壹、 前言

本次會議「二ＯＯ一年新興全球經濟威脅主管研討會」（2001 Emerging Global Economic Threats Managers Conference）係由美國司法部聯邦調查局（Federal Bureau of Investigation，FBI）舉辦，共邀請全球三十餘國之相關單位共八十代表與會，其中美國聯邦調查局派駐海外其他國家之聯絡官亦有近二十名與會，協助與其他國家建立合作關係；研討會於維吉尼亞州聯邦調查局訓練中心（FBI Academy，Quantico，Virginia）舉行，研討會主要討論的主題為：美國聯邦調查局對抗國際間白領犯罪（White Collar Crime），內容包含各種經濟詐欺（Various Economic Fraud）、網路銀行（Cyber Banking）、網際網路詐欺（Internet Fraud）、安全（Securities）、主要銀行詐欺（Prime Bank fraud）及反托辣斯及洗錢（Antitrust and Money Laundering）。本報告內容含參加 2001 Emerging Global Economic Threats Managers Conference 研討經過、訪查美國聯邦調查局國家資訊基礎建設防護中心（National Infrastructure Protection Center，NIPC）、訪查美國聯邦調查局舊金山分部（FBI Office San Francisco）及結語等。

貳、 研習經過

一、 美國聯邦調查局對抗國際間白領犯罪之作法

（一）加強與各國政府交流合作，協助取締不法。

（二）於重要國家美國大使館或辦事處派駐聯絡官。

（三）加強與銀行間之合作、監控防止白領犯罪之洗錢管道。

（四）協助訓練各國犯罪偵查人員，並巡迴舉辦各類研討會，共同打擊犯罪。

（五）建立聯絡對話窗口協同辦案。

二、 建立跨國司法部門合作：

（一）美國必須主動與其他國家司法部門建立關係。

（二）提昇訓練外國執法人員能力，美國聯邦調查局於二〇〇一年預計開設二六三種課程，召訓一六三國家計九二〇五人訓練，二〇〇二年預計開設二八九各種犯罪偵防教育訓練課程，預計召訓一〇、一一五人。

（三）因應不同新興犯罪建立相對應專責偵防單位：由於科技時代之進步，各類犯罪均已大規模使用現代科技為犯罪工具，各國亟須建立相對應單位，以能專業專責有效對抗。

三、 澳洲警方對抗白領犯罪之經驗：

（一）科技進步定由民間主導，是以必須與民間機構建立一互信機制，必協助建構一安全之網路經濟環境。

（二）加強國際合作。

（三）預防重於偵查，澳洲警方應主動宣導網路安全防止民間電腦被破壞，減少網路犯罪。

（四）要求業者自律及建立法規規範相關民間領域。

（五）教育訓練，提昇執法人員素質。

（六）情報與資訊互享。

（七）建立跨國性二十四小時聯絡機制。

四、 美國聯邦調查局對抗網路犯罪之專責單位及相關案類統計：

（一）全國資訊建設保護中心（National Infrastructure Protection Center, NIPC）**：負責駭客入侵、毀損電腦系統及竊取電磁紀錄等工作。**

（二）網路詐欺報案中心（The Internet Fraud Complain Center, IFCC）**:受理偵辦各類利用網路等工具之詐欺騙財案件、規劃防制策略、開發偵查工具等。**

（三）電腦解析反應部門（Computer Analysis Response Team, CART）**：主要負責線上追蹤歹徒、解讀電磁紀錄及赴法庭作證。**

（四）統計美國網路犯罪最嚴重之情形。

1、 **電子商務詐欺。**

2、 **電子郵件恐嚇。**

3、 **兒童色情。**

4、 **恐佈活動。**

5、 **賭博網站。**

6、 **海外洗錢網站。**

（五）經統計全球網路犯罪案件最多之國家為美國、加拿大、澳洲、英國、德國、新加坡、日本、烏干達、香港等地區。

五、 電子銀行面臨的問題及安全作為：

（一）面臨問題：

1、 **傳輸過程遭欄截、修改。**

2、 **帳號被他人取得。**

3、 **個人資料被竊。**

4、 **不合法之系統入侵。**

5、 **控制電子付款系統。**

（二）安全作為：

1、 進入系統認證程序。

2、 儲存、傳輸時間均應加密。

3、 兩種以上之控制、稽核機制。

4、 網路入侵偵測系統。

5、 事件反應單位。

6、 常態性安全偵測。

7、 行員之訓練。

（三）執行單位應有之作為：

1、 與所有電腦用者合作溝通。

2、 蒐集、分析資訊及教育社會大眾。

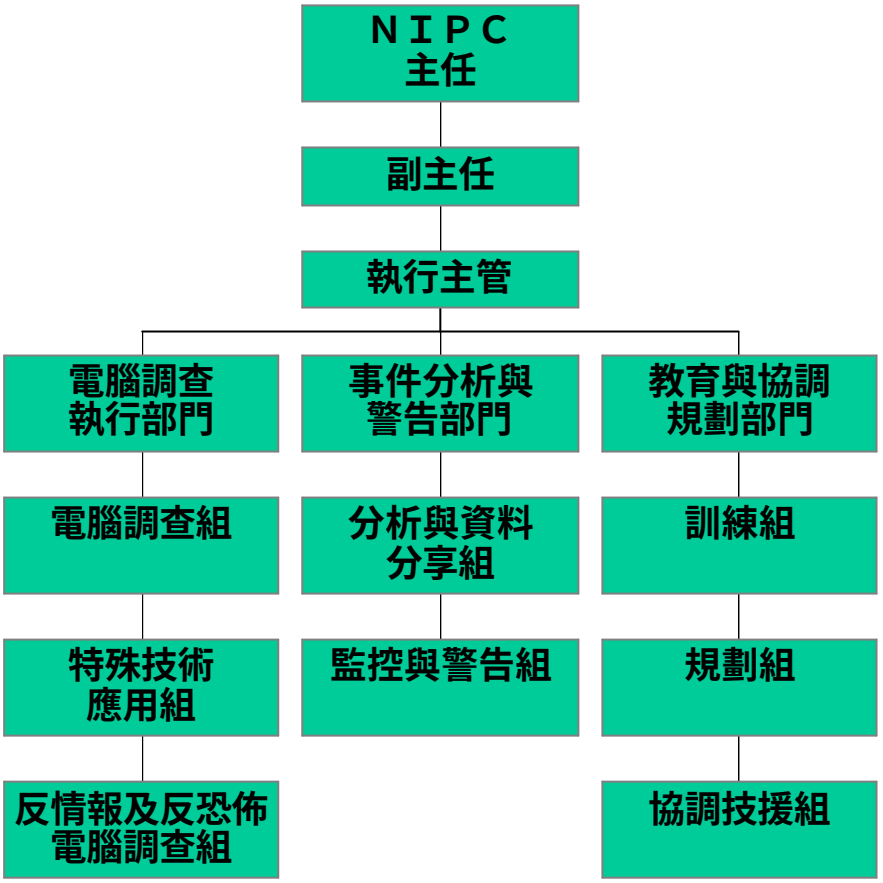
3、 致力跨國合作及討論司法管轄權問題。

4、 評估制定適度之網路犯罪法律。

參、 訪查美國聯邦調查局國家資訊基礎建設防護中心（National Infrastructure Protection Center, NIPC）：

為了解美國聯邦調查局第一線實際偵辦網路犯罪情形，本次訪查原欲前往聯邦調查局紐約辦事處及舊金山辦事處訪查，聯邦調查局表示因紐約辦事處現有重要案子待辦，不適前往，故安排至總部全國資訊基礎保護中心及舊金山辦事處訪查。

訪查國家資訊基礎建設防護中心主要任務及其組織成員如下：



一、 提供必要之協助與方法及協助與方法及協調各聯邦政府機構處理網路入侵及破壞等工作，並調查網路犯罪相關威脅。

二、 提供各種網路犯罪警訊及威脅，並協助網路犯罪相關單位進行分析與調查工作。

其成員約近百人，人員組成八十八人為聯邦調查局人員，十八人來自美國國防部、中央情報局、國家安全部門、飛安部門、商業犯罪調查等近十餘個聯邦政府相關單位，並有加拿大、英國及澳

洲等其他國家常駐代表派員參與，共同打擊網路犯罪。

(一)電腦調查執行部門（Computer Investigation and Operation Section, CIOS）：

1、**電腦調查組**（Computer Investigation Unit）：**負責電腦入侵等案件調查及支援其他單位偵辦網路犯罪案件**。

2、**特殊技術應用組**（Special Technologies Application Unit）：**開發運用電腦偵查技術及負責研發等工作**。

3、**反情報與反恐電腦調查組：建構策略性反應計畫及佈署緊急反應能力**。

(二)事件分析與警告部門（Analysis and Warning Section, AWS）：

1、**事件分析與資料共享組**（Analysis and Information Sharing Unit）：**蒐集資料，並分析歸納弱點、威脅及相關技術**。

2、**監控及警告組**（Watch and Warning Unit）：**二十四小時監控與警告功能，並能直接通知情報、執法及其他相關電腦使用單位**。

(三)教育與規劃支援部門（Training, Outreach and Strategy Section, TOSS）：

1、**訓練組**（Training and Continuing Education Unit）：**構築新課程訓練國內、外執法人員**。

2、**規劃組**（Strategy and Planning Unit）：**負責預算、計畫執行及人事等行政資源事項**。

3、**協調支援組**（Outreach and Field Support Unit）：

（1）**協調維持與友邦及私人建構之資訊交流**。

（2）**支援全國五十六聯邦調查局分支機構之資訊建設保護工作**。

肆、 訪查美國聯邦調查局舊金山分部：

由於舊金山分部管轄地區包含矽谷及其他國際性高科技大廠，亦為全世界高科技研發重鎮，其居民多為科技人才，且網路使用亦較為普遍，而濫用網路科技情形亦較為嚴重，故舊金山分部特別重視高科技犯罪。聯邦調查局舊金山分部網路犯罪分為下列專業分工多個部門：

一、 電腦入侵（Computer Intrusion）：本部門主要負責以電腦網路為目的之入侵攻擊事件及對國家重要基礎建設諸如重要資訊系統、軍事及經濟資訊建設進行非法入侵或阻斷攻擊服務，國家重要基礎建設包含電廠、交通控制中心、金融資訊系統及通訊資訊建設，除此之外有關私人機構入侵攻擊，亦在調查範圍之內。

二、 高科技犯罪（High Technology Crime）：本部門主要負責智慧財產權之盜用，著作權之保障以及諸如半導體商業機密之防護，不論是輸出、輸入或銷售，都在其調查範圍之內。

三、 工業經濟間碟案件（Industry Economy Espionage）：矽谷位於舊金山分部管轄區內矽谷為領先世界之高科技研發中心，而這些廠商多為其他競爭者之攻擊目標，尤其非法蒐集相關商業機密，如設計、規格、市場行銷等相關資訊。

四、 兒童色情（Child Pornography）：兒童色情（十八歲以下）

已被聯邦法律所禁止，舊金山分部亦有專責單位負責調查兒童網路色情之傳輸、製造及張貼；網際網路服務業者亦有義務舉發兒童色情案件。

伍、 結語

經講習與訪查活動得知美國偵辦網路犯罪之軟硬體設備大都須仰賴網際網路服務提供業者（Internet Service Provider, ISP）之協助，其最著名之 Carnival （肉食者）過濾監控網路軟體，聯邦調查局亦否認其之存在，有關電腦鑑識（Computer Forensics）設備方面，聯邦調查局提供數個商業軟體供我國參考。本次受訓最大之收獲在於建立與各國網路犯罪專責單位窗口之關係，並獲得美國允諾同意我國加入 G8 外圍國家之二十四小時不停頓之網路犯罪偵查機制，綜合本次訪查結論如下：

一、 成立跨部會偵辦網路犯罪專責單位，結合各單位網路專業人力，以有效打擊犯罪。

二、 結合民間技術人力，除協助提昇偵查技術外，並可掌握民間技術，免於落後。

三、 結盟各網際網路服務提供業者（Internet Service Provider, ISP），吸納其為整體治安之一環。

四、 運用學術研究機關，遇有網路不法威脅（如病毒、駭客入

侵方式）等，定期或不定期通報公、民營企業。

五、 研究運用美商業軟體現有之電腦鑑識軟體，避免投資浪費。

六、 爭取加入Ｇ８等國際聯盟國家成立二十四小時聯絡窗口。