之規範為基礎，檢討其於國家安全情報通訊監察工作實施過程中所可能遭遇的問題，並提出相關修正意見，以為法制參考。

貳、通訊監察對人權所造成之侵害

秘密通訊自由原已為我國憲法第 12 條明文保障，鑑於通訊監察乃明顯限制憲法權利保障之措施，故除必須依據法律始得為之外，依照憲法第 23 條：「以上各條列舉之自由權利，除為防止妨礙他人自由，避免緊急危難，維持社會秩序，或增進公共利益所必要者外，不得以法律限制之。」之規定，除須以法律限制秘密通訊自由外，該限制秘密通訊自由立法之內容更須實質正當[11]。由於在傳統中國文化中，並不存在個人權利概念[12]，而且國家往往藉由維護國家安全之名義，過度限制甚至剝奪人民自由權利[13]，因此如未能於概念上先釐清通訊監察所影響之權利內涵，實際上亦將無法判斷前

9 根據司法院五月底送交立法院的報告指出，通訊保障監察法自 2007 年底修正後，偵查中案件的通訊監察書須由法官核發，此後到今年 5 月 7 日，共監聽 49,634 件，平均每月 1,711 件，「已大幅降低監聽件數。」但朝野立委昨仍質疑監聽件數太多，法院核准率也太高，有侵犯人權疑慮。立法院「通訊監察執行情形調閱委員會」上月召開會議，要求國內情治單位向國會提出執行監聽報告。據司法院報告指出，情治單位申請監聽，核准監聽比率約百分之 75，其中以違反《毒品危害防制條例》案最大宗，約佔所有核准案的六成九。據司法院資料顯示，已結束監聽件數迄今有 14,238 件，不到監聽總件數的 3 成，且根據《通訊保障監察法》，結束監聽時須通知當事人，以利當事人事後救濟，但迄今未通知當事人件數也仍有 2,320 件，佔百分之 16。參閱何哲欣，監聽核准率 75 %「侵犯人權」，2010 年 06 月 10 日蘋果日報，<http://tw.nextmedia.com/applenews/article/art_id/32575905/IssueID/20100610>（最後造訪日：2010 年 9 月 3 日）。

10 蓋如現行有關通訊監察之法律不足以因應各種監察目的之通訊監察，其所實施之通訊監察自將因「無法可依」而成為「非法」之通訊監察。

11 司法院大法官釋字第 631 號解釋：「憲法第十二條規定：『人民有秘密通訊之自由。』旨在確保人民就通訊之有無、對象、時間、方式及內容等事項，有不受國家及他人任意侵擾之權利。國家採取限制手段時，除應有法律依據外，限制之要件應具體、明確，不得逾越必要之範圍，所踐行之程序並應合理、正當，方符憲法保護人民秘密通訊自由之意旨。」亦同此旨。

12 參閱陳愛娥，中國法律思想中的人權觀念著眼於其對臺灣社會法律意識的可能影響，政大法學評論，62 期，頁 3，1999 年 12 月。

述限制秘密通訊自由法律之內容是否實質正當。不過從多數美國人於九一一恐怖攻擊發生之初願意放棄權利對抗恐怖活動但事後仍回歸人權保障價值之現象[14]而言，是否為實質正當之限制規定，並非一成不變之概念，其實質內涵往往因發生重大事件而出現相對應之調整。

司法院大法官釋字第 631 號解釋理由書曾對秘密通訊自由有以下之描述：「此項秘密通訊自由乃憲法保障隱私權之具體態樣之一，為維護人性尊嚴、個人主體性及人格發展之完整，並為保障個人生活私密領域免於國家、他人侵擾及維護個人資料之自主控制，所不可或缺之基本權利。」依其說明，人民有在不為第三者所知悉情況下，利用各種通訊方式與他人互傳訊息與交流的權利；限制秘密通訊自由將使人民恐懼其言論遭不當引用，進而不敢表達內心之思想與意見，影響自由意志之交流與形成（甚至形成寒蟬效應）[15]，並侵害個人隱私[16]與資訊自主權[17]，有害人性尊嚴[18]與人格完整發展，徵諸世界人權宣言（Universal Declaration of Human Rights）第 12 條：「任何人的私生活、家庭、住宅或通訊不得任意侵犯，其榮譽和名譽不得加以攻擊，人人有權享有法律的保障，對抗這種侵犯或攻擊。」與公民及政治權利國際盟約第 17 條：「任何人之私生活、家庭、住宅或通信，不得無理或非法侵擾，其名譽及信用，亦不得非法破壞。」等規定，該項說明至為的論。

由於通訊技術之發展及廣泛利用有助於個人拓展生活與自由領域，對個人人格發展具正面且積極意義，當個人人格發展與社會形成高度依存於通訊網路設備時，一旦出現人民秘密通訊自由受到國家公權力侵害之現象，則受害人所能感受之「痛苦指數」與其對自由保障之負面影響，勢必將較傳統社會時期更為重大[19]。鑒於美國聯邦最高法院早於 1967 年即已主張為偵查犯罪所實施之通訊監察該當憲法第四修正案所指之「搜索」及「扣押」[20]，並於 1972 年

13　國家公權力是用來維護人權與公益，禁止不合理侵害人民權益。國家機關擁有廣泛蒐集資訊之權力，並藉所蒐得之資訊作為施政正當性之基礎，進而維繫國家存立最主要相互依存要素－安全與福祉。但在保護國家安全、促進人民福祉的冠冕用語之下，亦可能潛藏著限制、剝奪、干預人民自由權利之危機，猶如雙刃之刀。自由與安全、或福祉與干預等相對立的概念與詮釋，隨著時空環境與意識型態的轉變，具有不同階段之意涵。參閱李震山，多元、寬容與人權保障-以憲法未列舉權之保障為中心，頁 210，元照出版，2007 年 9 月。

14　例如，遭受 911 攻擊之紐約，理當被認為最支持安全政策，但其市政委員會之後反對聯邦當局要求之決議，認為國家安全與保護自由間並無牴觸，美國人可以既安全又自由。政府損害基本權利的安全措施，確實危害紐約市民所秉持價值觀，政府為了確定安全措施提升大眾安全，也應該以合理及審慎的方式進行，並且不損害到憲法賦予人民的權利或侵害人民的自由，參閱 John Battelle，陳琇玲譯，搜尋未來，頁 243，商周出版，2006 年 4 月。又有指出，911 事件造成重大死亡原因，應該檢討登機門乘務員是否當時有注意他們以現金買下單程機票，也沒有攜帶行李而警覺此異狀，參閱 Arthur S. Hulnick，蕭光霈譯，《情報與國土安全》，頁 42，國防部史政編譯室編譯處，2006 年 10 月。美國上尉 Ian Fishback 於 2005 年 9 月 16 日，在寫給參議員 John McCain 的信中表示：難道為了維護安全，我們就可以放棄理想嗎？恐怖主義引發恐慌，並壓抑了諸如自由和個人權利的理想，克服恐怖主義威脅所帶來的恐懼，是對我們勇氣的巨大考驗，我們是直接面對危險和不幸以堅持理想，還是在犧牲的幌子下退縮，放棄保障個人權利的承諾？如果我們在不幸和挑釁面前放棄理想，這就意味著我們從來就沒有真正擁有那些理想。我寧願戰死，也不願放棄哪怕是一丁點的美國理念，參閱 Anne-Marie Slaughter，馬占斌、田潔譯，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，頁 1、3，2009 年。批評極端反恐政策者認為，那些為得到一點短暫安全而放棄基本自由的人，將獲報以既無自由亦無安全，參閱蔡庭榕，＜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 37，2003 年 8 月。以上資料，轉引自周玄明，＜隨機性國際通訊情報偵蒐法制研究＞，頁 101，註 417，《國防大學管理學院法律學研究所碩士論文》，2010 年 1 月。

15　參閱曾正一，《偵查法制專題研究》，頁 308-311，中央警察大學，2006 年 10 月。

16　參閱許華孚，＜錄影監視系統在犯罪控制運用的省思＞，《犯罪學期刊》，12 卷 1 期，頁 17，2009 年。

17　司法院大法官釋字第 603 號解釋：「個人自主控制個人資料之資訊隱私權而言，乃保障人民決定是否揭露其個人資料、及在何種範圍內、於何時、以何種方式、向何人揭露之決定權，並保障人民對其個人資料之使用有知悉與控制權及資料記載錯誤之更正權」已肯認人民有資訊自主權。

18　一般而言，人性尊嚴是與生俱來，為具有普遍性與永久性且不可放棄、不容破壞，不問何地、何時、何人皆當然享有，對此國家權力應加以尊重與保護，其核心內涵有二：一為人在自己自由權利範圍內，有自治自決之高度自主性，不處於被操控的他治（律）他決的地位；二為人本身即是目的，不能成為純粹客體，不論依己意或他意，都不能被工具化、物化、商品化。參閱李震山，＜人性尊嚴＞，《法學講座》，17 期，頁 3，2003 年 5 月。

19　參閱詹鎮榮，＜秘密通訊自由＞，《法學講座》，21 期，頁 1，2003 年 9 月。

確認在進行國內安全情報（domestic security intelligence）的蒐集時，仍應遵守聯邦憲法第四修正案之規定[21]，因此，有關令狀原則應遵守的程序及要件[22]，縱於國家情報通訊監察事件，自亦不能免除[23]。即便在特殊情況下有緩和令狀原則之必要[24]，其要件及限制，亦應依憲法第 23 條比例原則之精神，由法律或符合授權明確原則之法規命令予以明文規定[25]。

參、情報通訊監察獨立規範之必要性

一、不同監察目的之相似性

隨著通訊科技的發展，人們對於通訊科技的依賴也越來越深，不論是犯罪偵查或是以維護國家安全為目的的情報蒐集，難免需要透過現代的通訊科技以達相關資訊蒐集的目的。雖然實施通訊監察將對人權造成一定程度的侵害，甚至如美國「水門事件[26]」造成嚴重的政治風暴。但因其事實上於查明案件事實、收集

---

20 See Katz v. United States, 389 U.S. 347 (1967).

21 美國聯邦最高法院於本案中指出，由於國安監察的範圍更為廣泛、可能涉及更多的消息來源、對象較不易特定，其性質也多偏向預防不法活動的發生及抗制可能的危害，故其要件及程序規定可以有較大的彈性，而與一般犯罪監察的有所不同。See United States v. United States District Court, 407 U.S. 297, 323(1972).

22 基本上需要法官事先審查核發員警搜索令狀原因如下，一為員警較主觀作出判斷何時應發動強制處分權，員警因為績效常會將搜索所需之相當理由自我弱化，因此委由法官決定較為客觀。二為預防無實質理由的強制處分，美國聯邦最高法院曾在判決中指出，所有的搜索扣押皆為惡害，在未事先仔細檢驗是否有搜索的必要性前，任何的搜索皆無正當性。因為員警並無專長與功能有效分辨何時得侵犯人民的隱私，當犯罪偵查與基本人權發生衝突時，員警可能過分重視犯罪偵查，而忽視人民的隱私，因此建立事先審查制度得預防違法搜索。三為避免事後諸葛判斷的偏頗，事先審查係在證據未發現前，即向法官聲請令狀，在證據未發現前，無所謂形成對被告不利的心證，因此法官比較能公正客觀判斷員警是否有搜索之實質理由。四為建立書面紀錄，可幫助嗣後再次審查相當理由的有無。五為以繁複之聲請程式篩減無必要的強制處分，因為聲請程式的費時費力，會讓員警考慮非有必要不聲請令狀，且為通過審查，員警在填具聲請書時，會仔細、冷靜思索並述明事實及理由，否則員警有時可能會過於衝動、過於草率。參閱王兆鵬，《美國刑事訴訟法》，頁 93-101，元照出版，2007 年。

23 值得說明的是，雖然我國搜索法制已於 2001 年修正改採令狀原則，不過因通訊保障及監察法未同步修正，在法務部堅持通訊監察異於搜索（該法為刑事訴訟法之特別法）之立場下，我國法制與實務曾存在有體物之搜索採令狀原則，而無體物之搜索（通訊監察）卻不採令狀原則之搜索一國兩制。此種荒謬之現象直至司法院大法官釋字第 631 號解釋明確指摘後（通訊監察之執行，除通訊監察書上所載受監察人外，可能同時侵害無辜第三人之秘密通訊自由，與刑事訴訟上之搜索、扣押相較，對人民基本權利之侵害尤有過之。鑒於通訊監察侵害人民基本權之程度強烈、範圍廣泛，並考量國家執行通訊監察等各種強制處分時，為達成其強制處分之目的，被處分人事前防禦以避免遭強制處分之權利常遭剝奪。為制衡偵查機關之強制處分措施，以防免不必要之侵害，並兼顧強制處分目的之達成，則經由獨立、客觀行使職權之審判機關之事前審查，乃為保護人民秘密通訊自由之必要方法。是檢察官或司法警察機關為犯罪偵查目的，而有監察人民秘密通訊之需要時，原則上應向該管法院聲請核發通訊監察書，方符憲法上正當程序之要求。系爭通保法第五條第二項未設此項規定，使職司犯罪偵查之檢察官與司法警察機關，同時負責通訊監察書之聲請與核發，未設適當之機關間權力制衡機制，以防免憲法保障人民秘密通訊自由遭受不必要侵害，自難謂為合理、正當之程序規範，而與憲法第 12 條保障人民秘密通訊自由之意旨不符，應自本解釋公布之日起，至遲於 96 年 7 月 11 日修正公布之通保法第五條施行之日失其效力。），才迫使法務部積極進行通訊保障及監察法第 5 條之修正作業。

24 許玉秀大法官曾指出：「是不是干涉自由，均涉及利益的犧牲問題，對行為人而言，因受監察程式之干涉，通訊自由受限制，個人認係對行為人之一種制裁，至於其他人是否因此完全犧牲個人利益，個人認為這是一個利益交換另一個利益。比如說線路被利用而被監聽之人，可解釋為通訊自由利益與其個人安全利益之交換。有關涉及個人權利受某法律限制，如有利益之交換，且利益保持平衡狀態，這樣的立法可以被接受。」參閱法務部，通訊監察法草案研究制定資料彙編，頁 99，法務部，1992 年。

25 對於跨境通訊監察之實施，有主張可參考國境檢查之模式，緩和令狀原則之要求，僅須符合法律保留原則即可：「《國家安全法》賦予警察或海巡人員對出入境人員物品運輸工具檢查之權；《海岸巡防法》賦予巡防機關人員執行安全檢查之權；《警察勤務條例》賦予警察為執行取締、盤查而在公共場所或指定處所、路段之臨場檢查或路檢之權，《海關緝私條例》賦予海關得對貨物及關係人檢查之權，《入境旅客攜帶行李物品報驗稅放辦法》賦予海關為了查緝而在機場進行檢查之權，五者本質上對人民自由都產生某種程度之限制，但人權在維護國家安全、公共安全與社會秩序考量下都適度退讓，五者另一相同處係都在國界上進行檢查，因此在跨境通訊線路上進行偵蒐，因具有跨越國界之特質，似可以相同道理看待。」、「通訊偵蒐如同上陳海關、員警、海巡人員之國界檢查方法，對不特定人之偵察時間是短暫的，無可疑即予忽略，若遇有危安或有利國家安全或利益之特定人線索且須長時間監視時，自須依通保法規定聲請通訊監察書，所以應無所謂持續、長時間侵害人民基本權，較監察之侵擾個人程度是有明顯不同，如同刑法第 321 條對竊盜罪規定加重刑責之態樣，在白天與夜晚侵入住宅對於內居人的感受是不同的。」參閱周玄明，＜隨機性國際通訊情報偵蒐法制研究＞，頁 94、108-109，《國防大學管理學院法律學研究所碩士論文》，2010 年 1 月。

證據方面成效卓著[27]，通訊監察在犯罪偵查與國家安全工作中仍越來越廣泛地被採用，成為現代刑事偵查與國家安全工作中不可或缺的手段。然而，就內涵而言，以犯罪偵查為目的之通訊監察與以維護國家安全為目的之情報蒐集並不完全相同。具體而言，一般的犯罪活動影響的層面通常較為有限，被害人的人數也通常較少；相對來說，破壞國家安全或利益的活動常常對國民造成極為廣泛的影響，被害的人數也通常遠較一般犯罪為多。此外，就行為人或監察對象來說，兩者也不盡相同，在一般的犯罪裡，前者多半純為本國人，但是在國家安全工作領域中，監察的對象很可能是以外國人，或是與外國人接觸的本國人。縱然社會偶有發生情節較為重大複雜之犯罪事件，不過，整體來說，對其通訊監察所產生的通訊干涉程度還是比因國家安全實施通訊監察來得簡單及輕微。

國家安全情報蒐集與一般犯罪偵查工作或許於概念上可以一分為二，但是，在實際運作上，這兩者恐怕有其難分之處，蓋兩者的執行單位可能是同一機關，以法務部調查局為例，依法務部調查局組織法第 2 條規定，調查局所掌理的事項便同時包含了「外患防制事項」、「洩露國家機密防制事項」、「貪瀆防制及賄選查察事項」、「重大經濟犯罪防制事項」、「毒品防制事項」、「洗錢防制事項」、「電腦犯罪防制……事項」、「組織犯罪防制之協同辦理事項」、「兩岸情勢及犯罪活動資料之蒐集、建檔、研析事項」、「國內安全及犯罪調查、防制之諮詢規劃、管理事項」，以及「上級機關特交有關國家安全及國家利益之調查、保防事項」，其同時負責犯罪偵查及國家安全的情報蒐集；此外，依照國家情報工作法第 3 條規定，海岸巡防署或警政署等傳統上負責犯

26　水門事件是美國歷史上最不光彩的政治醜聞之一，其發生地點就在水門大廈內，在 1972 年的總統大選中，以美國共和黨尼克森競選團隊的首席安全問題顧問詹姆斯·麥科德為首的五人，為了取得民主黨內部競選策略的情報，在 6 月 17 日闖入位於華盛頓水門大廈的民主黨全國委員會辦公室，在安裝竊聽器並偷拍有關文件時，當場被捕。事件發生後尼克森曾一度竭力掩飾與否認，但在隨後對這一案件的繼續調查中，尼克森政府內的許多人被陸續揭發出來，並直接涉及到尼克森本人，從而引發了嚴重的憲法危機。翌年 10 月 20 日，尼克森為了要罷免要求他交出證據的特別檢察官，迫使拒絕解任特別檢察官的司法部長辭職，司法次長繼任司法部長後，又因為拒絕罷免這位特別檢察官而辭職，最後第三任司法部長才答應罷免特別檢察官，尼克森更動員 FBI 封鎖特別檢察官及司法長官、次長的辦公室，宣佈廢除特別聯邦檢察局，把此案的調查權移回司法部。尼克森濫用行政權力來維護自己之行徑，招來國民嚴重指責。10 月 31 日，美國眾議院決定由該院司法委員會負責調查、搜集尼克森的罪證，為彈劾尼克森作準備。1974 年 6 月 25 日，司法委員會決定公佈與彈劾尼克森有關的全部證據。七月底，司法委員會陸續通過了三項彈劾尼克森的條款。尼克森於 8 月 8 日向全國發表電視演說，宣佈將於次日辭職，從而成為美國歷史上首位，也是迄今唯一一位因醜聞而中途辭職下臺的總統。不過社會大眾似乎以為當年尼克森是因部屬違法亂紀被迫辭職，但事實上導致他面臨國會彈劾的主要原因，是他企圖動用權勢壓下水門罪案，犯下所謂 OBSTRUCTION OF JUSTICE，亦即阻撓司法的明確罪行，如果水門案件僅限於部屬胡作非為，總統縱難免用人不當或失察之嫌，最多是聲望受損，不致構成彈劾理由。要談彈劾解職，必須是總統本人犯下實質罪行。美國在哈定、杜魯門主政時代，曾多次發生高級官員操守疑案，但該兩位總統並未遭到彈劾，因為沒有證據顯示總統貪瀆違法。雷根總統在任晚期，曾發生國安幕僚弄權非為醜聞，柯林頓總統在職期間，有關第一夫人的不利傳聞也層出不窮，但也未聞反對黨對兩位總統提出彈劾。參閱澳門日報，水門事件背景，＜http://www.macaodaily.com/html/2009-07/23/content_344736.htm＞（最後造訪日：2010 年 9 月 3 日）；敏洪奎，水門事件啟示錄，自由廣場，＜http://www.libertytimes.com.tw/2006/new/jun/15/today-o1.htm＞（最後造訪日：2010 年 9 月 3 日）。

27　據報導，「監聽雖違反個人隱私，但為了維護公眾安全、辦案需要，可以審慎授權去做，可是有通則就有例外，有例外就有濫用，近日臺南縣警局爆發員警利用監聽手機，確定發話基地臺位置，協助歹徒擄人勒贖一案，就是典型的例子。」、「義大利五月底提出監聽法，總理貝魯斯柯尼聲稱是為了保障個人隱私權，目前正在參議院審議，檢警批評真要依法行事，將來無法辦案，而媒體更強烈批判妨礙新聞自由，貝魯斯柯尼當然不是積極推動人權的人，他要保障的是政府與他個人的隱私權，工業發展部長近日已因為醜聞下臺，目前檢方調查的其他案子還牽涉好幾個部長，這都是靠監聽蒐證，而貝魯斯柯尼去年被應召女錄下的枕邊豪語，被媒體刊出，讓他付出大筆贍養費離婚，更讓他對媒體刊布隱私，恨得牙癢癢的。」、「義大利的監聽法草案，對監聽的使用與批准有嚴格的限定：檢警不能把本案監聽所得的錄音，轉移他案使用；除非是犯罪發生地，否則不能監聽汽車、咖啡館、辦公室等處；經過三位法官的合議庭同意，才能開監聽票，最長不得超過 75 天。檢警擔心，如此綁手綁腳，根本無法偵查黑手黨犯罪，美國助理司法部長也表示，新法通過後，將使得美意兩國間有關販毒、洗錢、反恐等打擊犯罪的合作受挫。新法同時規定媒體都只能在偵查終了，準備提起公訴時，才能夠報導監聽的內容，這引發媒體的公憤，所有報紙一致譴責，不分立場，即使是貝魯斯柯尼所擁有的報紙都公開反對，如果對偵查中的案子不能報導，偵查期間又長達幾年，不啻實施媒體封鎖，嚴重違反新聞自由。」參閱郭崇倫，忍受監聽還是忍受犯罪？中時電子報 2010-06-08，＜http://forum.n.yam.com/trackback.php/20100608505723＞（最後造訪日：2010 年 9 月 3 日）。

罪偵查的機關，仍有權執行部分國家情報事項，在該範圍裡，其仍屬於情報機關。由此可知，單純就執行機關來看，並不易判斷其所進行的是一般犯罪偵查，或是情報蒐集。

再就本質來說，外國情報工作及一般犯罪活動有很高的重疊性，通常言之，涉及外國情報的重要資訊，因與國家安全或國防軍事密切相關，其取得或洩漏往往都該當刑法上的犯罪行為；部分刑法上的犯罪行為，也都是外國情報工作的重點，舉例來說，行為人為外國蒐集我國國防秘密資訊的活動，應當屬於國家安全事項，不過，其行為也可能同時該當了刑法第 111 條第 1 項的收集國防秘密罪；相同地，將國防秘密交付於外國或其派遣之人的行為，除可能該當刑法第 109 條第 2 項外，其行為也會是國家安全工作所防制的對象。從這一方面來看，以犯罪偵查為目的之情報蒐集或以國家安全維護為目的之情報蒐集二者在概念上雖然能夠作一定的區別[28]，不過，在更多的時候，二者間只有程度上的差別，而沒有本質上的差異，很難截然二分。

另就情報蒐集所使用之方法而言，不論其係以犯罪偵查為目的之情報蒐集或以國家安全維護為目的之情報蒐集，國家情報機關或是犯罪偵查機關所使用的方式可能相差無幾，其多半皆以通訊監察、跟監，或是向其他機關或團體調取資料等方式蒐集必要的資訊。以通訊保障及監察法規定為例，為蒐集特定重大犯罪的相關證據，偵查機關可以進行通訊監察[29]，同樣地，為避免國家安全遭受危害，綜理國家情報工作機關也可以進行通訊監察，以蒐集外國勢力或境外敵對勢力的情報資訊[30]。是故，不論以犯罪偵查為目的之情報蒐集或以國家安全維護為目的之情報蒐集，各相關機關所可能使用的方式並沒有非常大的差別，故其對相對人所可能造成的影響或權利侵害也就不會有太大的差異。縱觀以上分析，不同目的之通訊監察在執行效能、執行機關以及執行手段上存在一定程度之相似性，或許正因以上的相似性，當初立法時才會以同一部通訊監察及保障法規範不同監察目的之通訊監察，然而這樣的規範本身是否符合不同目的通訊監察之需求，是一個值得進一步探討的課題。

二、監察與犯罪偵查無關通訊之必要性

除了傳統上所習知的與犯罪有關的國家安全事項外，事實上國家安全所涉及的情報蒐集工作，有許多與犯罪偵查並無太大關連[31]，蓋由於在罪刑法定主義的限制下，所有的犯罪都須以法已明文為要件，由於刑法係以處罰既遂犯為原則，而以處罰未遂犯為例外，因此關於那些尚未達未遂階段的不法活動，原則上並無法對其進行犯罪偵查。雖無法當作犯罪進行偵查，不過站在國家安全工作係以預防發生國安事件而非以將犯罪行為人繩之以法為主要目的之立場，對於尚未達犯罪階段之不法行為，仍不能說沒有予以事前管制監控之必要。換言之，國家安全工作往往有一個重要的特徵，就是其內涵可能與犯罪毫無關聯[32]，因此未必以將涉案人定罪為主要目的。

---

28 據研究指出，日本法僅允許監聽實施犯罪之關連通信，而所謂關連通信係指準備或事後湮滅証據等處置，為謀議、指示、相互連絡及其他關連該犯罪實行事項者，因此概念上有關兒女私情、家務理財、夫妻吵架等資訊並不能加以記錄。參閱朱朝亮，考察日本「通訊監察、暴力防制業務」報告，頁 21，2001 年；轉引自周玄明，＜隨機性國際通訊情報偵蒐法制研究＞，頁 32，《國防大學管理學院法律學研究所碩士論文》，2010 年 1 月。

29 通訊保障及監察法第 5 條及第 6 條參照。

30 通訊保障及監察法第 7 條參照。

31 有指出：「有關國家安全情報活動之監聽，不一定構成內亂、外患罪……從美國法律觀之，國家安全之監聽常係對抗外國對國內之活動及蒐集與國家安全有重大關係之外國情治資料，外國人在臺灣從事一般性情報活動不一定構成內亂、外患罪。」參閱法務部，通訊監察法草案研究制定資料彙編，頁 11，羅明通發言部分，法務部，1992 年。

32 舉例來說，「有些商業或日常生活行為資訊，就可能構成情報，而完全與犯罪無關。例如普通、合法但稍事修改即可配備軍用的民用產品、軟體和服務的消息，因為它會對國家安全構成威脅。日商的大型加工製造機械外銷蘇聯，協助改善其潛艇螺旋槳的靜音效果，使美國偵測難度加高，即影響了軍事平衡。另有關領導人之私生活及健康消息，他與同僚寒喧方式，也能幫助推定身心狀態與關係親疏。閱兵臺上官員們站立的相對位置，也能研判彼等政治行情的消長。其他如宗教觀點、

在所有與犯罪無關但卻與國家安全息息相關的情報蒐集中最引人重視的事件，應屬經濟安全事件。在資本主義制度之下，所有個人與群體利益的關係之中，最特別的應屬經濟活動與國家安全之間的關係，雖然資本主義學者認為，在大部分的情況下，在資本主義制度裡，個人與群體的利益，如國家的利益，是和諧的，不過在資本主義經濟的實際運作裡，個人與群體利益的衝突難免，尤其是負面的「外部性」條件存在的時候。這種個人與群體利益矛盾的關係之中，最特別的是經濟活動與國家安全之間的關係；因為獲利的是從事某經濟活動的極少數人，個人獲益感極為強烈，而受害者常常包含全國人民，個人受害感較為遲鈍。舉例而言，如一個國家金融監理不周、壞帳太多而產生金融風暴，導致銀行封閉或存戶不能提領現金或匯款，這是銀行體系中斷運作與服務，當然是對國家安全的傷害[33]；又如在2003年春天自中國傳入的SARS傳染疾病流行臺灣，假如最後導致臺灣醫療體系即使有醫院、醫師與護士，但一般病患即使有錢，卻不知道如何看醫生，得不到醫療照顧，這就等於醫療體系癱瘓，自然也是國家安全的傷害[34]。濟體系受到實質影響的議題上，國家安全所涉及的情報工作，基本上便與犯罪偵查沒有太大的關連。為了防止其他國家對我國經濟體系產生過度的影響，對於相關經濟活動的情報蒐集，原則上並無涉於犯罪偵查之進行，例如對於重要產業的情報蒐集，可能僅涉及是否允許開放進出口的決策，此時所為之情報蒐集工作便與犯罪偵查無涉。而鑒於特定重要經濟活動之管理將影響我國與他國貿易之依存關係，亦不能否定有對特定經濟活動進行情報蒐集以維護我國經濟安全之必要。

三、個別規範之必要性

由於國安情報監察的目的，尚包括保護本國不受到外國勢力或其工作人員的攻擊或敵意活動的威脅、維護國家安全，以及抗制恐怖主義或其他秘密情報活動之內涵，而為犯罪偵查目的所進行的通訊監察，多半僅是為了蒐集與已經發生的犯罪行為有關的證據，因此，兩者難免存在政策上及實際運作上的本質差異。事實上，在進行為維護國家安全的情報蒐集或監察工作時，其往往涉及較為廣泛且不同類型的資訊來源，監察的對象也通常較不特定，而犯罪偵查就比較不會有這樣的性質。再者，犯罪偵查發動的對象往往是本國人民，但是，國安情報監察往往涉及外國人，鑒於本國人與外國人受到我國憲法保障的程度本來就會有所不同，縱然犯罪偵查與國家安全工作固然有其相類似之處，但仍應有不同的規範。換言之，雖然情報蒐集不一定與犯罪偵查有必然之關係，然而一般犯罪偵查與國家安全工作情報蒐集間

文化、時間觀念、教育和訓練水準、資訊來源、媒體報導、民生用品等枝微末節，都可做為情報評估或推敲之要素」，參閱周玄明，＜隨機性國際通訊情報偵蒐法制研究＞，頁31，《國防大學管理學院法律學研究所碩士論文》，2010年1月。

33 雖然國家安全是一個抽象的上位概念，如果同意國家安全具有：「民主的政治、經濟、社會體制的穩定運作、免於中斷的危險與威脅」之內涵，必然也會肯認對於民主制度的政治、經濟、社會穩定運作基礎的威脅，可能來自國家內部，也可能來自國家外部。來自國家內部的威脅主要來自因為經濟活動或因為政府經濟政策不當，就其可能產生的原因分析，可能包括：⑴財富、所得分配不均或貧窮階級的大量存在，⑵金權政治與經濟倫理的淪落，⑶勞工與資本家互信的缺乏與關係的惡劣，⑷殘缺不足的社會福利與社會保險體系，⑸經濟活動造成惡劣的環境品質，⑹社經資源分配不當而產生的公共衛生體系問題，⑺政府財政紀律淪喪，以及⑻脆弱的金融監理制度等等。以上這些原因有的會造成階級間的、社區間的、族群間的暴力衝突；有的會因為政治、經濟、社會體制負荷過重而停擺；有的則會因為問題的骨牌效應或傳染性而演變成政治、經濟、社會體制的局部或全面癱瘓。而由國際經濟關係而產生的對國家安全的威脅，基本上屬於來自於國際經濟或特定國家的過度影響，以貿易關係為例，假如有大小兩國，它們之間的貿易量佔大國貿易量的百分之一，但卻占小國貿易量的百分之90，這對小國而言就是依賴，因為小國的貿易量百分九十必須仰賴大國及其政策的變化；可是同樣的貿易量對大國而言就是「宰制」，因為小國對大國的貿易量幾乎沒有影響力，可是大國貿易活動及政策卻能左右小國百分之九十的貿易量。因此，有主張遠離大國「實質影響」是獲得經濟安全的必要步驟。參閱林健次，經濟安全與國家安全，＜http://www.wufi.org.tw/republic/rep31-40/no32_17.htm＞（最後造訪日：2010年9月3日）。

34 參閱經濟安全與國家安全，available at: ＜http://mail.cysh.cy.edu.tw/～educytw/teach/edu/E-D-008.doc＞（最後造訪日：2010年9月3日）。

卻存在相當多類似之處。既然這兩者有許多相似之處，其在程序上勢必存在類似的遵循規範；不過，正由於二者並非完全相同，因此自無遵循完全相同規範之必要。舉例來說，國家安全機關為蒐集與犯罪無關之情報而進行通訊監察時，其所適用的程序要件因不存在犯罪嫌疑之故，本應有與偵查機關為偵查犯罪時所遵循之程序不同。又因國家安全情報蒐集具有較高之機密性，並可能嚴重危害情報工作人員之人身安全[35]，其與犯罪偵查之專業不盡相同，基於效能與安全因素之考量，美國國家安全委員會 1984 年修訂之第 9 號情報指令規定：「政府發佈與一般情報蒐集有關的命令、指令、政策或建議，除非特別聲明適用於通訊情報活動，否用均不適用[36]」，而美國之「外國情報監察法（Foreign Intelligence Surveillance Act，簡稱 FISA）」更以蒐集情資並非為偵查起訴犯罪行為可適用針對身分之較低標準，並進一步跳脫以「個別犯罪嫌疑」的犯罪偵查標準而以特定身分為是否許可通訊監察之判斷標準[37]，易言之，許可國安情報蒐集之門檻甚至應踐行之程序，原不必然等同於許可一般犯罪偵查標準，此觀美國雖已於 1968 年制定犯罪控制與街道安全法第三篇（Title III of the Omnibus Crime Control and Safe Streets Act，簡稱 Title III）允許得依標準更嚴格之令狀原則，在未經當事人同意前提下對涉犯重罪者之有線與口頭通訊進行監察[38]，並於 1986 年通過電子通訊隱私法案（the Electronic Communications Privacy Act，簡稱 ECPA）補強 Title III 於電子通訊（包含電子郵件與行動電話通訊）規範之不足[39]，卻仍於 1978 年單獨針對國安情報監察事件制定 FISA[40] 以規範國安情報蒐集之通訊監察[41]；英國國會除於 1989 年通過安全局法案（Security Service Act）明定國家安全局法定權限包含：保衛國家安全，反制外國諜報、恐怖及破壞活動以及意

35 參閱丁渝洲，《丁渝洲回憶錄》，頁 160，天下遠見出版，2004 年。

36 The special nature of COMINT activities requires that they be treated in all respects as being outside the framework of other or general intelligence activities. Orders, directives, policies, or recommendations of any authority of the Executive Branch relating to the collection, production, security, handling, dissemination, or utilization of intelligence, and/or classified material, shall not be applicable to COMINT activities, unless specifically so stated and issued by competent departmental or agency authority represented on the Board. Other National Security Council Intelligence Directives to the Director of Central Intelligence and related implementing directives issued by the Director of Central Intelligence shall be construed as non-applicable to COMINT activities, unless the National Security Council has made its directive specifically applicable to COMINT. 轉引自周玄明，＜隨機性國際通訊情報偵蒐法制研究，頁 33，註 105，國防大學管理學院法律學研究所碩士論文，2010 年 1 月。

37 參閱廖元豪，＜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 40，2006 年 4 月。

38 See 18 U.S.C. § 2581(3)(4)(5).

39 See Christopher Slobogin, CRIMINAL PROCEDURE: REGULATION OF POLICE INVESTIGATION, 190（West, 2002）.

40 基本上，FISA 將外國情報監察部分從通常通訊監察切割出來。See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-62). 因九一一恐怖攻擊之故，2001 年通過制訂之愛國者法案（the USA PATRIOT Act）將非外國政府支持的恐怖集團也列為通訊監察之對象。而布希政府強行主導通過之保護美國法（the Protect America Act of 2007）僅於 2007 年 8 月 5 日至 2008 年 2 月 17 日間有效施行，於 2008 年 7 月國會又通過新的 FISA 修正案（the FISA Amendments Act of 2008）以因應新的國內外情勢。

41 據美國媒體 2007 年 8 月 24 日報導，美國國家情報局局長麥康奈爾在接受訪問時，首次透露了情報局以往保密的竊聽工作，承認情報機構曾利用私人電信公司竊聽數以千計經美國接通的用戶通話。布希政府依外國情報監察法，利用電信公司進行這些無需向法庭申請批准的竊聽活動。麥康奈爾強調，若通話者至少一方在美國境內的話，政府就須申請法庭令狀才能進行監聽。麥康奈爾說：「如果有一個恐怖分子打電話入境給另一個恐怖分子，我想美國人都希望我們監視該境內人，因此，我們便申請法庭令狀。」但他強調，要申請一張庭令，需要 200 個工時來處理，要竊聽數以千計的電話，逐一申請很不實際。麥康奈爾接受這次訪問的前幾天，美國國會通過了臨時法（the Protect America Act of 2007），允許政府在調查一些關乎國家安全的活動時，無須先申請庭令便進行竊聽工作。這項臨時法案的有效期為六個月。2001 年發生九一一攻擊事件之後，美國總統布希許可情報官員在懷疑電話內容涉及恐怖活動時竊聽。至今年 1 月為止，竊聽工作無須法庭批准。國會由民主黨控制後，竊聽工作的合法性交由外國情報監察法下成立的特別法庭審核。法庭原本裁決政府可以進行竊聽，但後來，另一名法官裁決，竊聽由美國線路接通的電話需要令狀批准。麥康奈爾證實，一些電信公司面對侵犯用戶隱私的訴訟。他說，若新法得以通過，電信公司便會受到保護；但是，新法並無追溯的條文，電信公司不能對以往的竊聽免負責任。參閱大公網，美國情局曾利用電信公司竊聽，＜http://www.takungpao.com.hk/news/07/08/24/YM-785282.htm＞（最後造訪日：2010 年 9 月 3 日）。

圖以政治、經濟或暴力方式顛覆民主體制的不法活動，並得依法取得核可後，進行電子通訊監聽或竊聽工作（為執行此類工作，亦得依法秘密進入私人產業）[42] 外，在維護國家安全目的下，英國於 2001 年制訂「反恐、犯罪與安全法案（Anti-terrorism, Crime and Security Act（ATCS）2001）[43]」要求電信業者保留所有通訊活動以利事後調取 [44]；而德國亦於通常刑事訴訟程序外針對國安情報通訊監察制訂「限制信件、郵政暨無線通訊秘密法（簡稱 G-10）」將國安情報蒐集予以法制化等比較法制探討可得印證。就此而言，縱於我國法制上單獨針對國安情報蒐集之審查許可程序，制定一套迥異於以犯罪偵查為目的之通訊監察法制，亦無違民主國家潮流。

肆、現行情報通訊監察法制之概況與檢討

國家安全（National Security）就國家存續而言是一個至高無上的目標，也是國家機器運作的主要目的。國家安全在傳統的概念上可以說是「國防」的同義字，指的是保護國家的人民與領土，避免受到外來攻擊與威脅，就功能而言，國家安全乃是「一個國家保護其內在價值，使其免於受外來威脅的能力」。基本上，威脅除包含即將或已經發生的事實外，亦涵蓋某一事件發展至某一階段時，嗣後所構成的威脅，故當威脅影響到國家安全時，本應儘早掌握威脅的來源，避免威脅的發生以及可能的擴大[45]。關於以國安情報蒐集為目的之通訊監察，現行規範主要有國家情報工作法及通訊監察法，一般而言，前者屬於國家安全工作的一般性規範，後者始有針對以國家安全為目的的通訊監察予以具體規定。然而現行法制是否足資規範以國家安全情報蒐集為目的之通訊監察，並完善國家安全之建構，國內文獻甚少著墨[46]，自有予以檢討之必要。

一、國家情報工作法之相關規定及疑義

我國於 2005 年實施國家情報工作法，該法旨在規範政府所進行的情報蒐集活動，其中規定了情報工作所得使用的方式、所應蒐集的資訊類型、其他行政機關得協助義務、取得資料的處理及監督報告義務。依國家情報工作法草案之說明，情報工作係整體國力之一環，而反情報工作則是國家競爭力之根基。強大之蒐情能力可提供情報研析人員更正確、客觀之提出研析報告，以為政府決策參考。堅固之反情報網可遏制敵人之滲透破壞或竊取國家機密，保障國家之生存與發展。而遭濫用之情報工作可能戕害民主政治之正常發展，成為執政者掌控異議人士之工具，甚至是誣陷抹黑、政黨惡鬥之劊子手。冷戰結束後，由於全球化進程之加

42 英國政府中專責國內安全之情報機關自西元 1909 年成立迄今，已有近九十多年歷史，原先名為秘密勤務局（Secret Service Bureau），為因應第一次世界大戰國內安全需要設立，1916 年更名為 MI5，1931 年再更名為安全局（Security Service）迄今，惟外界仍習以 MI5 稱呼，MI5 與另一國外情報機構秘密情報局（Secret Intelligence Service 習稱為 MI6）分別負責國內外情報及安全工作。MI5 職掌幾經變動，東西冷戰結束後，英國國會於 1989 年通過安全局法案（Security Service Act)方才對該局的職掌及相關機制，均予以明確界定。歐盟人權委員會(European Convention on Human Right）對該法案中所賦予安全局的職掌及制衡監督均予以肯定。參閱調改論壇，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＞（最後造訪日：2010 年 9 月 3 日）。

43 See Anti-terrorism, Crime and Security Act (ATCS) 2001, available at: ＜http://www.legislation.gov.uk/ukpga/2001/24/contents＞（last visited: Sep. 3, 2010）.

44 不過英國資訊委員會（the Information Commissioner）卻認為僅因國安因素即要求保留通訊記錄有違人權法案（Part 11 requires communications providers to keep records of their users' activities for national security purposes. The Home Office and the ISPs are currently discussing a Code of Practice for implementing this that would require ISPs to keep subscription information for one year and web caches for four days. The Information Commissioner has released an opinion that using the information for anything but national security reasons would violate the Human Rights Act. Available at:＜ http://www.privacyinternational.org/countries/uk/surveillance/＞（last visited: Sep. 3, 2010）.

45 參閱廖述賢、王瑞源，＜軍事地理情報支援國家安全決策之研究—以資訊管理為觀點＞，《資訊管理展望》，第 4 卷第 1 期，頁 62，2002 年 3 月。

46 雖然司法院大法官釋字第 631 號解釋曾對通訊監察法制有所指摘，惟觀其內容，其僅檢討以犯罪偵查為目的之通訊監察，至於以國家安全情報蒐集為目的之通訊監察，該號解釋並未有所著墨。

速，針對國際恐怖主義組織、重大跨國犯罪等問題，對國家安全所造成之安全威脅，使得傳統上將基於專業分工與社會發展需求，常以情治工作分立而遂行各自業務職掌之觀念有結合之議，亦即運用情報機關之情資蒐集、分析及行動能力，協助治安機關偵防及打擊犯罪。尤其美國九一一恐怖攻擊事件後，情治相互支援之觀念已漸為先進民主國家所採行。國家情報機關作為「政府資訊提供者」、「國家安全守護者」、「國家利益促進者」及「協助危機處理」之角色功能，為建構 21 世紀情報機關應有之戰略、對策及應變作為，必須凸顯本身之特別優勢條件，提高並領先科技研發水準，同時要整合並增強情報綜合評估能力，運用政策及法律手段保障情報活動，方能符合政策面與國家利益之需求。

依國家情報工作法規定，情報機關[47]執行情報工作[48]必須兼顧國家安全及人民權益的保障，並以適當方式為之[49]，情報機關並不得涉入一定範圍之黨政活動[50]。此外，情報機關應就足以影響國家安全或利益之下列資訊進行蒐集、研析、處理及運用：一、涉及國家安全或利益之大陸地區或外國資訊。二、涉及內亂、外患、洩漏國家機密、外諜、敵諜、跨國性犯罪或國內外恐怖份子之滲透破壞等資訊。三、其他有關總體國情、國防、外交、兩岸關係、經濟、科技、社會或重大治安事務等資訊[51]。情報機關蒐集資訊，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式，並應遵守相關法令之規定[52]。情報機關為了執行情報工作的必要，可以採取身分掩護措施[53]或是設立掩護機構[54]。在維護國家安全利益之必要範圍內，各級政府機關有配合協助情報工作之執行的義務[55]。情報機關於獲取足以影響國家安全或利益之資訊時，應即送交主管機關（亦即國家安全局）處理，如果取得的資訊涉及社會治安之重大事件或重大災難者，除依法處理外，也應該立即送交國家安全局[56]。關於情報工作之監督，國家情報工作法設計了內部及外部兩種不同的監督機制。就內部監督來說，情報機關必須自行建立督察機制，其作業規定由國家情報主管機關（國家安全局）會商各個情報機關定之，並送立法院備查[57]。就外部監督而言，國家情報工作，應受立法院之監督，國家安全局局長與各情報機關首長應於立法院每一會期向相關之委員會做業務報告；於應邀時，並應列席做專案報告[58]，因此，立法者採行的是立法監督的型態，而不是司法控制監督模式。情報工作主管機關每年也應就情報工作的執行成效及興革意見，製作年度總結報告，送立法院備查[59]。大體而言，除以下所述之疑義外，國家情報工作法之規定於適用上尚不致產生規範衝

47 依國家情報工作法第 3 條第 1 項第 1 款與第 2 項等規定，此處之「情報機關」指的則是「國家安全局、國防部軍事情報局、國防部電訊發展室、國防部軍事安全總隊」以及「行政院海岸巡防署、國防部總政治作戰局、國防部憲兵司令部、內政部警政署及法務部調查局」等機關。

48 依國家情報工作法第 3 條第 1 項第 2 款規定，情報工作指的是「情報機關基於職權，對足以影響國家安全或利益之資訊，所進行之蒐集、研析、處理及運用」，也包涵了「應用保防、偵防、安全管制等措施，反制外國或敵對勢力對我國進行情報工作之行為」。

49 國家情報工作法第 6 條第 1 項參照。

50 國家情報工作法第 6 條第 2 項參照。

51 國家情報工作法第 7 條第 1 項參照。

52 國家情報工作法第 7 條第 2 項參照。

53 國家情報工作法第 9 條參照。

54 國家情報工作法第 10 條參照。

55 國家情報工作法第 13 條參照。行政機關應配合的事項及程序也是由主管機關會商各個相關機關制定後，送交立法院備查。

56 國家情報工作法第 18 條第 1 項參照。至於情報蒐集所取得的資訊究竟是否可以作為犯罪偵查或刑事審判之用，本法並未明文。

57 國家情報工作法第 5 條參照。

58 國家情報工作法第 4 條參照。

59 國家情報工作法第 20 條參照。

突，縱於監督模式之議題上存在是否妥適或符合我國憲政體制之疑義，不過該等疑義於本質上屬於立法政策之選擇，並不存在實質矛盾。

依國家情報工作法第 7 條第 2 項規定，情報機關蒐集資訊，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式，然而，同條項所指的「並應遵守相關法令之規定」究竟範圍為何？於情報工作者而言至為重要，蓋依通訊保障及監察法第 24 條：「（第 1 項）違法監察他人通訊者，處 5 年以下有期徒刑。（第 2 項）執行或協助執行通訊監察之公務員或從業人員，假借職務或業務上之權力、機會或方法，犯前項之罪者，處 6 月以上 5 年以下有期徒刑。（第 3 項）意圖營利而犯前二項之罪者，處 1 年以上 7 年以下有期徒刑。」及國家情報工作法第 32 條：「（第 1 項）情報人員或情報協助人員假借第九條及第十條職務上之權力、機會或方法而犯罪者，加重其刑至 2 分之 1。（第 2 項）犯前項之罪，圖自己或其他私人不法利益，因而獲得利益者，得併科新臺幣 100 萬元以下罰金。（第 3 項）犯前項之罪者，所得之利益沒收之，如全部或一部不能沒收時，追徵其價額。」等規定，未遵守相關法令之規定而進行國家情報工作者，將受到刑事處罰。因此僅依國家情報工作法卻「未」遵守通訊保障及監察法等相關法官保留原則或法律保留原則所實施之情報通訊監察，是否該當刑法第 21 條第 1 項「依法令之行為」而不具違法性並不受刑事處罰？換言之，國家情報工作法是否已為情報工作人員於從事情報通訊監察時提供足夠之阻卻違法事由？不無疑義。鑑於現行法制除國家情報工作法外，僅通訊保障及監察法針對通訊監察事項有所規範，如國家情報工作法第 7 條第 2 項「並應遵守相關法令之規定」所指的不是通訊保障及監察法，則其所指為何？於法制上似乎存在矛盾之現象。

或因立法協商之倉卒，國家情報工作法第 7 條之立法理由並未明示「並應遵守相關法令之規定」之範圍為何，因此無從得知立法者是否有意以通訊保障及監察法之規定（特別是法官保留原則）拘束情報工作者。而之所以會出現這個疑義，主要是因為國家安全工作除了具有調查犯罪之作用外，尚包含預防犯罪及與犯罪無關的單純情報蒐集。由於只有前者具有調查上的針對性，因此有關後二類情蒐工作，往往具有大規模實施且對象不特定的特徵。此特徵往往使得與犯罪調查無關之情報蒐集具有高度的不確定性，甚至在實施之前不具備相當理由（probable cause）或合理可疑（reasonable suspicion）而只單純具有可疑的因素而已。因此，關於國家情報工作之執行應遵守之法制為何？現行國家情報工作法第 7 條第 2 項後段「並應遵守相關法令之規定」除衍生前述疑義外，並未提供相當的規範。縱認於刪除「並應遵守相關法令之規定」文字後，即無完全依通訊保障及監察法規定實施情報通訊監察之必要，不過此種作法除將導致人民產生是否實施情報通訊監察即不需「遵守相關法令之規定」之疑慮外，亦未解決執行國家情報監察無法可據之困境。

二、通訊保障及監察法於國安情報監察之適用及疑義

雖然國家情報工作法已授權情報機關執行情報工作，不過徵諸實際，該法並未提供具體的執行依據，就情報通訊監察而言，縱前述國家情報工作法第 7 條第 2 項規定，情報機關蒐集資訊，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式，不過關於如何執行情報通訊監察工作，例如發動基準、申請程序、救濟程序等部分，國家情報工作法並未具體規定。與美國獨立制定 FISA 規範以國家安全維護為目的之通訊監察不同，我國現行通訊保障及監察法涵蓋不同監察目的之通訊監察活動，鑒於通訊保障及監察法第 7 條至第 10 條已特別對以國家安全維護為目的之通訊監察予以規

定，從而相關規定是否足以規範國家安全維護為目的之通訊監察，甚至非以犯罪偵查為目的之通訊監察適用通訊保障及監察法其他條文是否會產生矛盾，即有進一步探討之必要。

原則上，為避免國家安全遭受危害，有監察外國勢力、境外敵對勢力或其工作人員通訊，以蒐集外國勢力或境外勢力情報之必要，國家安全局局長得核發通訊監察書[60]，進行國安通訊監察。本條項所稱「外國勢力或境外敵對勢力」是指「外國政府、外國或境外政治實體或其所屬機關或代表機構」、「由外國政府、外國或境外政治實體指揮或控制之組織」或「以從事國際或跨境恐怖活動為宗旨之組織」[61]，而所謂「外國勢力或境外敵對勢力工作人員」則是指「為外國勢力或境外敵對勢力從事秘密情報蒐集活動或其他秘密情報活動，而有危害國家安全之虞，或教唆或幫助他人為之者」、「為外國勢力或境外敵對勢力從事破壞行為或國際或跨境恐怖活動，或教唆或幫助他人為之者」、「擔任外國勢力或境外敵對勢力之官員或受僱人或國際恐怖組織之成員者」[62]。換言之，其所稱外國勢力或境外敵對勢力不一定為我國所承認的國家，國際組織或是公司團體皆可能該當外國勢力或境外敵對勢力。惟如受監察人在我國境內設有戶籍，除非情況急迫，否則國家安全局局長於核發前項通訊監察書前，必須要先得到高等法院專責法官同意，方得進行通訊監察[63]。雖在情況急迫時，國家安全局局長得逕行核發通訊監察書，惟於事後仍應通知高等法院專責法官補行同意，如未在 48 小時內獲得同意，情報機關應立即停止通訊監察[64]。依前述規定之反面解釋，若受監察人在我國境內未設有戶籍，則無論情況是否急迫，國家安全局局長得不經高等法院專責法官同意逕行核發通訊監察書，進行通訊監察。由於通訊監察書係執行通訊監察之依據，因此國家安全局局長亦應依照通訊保障及監察法第 11 條第 1 項之規定，將案由及涉嫌觸犯之法條、監察對象、監察通訊種類及號碼等足資識別之特徵、受監察處所、監察理由、監察期間及方法、聲請機關、執行機關及建置機關等事項記載於通訊監察書上。原則上國安監察的期間為 1 年，如有必要延長，應附具體理由，在期間屆滿前 2 日，重新進行該法第 7 條之程序[65]。如在監察期間內，國家情報工作機關首長認為已經沒有監察的必要時，應該立即停止監察[66]。為有效達成監察目的，執行上情報機關可以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法進行通訊監察，但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。原則上，於執行通訊監察時，應維持該通訊的暢通[67]。又除法有明文外，依本法監察通訊所得的資料，不得提供與其他機關（構）、團體或個人[68]。而經國安監察程序所取得的資訊除發現有本法第 5 條所定情事外，僅得供國家安全預警情報之用[69]。為予以受監察人救濟機會，於國安監察結束後，監察執行機關應敘明受監察人的姓名及住居所等資料，報由綜理國家情報工作機關陳報法院通知受監察人，惟若認通知有害於監察目的之虞或不能通知者，應一併陳報於法院；除有上述妨害監察目的之虞或不能通知的情形外，法院應於接

60 通訊保障及監察法第 7 條第 1 項參照。
61 通訊保障及監察法第 8 條參照。
62 通訊保障及監察法第 9 條參照。
63 通訊保障及監察法第 7 條第 2 項參照。
64 通訊保障及監察法第 7 條第 3 項參照。
65 通訊保障及監察法第 12 條第 1 項參照。實際上此部分條文所指「提出聲請」並不正確，因為在同法第 7 條所規定之國安監察程序，並沒有向何人「聲請」進行通訊監察的程序，而只有請求專責法官同意或補行同意之程序。
66 通訊保障及監察法第 12 條第 3 項參照。
67 通訊保障及監察法第 13 條參照。
68 通訊保障及監察法第 18 條參照。
69 通訊保障及監察法第 10 條參照。

獲陳報並審查後，通知受監察人；不通知的原因消滅後，監察執行機關應報由國家情報工作機關陳報法院補行通知[70]。執行機關於開始國安監察後，應按月向綜理國家情報工作機關首長報告執行情形，綜理國家情報工作機關首長亦得隨時命執行機關提出報告或主動監督執行情形[71]，不過執行機關並不需對於其他機關提出報告。如有必要，執行機關可以長期留存監察通訊所得資料，如無長期留存必要，執行機關亦得於結束通訊監察後五年內保存所取得的資料，逾期後，始予銷燬；此外，監察所得資料全部與監察目的無關者，經執行機關報請綜理國家情報工作機關首長許可後，才會銷燬[72]。

先就通訊保障及監察法第 7 條特別以國家安全維護為目的之通訊監察規定而論，現行對在境內設有戶籍者進行通訊監察須經高等法院專責法官同意之規定，是否足為採行令狀原則之論據，不無疑義，蓋依令狀原則，通訊監察書（搜索狀）應由中立之法官核發，如對法官否准之決定不服，仍得向上級法院提出抗告。今該法僅要求應經高等法院專責法官之同意，其同意之性質為何，司法處分？行政處分？如該專責法官不同意，究應如何尋求救濟，抗告？訴願？觀之該法並未明文，適用上難免疑義。又現行經高等法院專責法官同意之規定，是否表示我國之國安情報監察不採令狀原則，該規定係令狀原則之緩和？觀其立法理由亦未說明，因此，對於國安情報監察得否僅因符合法律保留原則而由行政機關單獨決定發動與否，亦不免令人困惑。此外，相較於同法第 5 條以「有相當理由可信其通訊內容與特定犯罪有關，並危害國家安全或社會秩序情節重大」與第 6 條以「有事實足認犯特定罪名，為防止他人生命、身體、財產之急迫危險」為發動通訊監察要件之規定，通訊保障及監察法第 7 條似未明文發動通訊監察之要件，蓋該條「為避免國家安全遭受危害，有監察通訊以蒐集外國勢力或境外勢力情報之必要」等文字充其量僅揭示實施國安情報通訊監察之目的在於「避免國家遭受危害」，至於是否須具相當理由或合理可疑認受監察人具體涉及何等危害國安事件，該條並未規定，此種立法不免令人質疑是否只要足以避免使國家安全遭受危害，不論其事件為何，亦不論發動通訊監察時該事件具體程度為何，皆足以開啟國安情報監察程序。事實上，在現行通訊保障及監察法第 7 條之規範模式下，只要打著避免國家安全遭受危害之旗幟，不論理由為何，皆可任意進行情報通訊監察，有趣的是，雖該條要求對境內有戶籍之人進行通訊監察之前須得到高等法院專責法官的同意，但同意的對象為何？是足以避免國家安全遭受危害？或是有無監察通訊之必要？實在令人難以理解。因此，在欠缺進行情報通訊監察具體要件之前提下，現行通訊保障及監察法第 7 條之規範並不具有攔截功能，反倒令人產生空白授權國家情報工作主管機關自行決定通訊監察要件之疑慮。

再就通訊監察之方式而言，依通訊保障及監察法第 13 條第 1 項規定，情報機關得「以截收、監聽、錄音、錄影、攝影、開拆、檢查、影印或其他類似之必要方法」執行通訊監察，惟為免侵害人民之居住安寧，並防止國家機關藉通訊監察之名義侵入私人住宅，立法之際遂有立法委員提案增訂同條項但書「但不得於私人住宅裝置竊聽器、錄影設備或其他監察器材。」規定，以限制通訊監察之手段。依此規定，如於私人住宅裝置竊聽器等監察器材進行通訊監察，執行人員將觸犯該法第 24 條規定並受刑事處罰。然而，不論監察目的為何，限制於私人住宅裝置竊聽器、錄影設備或其他監察器材進行通訊監察是否有助於監察目的之達成，於手段目的之關聯上，似乎亦存在不小的疑慮。蓋依通訊保障及監察法第 3 條第 1 項規定，通訊監察之對象除以電信設備為媒介之通

70　通訊保障及監察法第 15 條參照。
71　通訊保障及監察法第 16 條參照。
72　通訊保障及監察法第 17 條參照。

訊外，尚包含「郵件及書信」與「言論及談話」等傳統通訊，對於此等傳統通訊之監察，因無法透過電子通訊監控之手段予以達成，果有監察之必要，似乎只能期待以傳統的通訊監察手段（錄音、錄影、攝影、開拆、檢查、影印）達成其目的。此時如不允許執行機關於私人住宅裝置竊聽器等監察器材執行傳統之通訊監察，在有必要的時候，執法人員似乎也只能「親自」至私人住宅秘密地執行有關的通訊監察，如此一來，恐將對於人民居住安寧產生更大的危害，而有違原來保障人民居住安寧之立法本旨。鑑於外國立法例並無相類似之限制規定，似可考慮將傳統通訊排除於通訊保障及監察法第 3 條第 1 項規定之外，或是刪除通訊保障及監察法第 13 條第 1 項但書規定，以符實際通訊監察之需要。而採前者的模式，並非一律允許傳統的通訊監察手段，只不過將其監察回歸到一般的搜索法則；而在令狀原則之保障下，不論何者均不致於對人民隱私權造成過度侵害。

三、情報通訊監察法制應有之內涵

基於以上之分析，現行國家情報工作法與通訊保障及監察法等相關規定並未充分提供國安情報監察工作所需之規範基礎。由於以犯罪偵查為目的之通訊監察與以國家安全為目的之通訊監察各有不同的需求與作用，因此本質上原不應以同一套通訊監察法制作為不同目的通訊監察之執行依據。鑒於以國家安全為目的之通訊監察存在個別規範之必要，且國家情報工作法第 7 條第 2 項亦要求情報機關遵守與國家情報工作相關之法律，因此現行通訊監察法制，即有針對情報工作之需求重新加以調整之必要，蓋於現行通訊保障及監察法制定之際，尚未制定國家情報工作法。又因現行情報法制存在上述缺點，因此在重新調整通訊監察法制時，特別在制定國家情報通訊監察法時必須要：㈠明定發動國家情報通訊監察之要件與審查基準，㈡明定國家情報通訊監察採行令狀原則，㈢明定緩和令狀原則之要件，㈣明定國家情報通訊監察法為國家情報工作法第 7 條第 2 項所指之相關法令，㈤明定國家情報通訊監察得採用任何有助於達成監察目的之執行方法，以及㈥明定國家情報通訊監察之聲請被駁回時之救濟程序。至於對國家情報通訊監察應採何種監督模式[73]、通知義務及免除通知義務之範圍與程序、違法監察之賠償責任、監察所得資料之利用、保存或銷毀、證據排除法則之適用[74]、是否設置專責法院或專責法庭以及如何強化司法審查之專業知能等議題，縱或於現行

73 前法務部長葉金鳳曾指出，『目前情報活動雖非全然沒有監督規劃，然或其規定散見於不同之法律，或實際運作結果無法發揮應有之監督功能，難收監督之效。首先就行政監督而言，情報機關與其他行政機關一樣，其上級機關當然有監督所屬下級機關之權限，且此種行政的自我監督往往是最有效的監督方式。惟如眾所周知的事實是調查局與軍事情報局雖分別隸屬於法務部與國防部，但其局長人選之最後決定權未必就是其所直接隸屬之上級機關法務部與國防部，則此上級機關所能發揮之監督功能自是有限。其次就司法監督而言，因受限於情報活動之隱密性及司法係懲罰於行為後之被動性與事後性，亦難發揮事前防範監督之效。再就監察院之監督而言，監察院固亦得行使彈劾及糾舉權，然亦侷限於違法或失職者，其監督效能之不足與司法監督無異。此外，民國 82 年雖有國安二法之公布，其中「國家安全會議組織法」第 8 條亦明定「國家安全會議及其所屬國家安全局應受立法院之監督」，然實施以來，除於審查預算時列席立法院報告並備質詢外，有關業務執行等之監督，仍然力不從心。…既然現有之行政、司法及監察院之監督機制，均難發揮監督之功能，不妨參採外國之立法例改由國會監督』，參閱葉金鳳，儘速訂立「國家情報監督法」，聯合報，91.01.10，15 版，<http://old.npf.org.tw/PUBLICATION/NS/091/NS-C-091-014.htm>（最後造訪日：2010 年 9 月 3 日）；關於外國兼監督模式的介紹，可參考（香港）立法局秘書處，議會監察情報機關的機制，1995 年 10 月，<http://www.legco.gov.hk/yr97-98/chinese/sec/library/956crp03.pdf>（最後造訪日：2010 年 9 月 3 日）；黃少健，（香港）立法會秘書處，選定地方議會監察情報機關的機制，2008 年 5 月 30 日，<http://www.legco.hk/yr07-08/chinese/sec/library/0708rp06-c.pdf>（最後造訪日：2010 年 9 月 3 日）。

74 與美國法制不同，為了避免受監察對象迴避使用通訊設備或導致情報機關將來不易取得監察許可，基本上英國情報機關亦同意通訊監察所得資訊僅得作為預警情資之用，並相當程度接納法院不採監聽資料作為定罪證據之見解。Given the extent to which American investigators and prosecutors rely on such evidence to build their cases, U.S. officials are amazed that the British have not changed their laws-especially as U.S. officials who work closely with British agencies say that U.K. authorities are very skilled at using electronic methods to gather intelligence. Why are the British so reluctant to change？ …The fear inside British intelligence is that if U.K. laws were to be changed, it might become more difficult for intelligence officers to obtain such surveillance permission. Some officials fear that surveillance requests would face more stringent initial scrutiny-such as a requirement that they be

法制已有明文，惟於立法政策之取捨，或有再行檢討之空間。

伍、通訊監察法制之新架構：代結論

由於通訊監察本身屬於有效的情報蒐集手段，因此不論其目的為犯罪偵查或國家安全，均存在實踐上之必要性。不過因通訊監察之實施將對人民造成相當程度之權利侵擾與限制，其於實踐上更需具備高度正當性。雖然立法者就通訊監察之要件與程序享有立法形成之空間，然於憲法第 23 條之拘束下，通訊監察法制之內容仍必須符合實質正當之要求。

本文旨在探討現行通訊監察法制於國安情報監察之適用及衍生之疑義，由於我國國家安全法制建制沿革上並未對通訊監察事項作整體規劃，在法務部與國家安全局各自主導通訊保障及監察法與國家情報工作法立法之前提下，有關國安情報通訊監察之法制間，難免出現不協調之流弊。經整體分析檢討現行通訊監察法制並指出現行法制於執行層面所衍生之疑義後，為能有效杜絕非法監聽，完善通訊監察法制，並滿足國家安全維護之需求，本文主張應制定以國安情報通訊監察為主要目的之專法，用以規範以國家安全維護而非以犯罪偵防為目的之通訊監察，如此亦可避免情報工作人員因法制不健全而罹刑章，符合轉型正義。此外，為免通訊監察法制間出現積極衝突，本文亦主張應修正現行通訊保障及監察法，使之成為以犯罪偵查為目的之通訊監察專法。而因不同目的之通訊監察各有不同之制度需求，因此二者間本質上原即存在寬嚴不一的發動要件與監督模式，此為建構完整通訊監察法制時所應特別注意之處。

參考書目

一、中文

1. 廖述賢、王瑞源，＜軍事地理情報支援國家安全決策之研究—以資訊管理為觀點＞，《資訊管理展望》，第 4 卷第 1 期，2002 年 3 月。
2. 李明，《監聽制度研究－在犯罪控制與人權保障之間》，法律出版社，2008 年 7 月。
3. 陳愛娥，＜中國法律思想中的人權觀念著眼於其對臺灣社會法律意識的可能影響＞，《政大法學評論》，62 期，1999 年 12 月。
4. 李震山，《多元、寬容與人權保障-以憲法未列舉權之保障為中心》，元照出版，2007 年 9 月。
5. Arthur S. Hulnick，蕭光霈譯，《情報與國土安全》，國防部史政編譯室編譯處，2006 年 10 月。
6. Anne-Marie Slaughter，馬占斌、田潔譯，《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，2009 年。
7. 蔡庭榕，＜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，2003 年 8 月。
8. 周玄明，＜隨機性國際通訊情報偵蒐法制研究＞，《國防大學管理學院法律學研究所碩士論文》，2010 年 1 月。
9. 曾正一，《偵查法制專題研究》，中央警察大學，2006 年 10 月。
10. 許華孚，＜錄影監視系統在犯罪控制運用的省思＞，《犯罪學期刊》，12 卷 1 期，2009 年 6 月。
11. 李震山，＜人性尊嚴＞，《法學講座》，17

approved by an independent judge rather than an elected politician-to ensure that electronic evidence ultimately would hold up in court. British intelligence officers are also concerned that widespread publicity about the use of electronic surveillance evidence in court could make criminals and terror plotters more cautious in their communications-and might put informants at risk. U.S. officials familiar with British investigations say that some recent apparent terror investigation slip-ups by British authorities can be explained by the gap between the raw intelligence-particularly in the form of electronic surveillance information-available on suspects and the inability of prosecutors and police to produce this evidence in court. In some cases, U.K. investigators have indicated to their American counterparts that they are certain that a suspect is up to no good, but have little if any evidence-other than electronic surveillance-to make the charges stick. See Intel Gap, Why Britain still bars wiretap evidence in its courts-and how this can affect terror cases, available at: ＜http://www.msnbc.msn.com/id/14588865/ns/newsweek-newsweek_national_news/＞（last visited: Sep. 3, 2010）.

期，2003 年 5 月。
12. 詹鎮榮，＜秘密通訊自由＞，《法學講座》，21 期，2003 年 9 月。
13. 王兆鵬，《美國刑事訴訟法》，元照出版，2007 年。
14. 法務部，《通訊監察法草案研究制定資料彙編》，法務部，1992 年。
15. 丁渝洲，《丁渝洲回憶錄》，天下遠見出版，2004 年。
16. 廖元豪，＜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，2006 年 4 月。

二、英文

Christopher Slobogin, CRIMINAL PROCEDURE: REGULATION OF POLICE INVESTIGATION (West, 2002).

三、網路資料

1. THE INTERNATIONAL COMMUNICATION UNION, About mobile technology and IMT-2000, available at:＜ http://www.itu.int/osg/spu/imt-2000/technology.html＞（last visited: Sep. 3, 2010）.
2. Anti-terrorism, Crime and Security Act (ATCS) 2001, available at: ＜http://www.legislation.gov.uk/ukpga/2001/24/contents＞（last visited: Sep. 3, 2010）.
3. 蘇位榮、熊迺祺，一見監聽譯文 白手套邱創舜 呆 住，＜http://udn.com/NEWS/NATIONAL/NATS9/5783445.shtml＞（最後造訪日：2010 年 9 月 3 日）。
4. 李子哲，監聽要嚴守法定程序，＜www.libertytimes.com.tw/2004/new/jan/15/today-o6.htm＞（最後造訪日：2010 年 9 月 3 日）。
5. 吳榮修，人民秘密通訊權的保障與限制，＜http://www.afa.gov.tw/friendlyprint.asp? tableName＝service&CatID＝657＞（最後造訪日：2010 年 9 月 3 日）。
6. 何哲欣，監聽核准率 75 %「侵犯人權」，2010 年 06 月 10 日蘋果日報，＜http://tw.nextmedia.com/applenews/article/art_id/32575905/IssueID/20100610＞（最後造訪日：2010 年 9 月 3 日）。
7. 澳門日報，水門事件背景，＜http://www.macaodaily.com/html/2009-07/23/content_344736.htm＞（最後造訪日：2010 年 9 月 3 日）。
8. 敏洪奎，水門事件啟示錄，自由廣場，＜http://www.libertytimes.com.tw/2006/new/jun/15/today-o1.htm＞（最後造訪日：2010 年 9 月 3 日）。
9. 郭崇倫，忍受監聽還是忍受犯罪？中時電子報 2010-06-08，＜http://forum.n.yam.com/trackback.php/20100608505723＞（最後造訪日：2010 年 9 月 3 日）。
10. 林健次，經濟安全與國家安全，＜http://www.wufi.org.tw/republic/rep31-40/no32_17.htm＞（最後造訪日：2010 年 9 月 3 日）。
11. 經濟安全與國家安全，available at: ＜http://mail.cysh.cy.edu.tw/～educytw/teach/edu/ED-008.doc＞（最後造訪日：2010 年 9 月 3 日）。
12. 大公網，美國情局曾利用電信公司竊聽，＜http://www.takungpao.com.hk/news/07/08/24/YM-785282.htm＞（最後造訪日：2010 年 9 月 3 日）。
13. 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＞（最後造訪日：2010年9月3日）。
14. 葉金鳳，儘速訂立「國家情報監督法」，聯合報，91.01.10，15 版，＜http://old.npf.org.tw/PUBLICATION/NS/091/NS-C-091-014.htm＞（最後造訪日：2010 年 9 月 3 日）；（香港）立法局秘書處，議會監察情報機關的機制，1995 年 10 月，＜http://www.legco.gov.hk/yr97-98/chinese/sec/library/956crp03.pdf＞（最後造訪日：2010 年 9 月 3 日）；
15. 黃少健，（香港）立法會秘書處，選定地方議會監察情報機關的機制，2008 年 5 月 30 日，＜http://www.legco.hk/yr07-08/chinese/sec/library/0708rp06-c.pdf＞（最後造訪日：2010 年 9 月 3 日）。