法務部矯正署綠島監獄廉政暨維護簡訊

107 年 1 月 12 日

廉能是政府的核心價值

貪腐足以摧毀政府的形象

公務員應堅持廉潔，拒絕貪腐

廉政檢舉專線：0800-286-586

「公務員廉政倫理規範問答集」

～行為規範內容～

問：本規範所稱「公務禮儀」為何？請舉例說明

答：（一）意義：指基於公務需要，在國內（外）訪問、接待外賓、推動業務及溝通協調時，依禮貌、慣例或習俗所為之活動（本規範第 2 點第 4 款參照）。

（二）舉例說明：如機關首長或同仁前往其他機關參訪，致贈或受贈紀念品；外交部、僑委會或其他政府官員在國外參加僑社舉辦之活動。

資安趨勢與發展藍圖

資安的概念就是風險管理的概念。通常人都會認為資安應該是要做到滴水不漏，沒有發生任何資安事件，才是好的資安，但是就如同網路長城一樣，再怎麼強大的防護，攻擊方總是可以找到漏洞，進而侵入系統。一個好的資安管理應該是以風險管理為核心，經由審慎地評估與辨識，找出整個環境中最應該保護的核心系統，並經由管理的強化和新技術的導入，而將風險降到最低，讓受保護的標的在完整性、可用性，和機密性的考量下，能維持正常地運作，在受到入侵時即能正確感知，同時更進一步地化為主動防禦。

「情資分享」是資安事件處理中重要的一環資安防護可以區分為早期預警、持續監控、通報應變，一直到協處改善等四個階段，而這四個階段也是以風險管理為核心理念進行循環，其中「通報應變」是最重要的一環，藉由即時迅速的通報機制，將所發的資安事件情形，藉由標準化的通報訊息，快速地傳遞給主管機關，不僅可以防止事件擴散，更能經由即時地通報，讓其他機關可以有警覺，並能進行防禦，而且經由快速的通報機制，也可以讓主管機關掌握事件的影響面，以確認是單一事件或是大範圍的攻擊，這對於資安防護都有重要的影響。例如以今年的 WannaCry 勒索病毒為例，經由事前的通知及提醒各政府機關應注意的事項，再加上病毒擴散期間各政府機關即時地回報，讓行政院資安處可以掌握最新的情形，將影響降到最低。而在事後，TWCERT/CC 也將相關的訊息經由國際連結管道，傳遞給其他國家，透過國內政府機關內的縱深防護，到跨機關的資安訊息交換，乃至跨國間的資安聯防，使得資安事件的影響可以降到最低，不致造成重大的損害。

我國資安推動四大策略我國因政治情勢特殊，曾經在一個月內遭受到

超過 2 千 4 百萬次來自境外的攻擊，這些攻擊樣態的樣本數遠多於其他國家，同時境外惡意組織經由攻擊我國所累積的經驗，進一步調整及優化後，轉而攻擊其他國家，因此許多國家都很希望和我國在資安方面進行合作，希望能取得並分析這些攻擊的行為與模式，而這也是我國長期累積經驗所取得的優勢。但是也由於我國內需市場中的資安產業規模不足，以及缺乏長期的資安人才培育制度，使得不管是政府或是民間產業，都有資安人才不足的危機，而這也是政府必須以整體面來思考，從資安通識人才的培育、到資安專才的養成、職涯的發展、以及高等資安技術的研究等進行規劃與推動。也就是說從教育體系、研究體系、國防體系、政府體系，以及就業體系等，必須有一長程且完整的規劃，以培育資安人才。目前行政院已經規劃了第 5 期的國家資通安全發展方案，期程從 106 年到 109 年，希望以打造安全可信賴的數位國家為願景，並以厚植自我防護能量，保衛數位國家的目標，逐步建構一個安全可信任的數位基礎環境。為達成這樣的願景與目標，我們擬訂了四大推動策略，分別是完備資安基礎環境、建構國家資安聯防體系、提升資安產業自主能量，以及孕育優質資安人才等策略。在完備資安基礎環境部分，考量每個機關的業務特性不同，所要保護的客體和風險管理的重點不同，我們將建立資安治理成熟度的框架，律定風險管理架構，經由 4 個構面 19 項評估原則，由機關依據實際需求，逐年提升資安治理成熟度。在建構國家資安聯防體系的部分，經由組織內的縱深防禦、擴大到跨機關的聯防、並進而擴張至跨國資安情資交換，讓資安防護從點到面，從內部到國際合作；此外，並以會影響國家社會安定的關鍵基礎設施為優先，要求水資源、能源、通訊傳播、交通運輸、緊急醫療、金融與經濟、高科技園區，以及中央與地方政府等八大關鍵基礎設施，建立資安訊息分享及聯防機制，以保護並維持國家的基礎運作。而在提升產業自主能量的部分，我們希望能建構資安的生態鏈，讓資安產業和產業的資安需求能夠銜接，再藉由關鍵基礎設施的場域，使國內資安業者有機會發展新型態的資安顧問與諮詢服務。最後也是最重要的是人才培

育，希望經由學校、研究單位、業界和政府的合作，為我國培育資安產業所需的資安人才，解決各方欠缺資安人才的問題，並完善國內資安自主產業生態鏈，確保各政府機關及關鍵基礎設施之自主性。

結論 資安即是國安，新型態的戰爭中，無實體攻擊所造成的破壞遠遠超過傳統實體攻擊所造成的破壞，例如利用網路攻擊癱 瘓金融體系、交通運輸，乃至水電的供應等，這對現代化國家而言，資訊系統一旦出了問題所造成的影響，將導致社會的運作不穩定，而國家的防衛也難以為繼，因此資安不再只是個人或是組織的安全防護而已，更涉及到國家整體的安全及生存。我國資安未來的發展藍圖，將打造一個安全可信賴的數位國家為願景，並以厚植自我防護能量，保衛數位國家安全為目標，從法規標準到資安聯防，建立自主資安產業到培育人才，期望經由此四個推動策略環環相扣，讓民眾在安全無虞的環境 下，安心使用科技所帶來的便利與服務。

安全維護

軍改後中共網軍所帶來的新風險

2015年11月24至26日，大陸國家主席習近平 於「中央軍委改革工作會議」上宣布啟動大規模軍事改革以來，共軍的一舉一動皆成為國際注目的焦點。從裁撤四總部、七大軍區改制五大戰區及成立新部隊等舉措，都顯示共軍此次變化之大勝於過往。其中，對共軍來說最大的改革便在於火箭軍以及戰略支援部隊的成立。在此次軍改中的兩個新軍種中，二砲部隊改組為火箭軍，並不意外，過去的二砲部隊本身就是一個獨立的兵種直屬中央軍委會的管理。但對另一個新組建的戰略支援部隊來說，卻是讓許多專家感到打破過去許多的傳統，甚至是在中共公布其新軍種後，也未見到太多對於戰略支援部隊的相關報導，更讓此一新軍種披上一層神秘的面紗。目前，外界多半將戰略支援部隊直接與網軍畫上等號，但此種遭到誤導的觀念很容易對其戰力造成誤判。從目前中共公布

的資料顯示，戰略支援部隊是統一掌管情報、網路、航天、電戰及指管系統等建構一體化聯合作戰的關鍵部隊。值得注意的是過去上述四項職能分別各自歸類在不同的組織之中，現今將這些單位聚集於新成立的戰略支援部隊，在戰力整合上是否能發揮預期效果？且這些整合的用意是否能發揮綜效，自然便是值得觀察之處。對網軍而言，在此次軍改後，情報與網軍隸屬於統一的單位之下，雖在公開資料中都顯示戰略支援部隊是為了對未來聯合作戰的信息化進行支援，處於在中央軍委會層面進行指揮，以及在戰區後方支援前線部隊的位置。但值得注意的是，情報單位與網軍單位的結合。戰略支援部隊包含了過去的網軍單位，這也象徵網軍本身亦屬於情報單位的一環，以人因情報搭配網路駭客，將竊取來的資訊由專業人士進行分析，增強網路作戰的效能。而從近期的攻擊樣本分析來看，目前對我國進行網路攻擊的組織，與過去有所不同，許多過去負責攻擊其他國家的組織，在此次軍改後有了變化。開始有混編的狀況，配合情報體系進行網路攻擊。這都讓以社交工程（Social Engineering）為主的APT（Advanced Persistent Threat）進階持續性滲透攻擊更具威脅。特別是在總參二部與三部的整合上，過去中共網軍大多歸屬於總參三部的麾下，但其多半偏重於技術領域的駭客，現今若與總參二部的人事情報與分析能力進行整合，勢必會讓中共網軍的實力如虎添翼，對其他國家的攻擊更為猖獗。如在中共網軍常使用的APT攻擊，是一個有組織有計畫的間諜行為，是一個為目標物量身打造的攻擊策略，需要仰賴的是目標的個人資料、交友關係、閱讀取向與人際網絡，假冒被害人的朋友、師長、同僚冒名發送被害人感興趣以及與時事相關的電子郵件，將惡意程式夾藏在Word、PDF、Excel檔案等方式附加在電子郵件中，讓被害人誤以為是重要文件或是對其主題感興趣主動下載，在檔案開啟的同時，目標的電腦也受到了入侵。因此，APT攻擊除了技術之外，更需要的是對於目標的瞭解與其基本資料的認識。這些資料的蒐集都不是專注於資訊領域的駭客所擅長之處，故若在進行情報組織整合之後，新成立的戰略支援部隊以人因情報搭配網路駭客，中共網軍的

活動應會更為頻繁，配合其他情報體系加強對我國與其他國家的刺探，並且這些行為會更加的專業化與精密化。於2015年底及2016年初時，中共網軍的攻擊有出現較為混亂的狀態，從時間點來判斷期間恰為軍改之際，很有可能正在進行中共網軍組織的調整與重組，而在2016年3月間又恢復攻擊。但在美方的資安報告中，卻認為中國大陸遵守了與美國達成的相關承諾，停止支持網上竊取美國商業機密以利中國大陸公司的商業競爭，報告中指出來自中共網路攻擊的數量下降90%，尤以雙方簽署有關協議後，下降幅度最大。不少解讀認為此舉為中共對美國所釋出的善意。但從科技技術的角度來看，協議的簽署意義並不大，特別是在網路的虛擬空間中，想要透過技術追蹤是有相當的難度，若是透過 VPN（Virtual Private Network）跳板或是殭屍網路的配合，更是增添了追蹤的難度。近期對美國的網路攻擊次數下降，有可能是在軍改部隊轉換時的空窗期，甚至也有可能是中共網軍的攻擊技術更加的進步，更能隱藏在角落持續的刺探目標。這也代表在網域空間中的戰爭，雖然技術不是絕對的參考指標，但是在探討戰略與國際網路安全協議時，若是沒有相關技術做為知識背景，很容易讓協議變成徒具形式的紙上文件。

未來戰爭中，網路安全絕對是致勝的關鍵之一，數位軍火在戰場能發揮的影響力絕不亞於傳統飛機與大砲，如何結合人才技術以及軟硬體的發展並且搭配國家安全的理念，以國防產業的思維來培植資安產業，藉此強化國安與經濟，是我國可以發展的方向。現今的資安問題，已脫離純技術的領域，如網軍攻擊其造成的影響與破壞早已超過黑帽駭客的威脅，這表示資安問題的層級需提昇至國家戰略的高度，也就是蔡英文總統在我資通電軍成立時所說「資安就是國安」，政府應以更全面性的國家安全思維來看資安議題。過去資訊安全的學術研究大多集中在密碼學與理論上，導致與實務脫節。而資安公司的研究又多偏重在實務的操作上，卻忽略了整體面上的思考。因此，未來在網路戰領域的研究，應結合國家戰略的觀點，輔以情報學的思維，並導入國防產業的角度，以「科際整合」來思考資安議題，藉此防衛我國數位國土，進而達成保家衛國

之目的。

消費新知

私人虛擬網路 —資訊攻防主戰場

資訊戰是當今不分平時戰時，幾乎每 分每秒都要面臨之安全挑戰；基於其執行主體為國家機關，或是非屬國家體系下之私人體系，分別成為國安與治安上不同範疇之威脅。 不過嚴格說來，當治安情況嚴重到影響國家公共秩序，或人民生活重要福祉時，將資訊安全歸納為國家安全範疇內加以應對，確實是當前全球主要先進國家共同具有之主流思維。網路之所以影響力驚人，在於其通聯能力，其威脅亦係相伴此特質而生。在討論網路資訊攻防之前，必須依據網路聯通方式與範圍，掌握資訊網路的三大類別。首先，談到專為政治與軍事目的建構之「封閉性網路」；原則上，幾乎所有國家武裝部隊都會建構獨立的作戰指揮網路，並與一般民用網際網路嚴格實體隔離。該網路可同時作為情報傳輸、人事調度、後勤管理與財務會計通聯管道，但此網路基本屬性仍以作戰指揮為主。戰時政府領袖將進行戰爭指導，情報機構與外交部門亦須掌握戰爭動態，因此該網路需與國防軍事單位以外部門通聯，但整體來說，其與民間網際網路毫不通聯。由於此種實體隔離架構，且其資料存取具層層管制，增加攻擊上的困難，亦讓駭客不易得手。其次就是所謂「全球性網際網路」；原則上，可以將其視為—針對人類共同公益目的存在之開放性網路。架構此種網路之網站，基本上對於資料存取與傳輸並無限制，通常其資訊內容亦不會聯結任何機件或自動控制設施，就算其中所含資訊有所錯誤，對於人類社會所產生之干擾或傷害，都必須是閱讀其網站內容者，願意相信其論點，再配合作出相關舉措。在資訊攻防上，不常成為主要目標。最後則是本文所要探討之資訊攻防主要對象—「虛擬私人網路」；虛擬私人網路係架構於全球性公開網際網路上，藉由通信保密規範與加密通道協議（Tunneling Protocol）所建立之保密通信規範，其或稱虛擬專用網路（VPN ： Virtual Private Network），所

處網路空間，雖與全球性公開網際網路共享，但其通訊內容是由人工保密技術加以隔離，其運作就像是由人工所專門架構，建立出另外存在之網路空間。成立完全實體隔離網路，並且維持其運作，必須付出極高成本。就算是美國，其仍有諸多遍及全球之保密性政府資料庫或行政性網路，諸如 NIPRNet、OpenNet、NSANet 及JWICS 等，必須或多或少與公開性網際網路交聯，並藉由虛擬私人網路技術，設定使用權限，限制無權限用戶入侵，但非達到完全實體隔離地步。 同樣地，美國政府幾個事涉機密之敏感資料庫，諸如聯邦調查局及所屬外站用於檢索犯罪偵防資訊之「局內百科」(bureaupedia) 資料庫；美國國防部所架設，專供國防科技以及軍事採購圈內人士，檢索分享軍事科技資訊之「國防科技百科」(DoDTechipedia) 資料庫；美國國務院以及駐外使館所共享之外交檔案電子資料庫「外交百科」(Diplopedia)，亦是運用虛擬私人網路技術加以防護，並管制使用者存取權限，保密程度則是依據資料機敏性加以區分。誠然實體隔離之獨立網路可顯著增加保密性，但基於成本考量，不論是建構階段之硬體鋪設經費，以及日後維護管理成本都極為驚人。在無法負擔高額成本建構實體獨立網路，又有資料保密實際需求時，常求助於虛擬私人網路技術。目前在全球網際網路架構，專為人類社會特定目的存在之封閉性網路，包括交通號誌、飛航管制、金融交換、票券交易、彩券投注、遠距教學、醫療看護、治安監控、環境監測、電力配送、資料檢索與公文交換等，皆須考量保密安全，避免外力介入干擾。掌握網路性質，對資訊安全政策指導至關緊要，資訊安全防護必須適切配置資源，若以高效率方式分派資源，投入最受威脅資訊攻防目標，就能夠產生最理想防護與應變作為。

文字教育

密碼安全性原則，困擾的是駭客-還是自己？

密碼複雜度的設計原來是錯的？當初的發起者已公開坦承錯誤。與其規定英文、數字、特殊符號等組成複雜度，不如追求密碼長度，方便使用又確保安全。

資安事件層出不窮網路 E世代的來臨，使用網路雲端服務已經是日常生活中的一部分，舉凡社群網站（例如臉書）、Google服務（例如信箱、雲端硬碟），或是購物網站、網路銀行等；這些雲端服務提供了使用者便利性，卻也帶來了資安上的風險。近年來重大資安事件接連爆發，連大型的企業組織也不能倖免，例如 yahoo 就曾於2013年爆發10億筆帳號資料外洩，而Apple也曾因為iCloud身分驗證機制的安全缺陷造成多位好萊塢女星私密照外洩，而這些資安事件皆是帳戶身分驗證的環節出了問題。密碼複雜度高就是安全？發明人卻後悔了！身分驗證是存取網路服務的第一步，也是保護個人資訊安全的最基本機制。據統計，民眾最常用的密碼包含：123456、123456789、password、qwerty（鍵盤上的橫排）等，而為了強化帳戶的安全性，防止帳戶被有心人士盜用，許多單位會訂定密碼安全性規範，避免密碼被輕易破解。以 微軟伺服器作業系統所設定的密碼複雜度原則為例，其要求為不包含使用者的帳戶名稱或全名的重要資訊，且必須包含下列4種字元中的3種：英文大寫字元（A到Z）、英文小寫字元（a 到 z）、10 個基本數字（0 到 9），以及非英文字母字元（例如 ！、$、#、%）。照此設定方式，再加上最小密碼長度設定為 8 個字元的話，確保至少 218,340,105,584,896不同單一密碼的可能性，目的是避免密碼被惡意人士用暴力窮舉法輕易破解。這種密碼設定方式開始流行，起因於2003年美國國家標準技術研究所（NIST,National Institute of Standards and Technology）所制定的一份文件附錄，有趣的是，撰寫該安全密碼最佳實踐原則的作者 Bill Burr近日接受華爾街日報訪問時卻直言當初所制定的方式並不十分恰當，並為此造成使用者的不便感到抱歉（“Much of what I did I now regret.”）。他並不是在鼓勵使用容易被破解的密碼，而是因為當初撰寫時沒有考量到人類的惰性問題，太複雜的密碼組成要求不僅徒增困擾且可能還有反效果。與其追求字符複雜度，不如擁抱字串長度其實早在Bill Burr 接受訪問之前，NIST 已變成強調密碼長度而非組成複雜度，只要密碼長度足夠，即使是一串簡單的英文字元所組成的密碼，其排列組合的可能性數量就已足夠。且考慮到一般民眾為了使用方便好記又符合複雜度要求的密碼，常常會利用鍵盤排列（例如 !@#$QWERasdf）、象

形文字（例如將 s 取代成 5，或是將 a 取 代成 @）等手法來設計密碼，這也是為什麼 P@55w0rd 也會登上密碼使用排行榜上的前段班。而對駭客而言，為了節省破解時間，一開始會先利用「慣用密碼紀錄表」來進行密碼破解，故其實“P@5 5w0 r d”比“ilovemycompany”這類簡單規則組成的字串更能輕易被破解。但要特別注意的是，使用簡單組成規則的前提是字串長度要夠長（建議至少 12 個字元），可能性數目才足夠。

改變使用密碼的壞習慣理論上，密碼組成字符愈複雜確實會提升破解的難度，但因為使用的對象是人而非機器，人類的創造力可以無限，但記憶力卻是有限，無法記憶過於複雜的密碼，為了配合複雜度要求反而容易產生其他不安全的使用行為，導致變得更不安全。例如，好不容易創造了一組好記又複雜的密碼，所以在各種網路服務都使用同一組帳號密碼，一招打天下的概念，卻也讓駭客相對省事，拍賣網站淘寶網就曾於 2015 年被駭客利用從他處取得的 9,900 萬筆帳密資料進行比對測試，發現有近兩成的帳戶真實存在，部分帳號因此被用來進行詐騙。用戶可以將重要服務（例如網路銀行）的帳密跟一般服務（例如會員電子報）所使用的帳密有所區隔，至少可以減少帳密外洩的危害程度。另一種常見的密碼安全性政策是要求更換密碼的頻率，例如90天內強迫更換密碼，且限制密碼不可重複使用；這些規定立意良善，出發點是為了避免用戶仍重複使用那幾個愛用的密碼，但所謂上有政策下有對策，例如用戶就會在密碼尾數加上字元 1，下次變更時尾數則變成 2，依此類推，如此一來就喪失了變更密碼的本意。頻繁變更密碼的要求也是在考驗用戶的記憶力，於是有些用戶就將密碼抄錄於紙本或存在電腦桌面的檔案裡，甚至整理成一個 Excel檔記錄各個密碼，心存僥倖的心理使然，反而變成更不安全。為了應付現今各種網路服務制定的各種帳號密碼要求，目前市面上已有業者開發出密碼代管服務，用戶只要記憶一個「超級密碼」，登入該服務後就能存取及管理所有的密碼紀錄。筆者認為一般民眾可能不需要那麼專業的密碼管理服務，但最低限度也不能將密碼寫下來放到抽屜裡藏著，可以自製陽春版的密碼雲端儲存機制，把密碼紀錄檔案寄送到自己的雲端信箱（例如 Gmail）以隨時查詢，至少存取

前還有一層身分驗證的保護，且是免費並能 兼顧易用性。

結語 臺北捷運初期宣導搭乘手扶梯應「右側站立，左側通行」的政策，即使十年前就已經改為「緊握扶手，站穩踏階」，但人類的創造力可以無限，但記憶力卻是有限，密碼設定與其追求字符複雜度，不如擁抱字串長度。一般民眾養成的習慣已經改不過來。目前密碼複雜度要求已成為「顯學」，即使當初的作者坦承錯誤，但現實風向已經「回不去了」，用戶也必須自我學習，改變使用密碼的壞習慣。資訊安全與使用便利性常常是背道而馳的設計理念，系統開發人員必須找到一個平衡點，並依機密程度、業務影響層級及法規要求等面向評估系統安全等級，以訂出適切的密碼安全政策。

電化教育

社群網路與情資蒐集

近幾年恐怖分子活動頻繁，例如伊斯蘭國（IS）及蓋達組織（AI-Qaeda），其間的串聯與活動亦搭上了社群網路的發展，在其推波助瀾下，政府當局不得不投注心力想方設法遏止這股潮流。身為社群網路龍頭之一的臉書（Facebook），也宣示極力發展 AI（Artificial Intelligence）人工智慧技術以偵測恐怖分子於社群網路上散播之惡意訊息。在此背景之下，本文旨在介紹當前社群網路技術發展及情治機關情蒐方向可能之發展。 社群網路簡介社群網路興起於 2002 年初期，當時由於Web 2.0的發展，使得網頁應用程式不再隨著網路技術普及再加上無線通訊的發展，人手一機走到哪瀏覽到哪的現象隨處可見。當單純地瀏覽網頁已不能夠滿足一般使用者的需求，隨之而來的是提供使用者互動交流的社群網路應用服務，讓使用者無論身在何處皆可與親 朋好友分享生活周遭的一切。然而當原本立意良善的科技發展被惡意人士濫用時，所衍生的後果往往需要花費更多工夫加以補救。侷限於讓使用者單方面從伺服器端接收資訊，使用者開始可以與網頁產生更多的互動，甚至可以藉由網頁與其他使用者產生 連結，逐漸地建構了社群網路的雛形。所謂的社群網路其實就是現實生活中的人際關係及虛擬的網路世界兩者的互相投射與聯結。以現在全球最受歡迎的社群網路臉書為

例子，使用者可以透過臉書應用程式與朋友互動，傳送彼此間溝通的訊息、推薦喜歡的餐廳、評價某部電影的內容等。藉由這些互動，臉書可以將使用者與擁有共同興趣或喜好的第三人串聯在一起，逐步擴大自己的生活圈。這種自動推薦朋友的方式很容易將一群人連結成一個群組或社團，以往我們熟知的實體社團已被這種虛擬的社團所取代，當要號召同一社團內的成員集體行動時，不再需要為了聯絡方式而傷透腦筋，只須在網路上一個簡單的訊息傳遞便可以達到一呼百諾的情勢。2011 年初的茉莉花革命以及2014年在臺灣發生的太陽花學運都是藉由社群網路凝聚了龐大的人潮。然而原本立意良善的技術經由有心人士的利用，瞬間變成了犯罪者的溫床。恐怖分子便相中了這塊執法者公權力尚無法直接介入的祕境，開始進行了組織性的宣傳及招募新血，誓言將他們所宣稱的聖戰傳遞到世界上的每一個角落。透過網路的渲染，惡意的假消息及串連活動防不勝防。既然這是由於社群網路技術發展所致，當然也應該由社群網路技術本身來加以制衡，這也就是最近幾年社群網路大廠競相投入最重要的研究議題之一。社群網路語意分析語意分析是自然語言處理（Natural Language Processing）的應用之一。自然語言處理簡而言之就是教電腦可以自動識別人類使用的文字，應用的層面包含自動翻譯、文字校對、自動問答系統及語意分析等。語意分析除了讓電腦自動識別文字內容以外，還需要進一步理解文字背後所隱含的意義。例如：「科比．布萊恩全場投20中1，不愧是打鐵界的一哥」這句話看似稱讚，其實是在暗諷投籃命中率過低。語意分析便是能夠自動察覺使用者實際所要表達的意思。社群網路由於連結全球數以萬計的使用者，每天產出的資料量呈現爆炸性的發展。這些巨量資料裡頭或許隱藏著恐怖分子間溝通的暗語，或是不法分子意圖攻訐政府所散布的假新聞等，這些資訊對於執法機關而言都是相當珍貴且有 用的訊息。然而如同在砂礫中找尋珍珠般，這項工作無法單靠人力來完成，必須仰賴電腦的人工智慧來發掘不易發現的線索，隨之而來的技術就是社群網路語意分析。一套完整的社群網路語意分析系統包含下列4項步驟：資料蒐集、資料

整理、資料分析及資料呈現，如下圖所示。資料蒐集其實就是網路爬蟲，針對我們鎖定的目標，持續性地透過程式蒐集相關資料。現在熱門的社群網路，像是臉書及推特（Twitter），皆有推出相對應的應用程式介面（Application Programming Interface, API）方便研究人員擷取該網站上的資料，至於沒有提供API的社群網站，例如PTT（批踢踢實業坊），我們可以使用專為處理大量資料而開發的程式語言（Python或是R language）提供的套件輕鬆蒐集資料。以往繁複的資料蒐集工作並沒有隨著資料量指數型遞增而越發困難，相對地開發者則是擁有越來越多便捷的開發工具。資料整理則是在做資料清洗（Data Cleaning）。第一階段蒐集完資料後，並非所有資料都是有用的，必須汰除不需要以及冗餘的資料，並且將資料正規化以利下一階段資料分析。資料分析是關鍵所在，現在最受歡迎的技術是基於類神經網路（Neural Network）而發展出來的深度學習（Deep Learning）技術。拜 AlphaGo屢屢擊敗圍棋高手所賜，深度學習這個詞彙常見諸於新聞媒體上。身為資料探勘（Data Mining）中分類（Classification）技術的一種，深度學習並不限於下圍棋的應用上，而是可以廣泛地運用在任何需要依靠電腦自動判斷並分類的應用中。如前述文章中所提，語意分析是當電腦讀取一段文章後自動判斷出文章的屬性。舉例來說，我們想要做的分析是判斷某一段文章是否與恐怖攻擊有所關聯，所以當電腦讀了一段文章後，程式必須決定該段文章是屬於恐怖攻擊正相關屬性或者是低相關屬性，按照這種模式，我們可以把這個問題歸類成分類的應用，於是乎深度學習便躍於資料分析的舞臺上。資料呈現主要著重在資料視覺化呈現。當完成上述 3 個步驟之後，最後只差如何將結果具體且顯著地讓第三方知道。傳統報表式的數據雖然可以做到不失真，但是失去了吸引讀者以及達到一目瞭然的效果，於是乎以圖形取代冰冷冷的數字已經成為一種顯學。幸運地，資料視覺化相關的套件有如雨後春筍般一個接著一個推出，從最基本Excel所提供的製圖工具到專為資料科學而生的程式語言（Python 或 R Language），甚至是網頁程式的D3.js（DataDriven Document

JavaScript package） 都可以輕鬆地輸出專業且美觀的視覺資料。

結語 隨著犯罪智慧化，網路已經成為犯罪的重要媒介之一，因此網路情蒐也是接下來重要的犯罪預防手段，若能早期發現可疑的犯罪行為，執法機關才得以籌劃對策，防範於未然。社群網路的蓬勃發展已是不可擋的趨勢，當然它提高了犯罪的隱蔽性，但同時也提供了執法者發掘案源的全新管道，若是能夠善用社群網路情蒐這個工具，原本看似危機的新科技，換個角度，卻是嶄新的轉機。

廉政署檢舉專線：「0800-286-586」(0800-你爆料-我爆料)。

法務部矯正署綠島監獄廉政專線：089-672297

E-mail：gipn@mail.moj.gov.tw