

國軍 111 年 7 月份保防教育專文

「建立安全共識，防敵滲透蒐情」

壹、前言：

國軍教戰總則第一條即明確揭示國軍有維護領土、主權及肩負保國衛民的重要使命，這不僅僅是種驕傲，同時也是責任的承擔，尤以中共日益猖獗的機艦擾臺行為，更顯示其從未放棄以武力解決臺海問題的企圖，而為創造軍事行動的優勢，更不斷透過各式滲透管道，竊取我國重要軍事機密與發展組織，對我國國家安全影響甚鉅，國軍是國家安全的保護者，應對當前的安全威脅具備基本的認知與素養，才能洞悉中共蒐情、滲透及發展組織的企圖與手段，進而建立安全共識，強化保防作為，確保我國家安全。

貳、敵情威脅與挑戰：

一、當前反情報工作挑戰：

隨著中共經濟與軍事實力的增長，加速其在國際間的影響力，意欲打破現今國際局勢與平衡，並運用諸般手段對世界主要國家採取多層次、多管道及多面向的滲透，例如各國大學「孔子學院」的設立，藉學習中文之名干涉該國教育、政治等行為，各國情報組織均不約而同提出警訊，其諜報活躍程度已超越冷戰時期，尤其是軍事情報、關鍵科技技術或重大商業機密等均為蒐報重點，而網際網路的普及更使得中共的「紅色滲透」更加氾濫、難以防範，透過滲透社會各界人士，操控網路言論、影響國內輿情，企圖擴大「隱蔽戰線」鬥爭，運用諸般

手段滲透我政府、民意機關、社會及國軍內部，為「不放棄武力犯臺的企圖」及「不打沒有內應的仗」積極作準備，因此全體官兵都應深刻認知「敵人就在你身邊」不是句口號，而是會真實發生在你我周遭，時時提高警覺，為國家安全盡一分心力。

二、中共多層次、多管道及全方位的滲透佈建原則

近年因政治及疫情因素，兩岸交流趨於平緩，但共諜的觸手仍未停止，不斷探詢我軍事機密；就近年本部與國安單位共同偵破與國軍有關之共諜案件，發現其對我滲透手法逐漸由竊取機密轉變為發展組織，對象由高階幹部轉向基層官兵，不分軍種及階級，甚至拓及親友及師長，採取廣泛性、全面性及多管道方式，伺機物吸發展組織或運用網路社群軟體隨機撒網吸收，國軍人員務必當心留意。

三、鎖定現役官兵、軍眷、退伍軍人或專家學者為接觸對象

舉凡赴陸投資之臺商、退役人員及軍眷，均為中共蒐情物選對象，其吸收方式以先期接觸，瞭解政治傾向、思想品德、家庭狀況、經濟需求、個人經歷等，伺機投其所好或掌握其弱點，運用統戰爭取、金錢利誘或威脅恫嚇方式吸收，以編織情報網絡，再伺機返臺接觸國軍現役人員。其接觸滲透方式，不外乎運用袍澤情誼、眷屬親情、舊識引介等方式，消除現役人員戒心，迂迴接近或建立個人私誼關係，最後遂行其統戰、發展組織及伺機蒐情的工作目標；另透過金錢收買、提供優惠條件或

色誘等方式，說服接觸對象提供單位一般性資料後，待掌握證據或合作成為既定事實後，再續以脅迫手段，要求為其蒐報我機敏內部資料，致使少數官兵因無法覺察背後危機而深陷其中，一錯再錯無法自拔。

參、案例檢討與態樣分析：

國軍人員來自社會不同家庭與各個階層，容易遭到社會氛圍影響而沾染惡習，從本部破獲共諜案件研析中共滲透態樣（如附表 1），金錢利誘、把柄要脅、弱點突破，向為中共情報部門慣用伎倆，而易遭中共情工人員吸收風險人員，不外乎有「涉陸背景」、「財務失衡」、「保密違規」、「不當行止」及「出國異常」等特徵，其手段不外乎抓把柄、撒大錢、用美色、提供商機、協處債務及設陷脅迫等項，相關案例及研析如后：

一、迂迴接觸現役官兵，情誼枷鎖誘吸蒐情

審視近年涉犯國安案件人員，多數利用親屬、師生、部屬、舊識等情誼關係，採迂迴路線拉攏現役人員，進而建立不法蒐情網絡，例如「共諜鎮○○來臺發展組織」及「退役上校○教官為敵蒐情及發展組織」等案例，遭渠等接觸人員，基於情誼與信任，初始均無防備之心，單純以為僅只是參加舊識餐敘，嗣後均遭誘騙赴境外與中共官員會晤，或因不察而提供單位資訊，甚至受金錢利誘或債務壓力，主動販售機密資料，逐步深陷而遭人吸收運用，鑑此，國軍人員應當提高警覺，絕無白吃的午餐或是不勞而獲的財富，方能防範敵人蒐情陷阱。

二、拓展接觸運用層級，突破機密資訊管控

中共滲透發展對象多鎖定國軍中、高階幹部或者是接觸機密人員，因為擔任機敏要職，不僅經手且容易獲悉各類機敏資訊；然而近期破獲○軍中士販售機密資料或退役士兵蒐情等案例，渠等雖位階較低，僅能接觸基層部隊資料，仍遭物吸利誘；另外近年中共新興蒐情手法，主動提供官兵手機以躲避稽查、夾帶入營方式，要求伺機翻攝公務電腦螢幕等機密資訊，藉以規避國軍「移動式儲存媒體(USB)管控系統」及「印表稽核系統(浮水印)」之嚴格檔案輸出及文件列印管控措施，顯示中共手法創新多元，不斷尋找國軍安全罅隙，國軍人員必須謹守本分、遵守保密規定，使敵無可乘之機。

三、網路社群隨機接觸，虛擬分身物吸利誘

近年受疫情影響，傳統人員情報作為不易，中共情工復以網路具隱匿及溯源不易等特性，鎖定臉書個人公開資訊，蒐集自述為現役軍人或就讀軍事院校等對象，再以假冒高薪招聘智庫顧問、求職網專員或提供資金融貸等身分，與國軍人員接觸，初期騙稱僅須提供部隊一般資料即可獲取高額獎金等手段，利誘官兵蒐情，例如○下士因個人財務失衡上網搜尋借貸訊息，遭到不明人士接觸，遂以單位機密資訊換取報酬，遭國安單位偵掘查獲，移法偵辦。爰此，提醒國軍人員應具備正確的理財觀念，切莫貪圖不當利益，且網路社交活動，應提高安全警覺，倘遭中共情工接觸時應斷然拒絕，切記網路活

動凡走過必留痕跡，勿因貪圖小利而觸法。

四、統戰宣傳情戰造勢，北平模式發展組織：

中共對臺的滲透統戰作為，觸角越來越廣，執行模式愈趨細膩，不僅藉由兩岸交流名義物吸對象，並企圖複製1949年「北平模式」，以「政治滲透、干預及顛覆模式」，運用少數不肖份子蟄伏於各階層，在國內發展潛伏的內應力量，或滲透國軍內部，期在關鍵時刻發揮裡應外合、以戰逼降及消極不抵抗的滲透目的，例如○姓民眾遭中共情報人員吸收返臺發展組織及退役○姓中校遭中共情報人員吸收返臺接觸現役人員等案，其態樣均以餽贈金錢、禮品及招待旅遊等誘因，要求渠等引介現役軍人至第三地會晤，要求協助發展共諜組織，或仿「北平模式」表態支持統一，並稱現階段暫不賦予刺密蒐情任務，若中共武力犯臺時，採消極不抵抗作為，期在重要時刻發揮關鍵作用。

肆、應有認知與作為：

中共對國軍的情報滲透模式，多以合法管道掩護非法活動、以迂迴途徑滲透目標對象、人海戰術刺蒐機密資訊、金錢美色收買個別情報、公開資訊獲取密情、資通科技偵蒐軍事情報、網軍侵入竊取各類情報及運用社群網站接觸物吸對象等，利用極少數的不肖人員「拉出」加以運用，進而接觸敵人機密，大幅縮短情報工作周期，從美國、日本等軍事大國陸續破獲共諜竊密案，以及我國國安局、法務部陸續偵破多起共諜案，更加印證中共近年加大力度遂

行「紅色滲透」，戮力投入這場沒有煙硝的戰爭，面對這樣威脅我們應當有下列的認知與作為：

一、體認軍事倫理，信守忠誠義務

軍人的責任在保國衛民，必須具備高尚的精神氣節，以及發揮智、信、仁、勇、嚴的軍人武德，才能在面臨犧牲生命危難之際，依然秉持著誓死達成任務與成功成仁的信念。各位回想從軍報國得初衷「余敬謹宣誓，效忠中華民國，保衛國家人民，恪遵軍中法令，服從長官命令，盡忠職責，嚴守祕密，如違誓言，願受嚴厲之處分。此誓…」的誓詞仍在耳邊迴盪，這是每位軍人入營服役都要宣誓的誓詞，同時也揭櫫軍人「忠誠」、「守密」的義務，而我國憲法第 138 條明定：全國陸海空軍，須超出個人、地域及黨派關係以外，效忠國家，愛護人民。更明確的指出國軍軍事倫理最核心的一部份，不僅是全體國民託負的使命，也是軍人必須全心全意奉行的圭臬。因此，全體官兵應養成嚴謹的生活態度、端正的品德操守，將效忠國家之核心價值，根植心中，方能確保國家安全。

二、踐履反情報責任，鼓勵反映違常

國軍反情報責任制度的基本要求是「個個參與，人人有責」，從個人做起、從單位做起，構成綿密強固的安全網絡，每一位官兵不論其階級高低或職務輕重，都不能將部隊安全工作置身事外，面對中共各層面的滲透蒐情，全體官兵均應當建立正確認知，踐履「反情報責任

制度」。從近年破獲共諜案例統計，多由官兵主動檢舉偵破，足見保防教育成效日益彰顯，然而我們不能以此自滿，因為敵人的滲透蒐情手段日新月異，並且涵蓋社會各個層面，「保密防諜，人人有責」絕不能只是口號，必須全體官兵共同配合及身體力行，落實「見可疑追查到底、遇問題立即反映」的基本要求，發掘潛存危安因素，踴躍檢舉反映違常，才能達到「掌握機先、弭患未萌」，瓦解敵人陰謀滲透破壞伎倆；另為鼓勵自首或自清表白及勇於檢舉反映違常，凡主動舉發敵諜線索因而破案者，本部將秉「從優給獎」、「即時獎勵」原則辦理議獎，最高獎金可達新臺幣 500 萬元，針對曾遭敵接觸而知情不報者，追究責任從嚴議處，以阻斷中共陰謀滲透。

三、建立法治觀念，避免誤蹈法網

鑑於「退役○上校涉發展組織案」、「共諜鎮○○吸收退役軍官案」等多名退役軍官遭中共物吸，利用過去人脈在臺發展組織及刺蒐軍事機密等同「叛國行為」，惟犯罪時法律量刑過輕，為社會大眾所質疑，爰此，民國 108 年立法院已通過相關國安法令修訂，完善犯罪態樣的規範及大幅提高違犯國安案件罪責，凡為敵利用蒐情，最重可處無期徒刑，以遏止境外勢力滲透破壞（如附表 2）；另本部殷鑑中共透由各管道接觸現、退役人員及眷屬發展組織，因此於 110 年 10 月 7 日修頒「國軍正義專案作業實施規定」，明確律定國軍人員主動反

映、檢舉違常之反情報基本要求，凡與大陸地區人民及香港、澳門地區居民接觸應事先報備，並嚴禁於營內接觸聯繫，同時訂有行政懲罰基準。因此，全體官兵不論現（退）役均應明確體認，遇有不明人士接觸應立即回報，更切記莫為敵蒐情及加入共諜組織，免得觸及法網，身限囹圄。

四、恪遵資安規定，培養保密素養

美方調查近年的駭客行為近 9 成來自大陸，涉及竊取數十億美元的智慧財產及駭入美國軍方合作的多所大學研究實驗室、武器裝備系統承包商，意圖盜竊先進科技的行為；另英國、德國、加拿大、日本、瑞典、澳大利亞與荷蘭等國，均曾指控中共竊取網路資訊。由此可知，中共憑藉經濟發展優勢不斷擴張網路戰力，企圖突破歐、美、日等主要國家資訊安全防護網，以達戰略企圖。因此全體官兵應認知「保密是軍人的天職」，更是軍人的基本素養，尤以智慧智慧型手機已成為現代人不可或缺的重要資訊工具，於營內使用更應確遵相關規範，除不得透由任何方式，將業務上所知悉之公務（機密）資訊向無關人員透漏外，更不得於手機儲存、編輯公務資料，以確保公務資訊不因個人疏失或惡意軟體入侵而外洩，進而肇生危害國家安全之情事；另確實安裝「國軍智慧型手機自動化管理系統 MDM」，關閉定位、照相與藍芽傳輸等功能，於營內應確實上鎖，並配合軟體定期更新，確保「MDM」功能運作正常。且針對營區

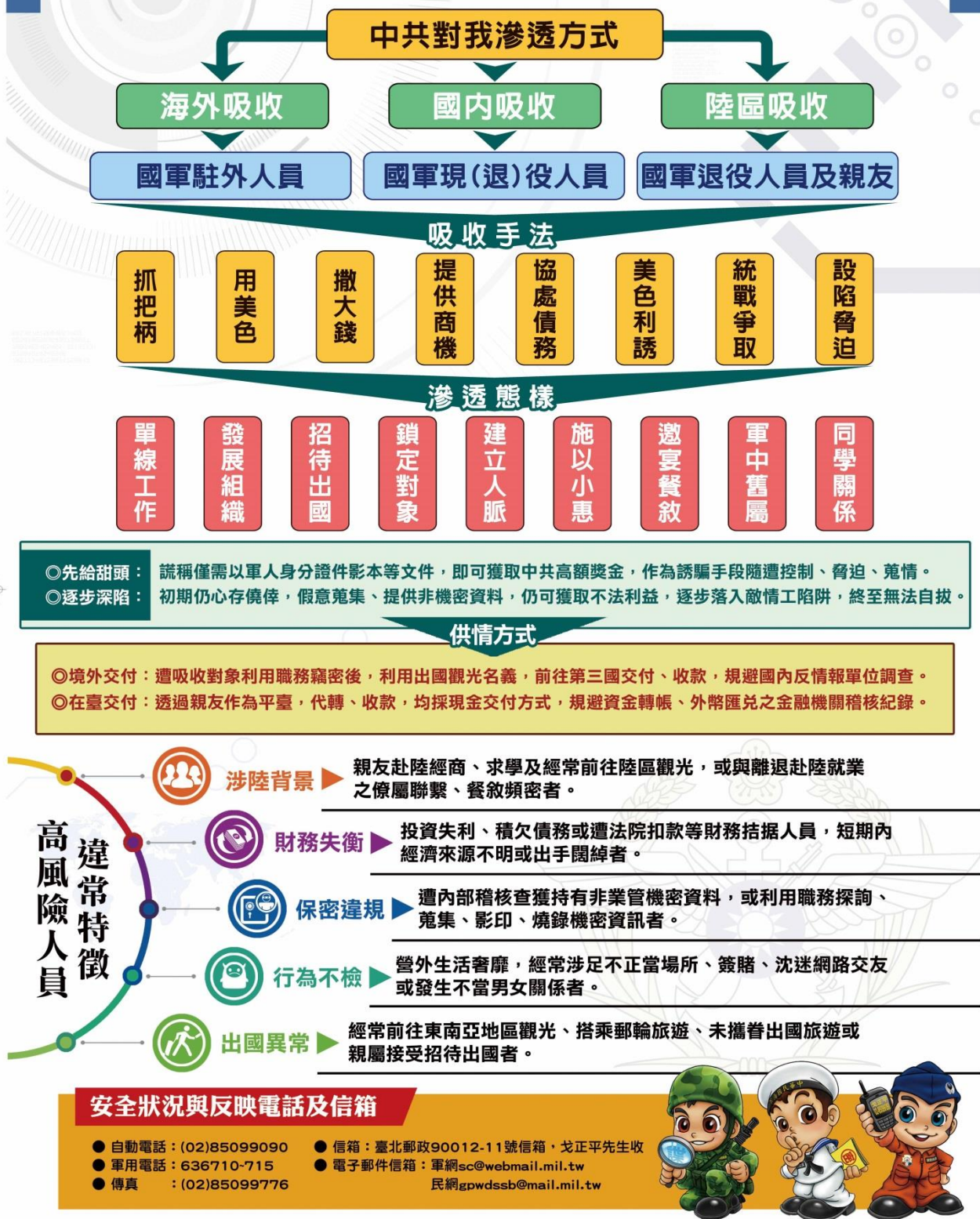
內機敏性場所、各項演習及重要會議會場，嚴禁管制智慧型手機使用，以落實資安管制，避免個人淪為國軍保密工作的破口，以確保整體國防安全。

伍、結語：

隨著臺海兩岸受國際政治環境與疫情影響，中共仍持續透過數位傳播與網路的發展趨勢，對臺遂行刺密蒐情策略，未來國軍安全工作環境將日趨複雜與嚴峻，全體官兵均應具備正確認知，並保持個人良好品德操守及建立正確理財觀念，勿使敵人有可趁之機，同時，踐履「國軍反情報責任制度」，主動檢舉不法與違常，發揮「見可疑追查到底」、「遇問題立即反映」的精神；另外，要提醒周遭親友、眷屬，遇有大陸人士主動接觸，招待餐敘或出國旅遊，一定要提高警覺，才不會陷入敵人所設的陷阱，若遇到類況，立即向國軍保防部門檢舉反映，以維護國家安全。

附表 1

國軍人員遭中共情報部門吸收運用案例態樣分析



中華民國國防部政治作戰局保防安全處 / 提醒你

如附表 2

歷年破獲共諜案件常用法條

刑法§109-112	意圖或實際刺探、收集、洩漏、交付國防應秘密之資料。	最重處10年以下有期徒刑
陸海空軍刑法 § 17-22	為敵從事間諜活動、刺探、收集、洩漏或交付國防應秘密之文書等物品。	最重處死刑或無期徒刑
國家安全法§5 ID: 8996170A	為大陸地區發展組織。 ID: 蔡爾藏 GPB02315000094 ID: 8996170A	最重處7年以上有期徒刑，得併科罰金1億元
國家情報工作法§5	違法洩漏、交付情報來源及有關情報人員、協助者等資訊。	最重處7年以上有期徒刑，得併科罰金1億元
國家機密保護法§5	洩漏、交付情報來源及有關情報人員、協助者等資訊給外國、大陸地區等境外勢力。	最重處10年以下有期徒刑
貪汙治罪條例§5	職務上要求或收受賄絡。	最重處7年以上有期徒刑，得併科罰金6千萬元