破解營建工程材料檢驗作弊伎倆

監督者用心，破解不法承包商作弊伎倆並非難事。

◎ 楊秉蒼

為求生存、增加獲利，不法承包商面對工程推動過程，其思考如何作弊的時間，會比花在工程品質確保的時間來的多。所謂道高一尺、魔高一丈，足以說明不法承包商的能耐。雖然這些不法承包商有其作弊伎倆，然只要「了解檢驗要求的重點」，要破解不法承包商作弊伎倆並非難事，「最怕監督者無心」，才使得不法承包商有機可乘。由於營建工程材料屬性差異，所以檢驗項目也會有所不同，當然檢驗需求也有異，作弊伎倆也有所不同。下列依營建工程常見之工程檢驗項目，依取樣、送驗及檢驗的角度，說明不法承包商可能作弊的伎倆。

由下列論述不難理解，承包商作弊的行為模式，依序為「取樣過程著重於取得監造信任、送驗過程著重於欺瞞監造、檢驗過程著重於收買（或恐嚇）實驗室」。若以整體流程觀視，承包商作弊除其有心外，大多為監造監督不周或在同流合污下，使承包商有機可乘；此外，實驗室的職業道德與操守，亦應特別重視，不要忘記自己是扮演公正第三人的角色。

鋼筋混凝土材料檢驗作弊伎倆

一、混凝土圓柱試體抗壓強度檢驗之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，選擇事先計畫好的特製（提高混凝土強度）混凝土預拌車，其餘預拌車強度可能有問題。
2. 送驗：欺瞞監造將試體偷走，或偷換試體模仿簽字。
3. 檢驗：欺騙實驗室送樣錯誤，或進入實驗室偷換試體，或勾結實驗室調整儀器抗壓速率、烘乾試體抗壓或修改報告數據等。

二、混凝土鑽心試體抗壓強度檢驗之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，選擇事先計畫好的鑽心取樣位置，以確保有足夠混凝土抗壓強度。
2. 送驗：假借名義使試體離開監造視線（例如檢查或清洗試體等）偷換試體，或於送驗過程於車廂暗藏其他試體掉包。
3. 檢驗：欺騙實驗室送樣錯誤，或進入實驗室偷換試體，或勾結實驗室調整儀器抗壓速率、烘乾試體抗壓或修改報告數據等。

三、鋼筋混凝土用鋼筋檢驗之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，檢送合格標準品（輻射合格、單位重高、降伏強度符合規範、抗拉強度大及彎曲無裂紋），或使監造在無任何選擇空間，選用預先準備的合格品（加工料最常見）。
2. 送驗：欺瞞監造將試體偷走，或假借名義使樣品離開監造視線偷換樣品，或於送驗過程於車廂暗藏其他樣品掉包。
3. 檢驗：欺騙實驗室送樣錯誤，或進入實驗室偷換樣品，或勾結實驗室或修改報告數據等。

瀝青混凝土材料檢驗作弊伎倆

一、瀝青之混凝土瀝青含量檢驗、混凝土篩分析檢驗、混凝土試體容積比重檢驗、黏度檢驗等之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，事先於工廠拌製合格樣品（油量高、黏度低、級配合格，且粒料比重輕的骨材），隨車送至工地，假裝取樣，並取出預埋的合格樣品送驗。
2. 送驗：假借名義使樣品離開監造視線偷換樣品，或於送驗過程於車廂暗藏其他樣品掉包；若發現送樣時，樣品溫度變爲常溫應特別注意（取樣時，樣品溫度應高於 120˚C 以上）。
3. 檢驗：欺騙實驗室送樣錯誤，或進入實驗室偷換樣品，或勾結實驗室修改報告數據等。

二、瀝青之混凝土試體厚度檢驗、混凝土試體壓實度檢驗等之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，預先於取樣位置挖深，使鋪設厚度足夠，並將特別拌製之熱拌瀝青混合料（加入金屬物增加重量，例如鉛塊、礦砂、轉爐石或高爐石等）局部性鋪設於取樣位置附近，並做上記號；待取樣時，依地上標記（例如紅磚或噴漆）取樣。
2. 送驗：假借名義使試體離開監造視線（例如檢查或清洗試體等理由）偷換試體，或於送驗過程於車廂暗藏其他試體掉包。
3. 檢驗：欺騙實驗室送樣錯誤，或進入實驗室偷換試體，或勾結實驗室修改報告數據等。

土壤與級配材料檢驗作弊伎倆

一、土壤阿太堡限度檢驗、粒料篩分析檢驗、土壤及級配室內夯實檢驗等之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，製作一批合格土壤或級配試樣（無黏性級配、級配合格，且粒料比重輕的骨材）提供送驗，或於工地堆置一小堆合格樣品提供取樣用，以矇騙監造。
2. 送驗：假借名義使樣品離開監造視線偷換樣品，或於送驗過程於車廂暗藏其他樣品掉包。
3. 檢驗：欺騙實驗室送樣錯誤，或進入實驗室偷換樣品，或勾結實驗室修改報告數據等。

二、土壤及級配工地密度檢驗之作弊手法，包括：

1. 取樣：在監造不堅持取樣方式下，預先於取樣位置埋置特製級配（加入 3/4”以下粒料，或加入金屬物增加重量，例如：礦砂、轉爐石、高爐石等，或挖掘過程將試驗洞外之粒料丟入袋中）。
2. 送驗：假借名義使樣品離開監造視線，打開試驗土堆袋子丟入粒料或土壤，以增加重量。
3. 檢驗：進入實驗室假借關心名義將粒料或土壤丟入未烘乾秤重之土樣內，藉以增加重量（丟太多會出現乾土樣比濕土樣重的現象，使實驗結果出現異常），或勾結實驗室修改報告數據等。

（作者現任正修科技大學土木與工程資訊系助理教授）

（本篇摘錄自法務部調查局清流月刊 97 年 1 月號）

從端點安全談政府機關資料治理

要確保安全，把網路資源一視同仁地通通鎖起來是不對的，正確的方式是細心地關注誰有權力看到什麼資料。

◎ 吳文進

一、前言

端點安全(Endpoint Security)已成爲近兩年資安領域的熱門話題。所謂端點是指連接 s1f 網路的各項接取設備，包括電腦、PDA 及隨身儲存裝置等。此議題受到關注的原因其來有自，因爲不論是企業組織或政府部門的資安或網管人員，花費多少力氣來建構單位安全防護網，但總有隨身碟、筆記型電腦或無線網路接取設備這類的漏網之魚，將蠕蟲、病毒、木馬，甚或間諜程式帶進組織網路，或將機密資料帶離內部網路，以致衍生洩密事件。而這些機密資訊外洩事件除見諸媒傳披載之外，實際上的損害程度恐非一般人所能想像。究析事件肇生原因，絕大多數是機構內部人員輕忽或認知不足所引發，畢竟現有的資安防護機制與措施，均針對外人而設，而內部成員通常擁有較高的權限，也熟悉機密資訊存放路徑與取得方法，更懂得如何避開現有的偵監機制，因此所造成的損害也特別的大。雖然機密資訊外洩可依相關法令規範檢討究責，但已使整體國家安全受到威脅；而一般企業的商業機密外洩後，可能危及企業的永續經營。

防制資料外洩固然重要，但目前卻無有效的、合適的與全面性的方案。雖然陸續有資安廠商推出 DLP(Data Lost Protection)、ILR(Information Leak revention)等針對資料外洩防護的解決方法，這類技術無非是透過數位版權管理(DRM)、內容過濾、身分識別及權限控管等機制來加以實現，離全面防堵組織核心機密資訊外洩，仍有不少可努力及精進的空間。本文試著以端點安全爲核心，以深度防禦的觀念重新思考，試著由各個面向著手，同時也明確地了解威脅來源及管道，除將防禦點擴大爲線，乃至於面之外，實務上必須具備「深度防禦」的精神。因此本文深入分析威脅現況、資料外洩成因、威脅管理及資料治理等，期藉了解風險、管理風險，進而轉移至減緩風險，以確保機密資訊安全無虞。

二、安全威脅現況分析

依據趨勢科技公司在資安人雜誌 96 年 8 月 14 日所舉辦「全方位防制資料外洩研討會」中提供的數據分析，當前惡意程式類型以間諜(木馬)程式及感染可執行檔的病毒(PE)比例最高，各佔 31%，其次是 HTML 及蠕蟲的感染，各佔 11%。透過惡意程式的分析，可發現以下隱含的意義，包括：

1. 間諜程式主要以竊取機敏資料爲主。
2. 感染可執行檔將增加解毒的複雜度。
3. 感染管道以 HTTP 及系統弱點爲主。

另就惡意程式植入的目標分析，絕大多數都在用戶端發現，這些包括行動用戶常用之筆記型電腦、PDA，以及可攜式儲存媒體等，因此端點安全將成爲現階段資安防護的最後一道防線。另分析前 10 大惡意程式，可以發現：

1. 40%的病毒會自我加密或採用特殊程式加殼。
2. 平均病毒檔案大小爲 71Kbytes。
3. 90%的病毒以 HTTP 爲傳播途徑。
4. 60%的病毒以郵件傳輸協定(SMTP)爲傳播途徑。
5. 皆與病毒自動下載器(downloader)行爲有關。
6. 50%的病毒會利用開機自動執行或自動連上惡意程式網站。
7. 皆會產生其他病毒檔案。
8. 通常會造成使用者應用程式或系統運作不正常、郵件伺服器繁忙或網路流量增加。

三、如何檢視端點安全

內部人員在不知情或不小心的情況下洩漏機密資訊，將對單位造成嚴重的傷害與威脅，然而許多企業組織可能低估了這項風險。資料外洩不僅造成金錢的損失，對商譽更可能產生無法逆轉的永久傷害。根據美國密勤局與卡耐基大學軟體工程學院在 2005 年針對「關鍵基礎設施內部資安事件」的研究中發現，超過 81%的內部資安事件會導致財務上的損失；另 28%參與研究的單位表示，企業的形象與商譽將因而受損。隨著電腦網路環境日益複雜化，企業內網路逐年擴增，相對地產生防護漏洞的數量亦隨之成長，更加深內部威脅的嚴重性。往常以企業網路邊界爲主的資安防禦措施，已被應用程式、行動辦公者、商業伙伴及客戶間編織成錯綜複雜的網路環境所淹沒。根據著名的科技產業情報分析與諮詢顧問公司 IDC 近期的研究報告指出，預估 2009 年全球行動工作者將超過 8 億 5,000 萬，總數將達全球工作人口的四分之一。因此遠距的行動工作者將成爲企業組織網路未來最大的隱憂，而這股無法抵擋的趨勢亦凸顯端點安全的重要性。

反觀現行網路基礎建設的防護設備與機制，僅能提供片面的資安訊息，以致無法在關鍵時刻提供精準的資訊，易坐失解決問題的黃金時機。而資訊專業人員多數僅著眼於科技的技術層次，但隨著複雜度的增加，企業所面臨的風險也相對提高。爲解決端點安全的問題，美國資安顧問 David Strom 在 2007 年 5 月間曾提出四項指標，可做爲資安人員參考之依據：

1. 現有安全基礎建設有哪些？

根據目前所擁有的設備，了解可能的安全組合及防衛模式，找出可能的問題點，輔以入侵偵測、防火牆系統或 VPN 閘道器等機制來補強端點安全。

2. 所欲保護之標的爲何？

其次是清楚了解所欲保護之標的後，據以決定如何部署這些防護設備，如某些設備應該直接置於防火牆之後，以便涵蓋整個網路；有些則最好置於交換器之後、伺服器之前，或是部署在主要保護的子網路或部門網路上，並經過認證，以確保這些網路資源都受到保護。

3. 使用者對安全政策的接受度？

利用弱點掃描設備對組織內部端點進行掃描是了解安全強度最好的方法之一，因爲它可以根據安全強度提供端點的修正以及網路資源的保護。這些檢測工具主要檢查開放的通訊埠、執行的服務、在檔案系統上查看是否有問題的檔案與惡意軟體、監控系統登錄、確定防毒軟體病毒碼的更新，以及檢查個人防火牆是否開啓或被竄改等。有些組織甚至安裝代理人程式（agent）來監控端點的安全狀況，通常這些軟體會讓使用者在登入時多花上數分鐘，因而感到不便。若沒有適切地宣導並輔以權限管控與稽核，則政策將無法落實，畢竟政策及程式運用是固定的模式，如果使用者找到規避稽核的巧門，則安全風險仍然存在。

4. 非 PC 的端點管理現況？

要落實端點安全，首先應知道網路上有什麼？及要管理什麼？因爲組織網路上的印表伺服器、筆記型電腦或 PDA 等，都有獨自的作業系統與 IP 位址，它們無法輕易地被端點設備所控制。而幾乎所有的應用程式爲達可用性，均提供對網卡編號或 IP 位址做白名單或前置驗證，因此設備還是可以連上網路並進行工作。而這些移動式設備極易感染惡意程式，除非有能力偵測這些設備並實行政策，否則威脅將隨著這些設備而爆發。例如我們可以利用政策限制設定網路印表機的封包只能用作印表之用，如果有人假冒印表機的 IP 位址，防護系統應仍能偵測出改變，並將設備隔離及斷線，以確保它們不會帶來威脅。尤當企業有異質網路、設備或作業系統太廣泛時，想要找出完美的端點安全方案是非常不容易。

四、端點安全與威脅管理

端網路連線日趨密集，網際空間威脅的擴散程度也隨之升高，其範圍與規模就如同駭客、電腦詐騙者、病毒與蠕蟲撰寫者，以及間諜程式、廣告軟體、垃圾郵件之發佈者一般擁有豐富的想像力，以致無邊無際。不幸的是，隨著網路轉變所帶來包括存取、資訊共享、匯集、整合與即時分享等優勢，即使是犯罪者、恐怖分子或其他心懷不軌者也都能使用，並未有所限制。如果不加以預防及管理，可想見這些威脅必會癱瘓 21 世紀的網路活動。而我們必須在這之前加以遏止，即使無法澈底制止滲透網路的威脅，仍要設法進行預防管理。所謂預防管理是利用整合式的方法來管理威脅，著眼於「遠端存取」與「端點安全」的結合；置重點於瀏覽器安全、主機完整性、惡意軟體偵測和資訊控管。瀏覽器是當前網路運用的主要存取方式，確保遠端存取期間的瀏覽器安全相當重要。瀏覽器可能儲存的資訊，包括快取與自動完成的記錄資料，以及離線瀏覽的暫存檔等等。例如，瀏覽器的快取必須在每個連線期間都進行加密，並且在連線結束後清除；主機完整性的檢驗應先掌控遠端設備自身的安全性，例如針對遠端設備是否有基本的防毒措施、客戶端防火牆與特定軟體版本的更新狀態等進行檢查，以避免不安全的遠端設備經由遠端連線後，危害到整個企業網路；而惡意軟體的偵測在確保所傳輸的資料，無法被潛藏的鍵盤側錄攻擊或畫面擷取程式所竊取，即使它們在進行連線前便已存在終端設備中。最後則是資訊控管，企業資訊一旦經由遠端存取到行動工作者的電腦中，無論是不經意的洩露或遭竊取，都將對企業造成損害，因此企業對外提供遠端存取時，必須適切運用加密機制有效控管，並能限制轉存檔案、複製至剪貼簿、列印，甚至連螢幕拷貝都要能控管，才能確保企業資訊的安全。

整合式的安全方法讓威脅管理與企業得以密切配合，有助於預先掌握安全威脅及採取補救措施，進而在安全事件影響組織前加以阻止。就實況而言，如只導入更多的安全設施，非但不能產生多大的效益，反而會增加管理的負擔，甚而降低效益。因此最佳的解決之道在於良好的管理，而非更多的產品。所以嘗試透過大量但不完整的個別解決方案來處理資安威脅，只是讓問題更形複雜且需高額的費用來排除彼此衝突、備援及協同性不佳等問題。個別解決方案的根本問題在於其只能滿足總體安全管理所面臨挑戰的一小部分，因爲以任何方式與「外界」(即個人電腦外部世界)交互作用的任何活動，幾乎都有可能使個人電腦遭受感染。有效的整合式威脅管理核心，是要了解企業的關鍵業務問題，以及在業務實踐的過程中，運用關鍵資訊科技的安全管理能力，解決當前安全的挑戰，又能滿足未來的需求，從而降低風險、降低成本，達到保護資產及提供持續性服務，並能符合法令規範之效益。

五、資料治理

資料治理觀念乃是企業內部對於所有營運資料的可用性、使用率、完整性與安全性的整合性管理機制，透過人員(People)、過程(Processes/Procedures)與安控產品(Products)等 3P 之資源投入，有效達到預期的目標與效益，包括：增加「經營決策」時的「一致性」與「信心度」、降低可能違反「資料法規」的損失風險、改善「資料安全」、最佳化與最大化資料所可能延伸的企業收入效益。

然而企業資訊主管如何獲知與了解單位內的資料治理品質與成效呢？首先需要清楚了解企業內部目前的營運資料真正存取管道與使用狀況，透過正確、有效、無副作用的「資料庫安控稽核方案」，將讓資安長、資安官、稽核人員從過去概念性的假設想法，如釋重負地眼睛一亮，清楚透視出企業資訊金庫的使用率、完整性、安全性，解決下列在資料治理上的安控痛楚，究竟是「誰」透過「哪種方式」將「交易資料抽單、新增 DB 特殊權限使用者、修改成本資料、刪除客戶資料」？能否自動察覺與阻斷「單次查詢超過合法權限資料筆數(例如：SQL Injection)」的狀況發生？如何確保「資料庫特權使用者」，都按照單位與企業的授權範圍正常運作？如何「快速、正確、完整、自動」產出符合 ISO27001、新巴塞爾、個資法、沙賓等相關資安法規中最重要的「機敏資料存取行爲稽核報表」？資料安全是不可忽視的營運問題。「本公司並無太大的風險」，這是我最常聽到管理階層講的一句話，其實他是說「我們無法修補我們不知道的弱點」、「我們不知道那些完全不懂的領域」。不管內部員工是惡意地或不經意地犯錯，你要管理的是存放公司大量機敏資料的網路，是不容許被入侵的。公司的營業交易秘密、財務報告、員工資料與客戶資訊，一旦遭竊就別想全身而退。雖然嚴重的安全意外總是出乎意料之外地出現，而且多數企業是承受不起一滴點的資訊外洩，但是要記住，科技是無法自動幫你解決所有問題的。面對內部威脅，保護公司資產的過程絕對不輕鬆，必須要尋求管理階層買單，透過高層宣示網路用戶的責任以及可歸責性，取得老闆的支援，大力鼓吹安全政策，才是有效與員工溝通的不二法門。我們必須不斷地提醒員工要照章辦事，因爲以科技過濾資訊內容雖可以達到許多目的，卻不是資料保護措施的終點站。然而，只要能夠合理地應用這些科技，至少它能提供強而有力的監控功能，以確保組織內部的重要資訊不會從網路上溢出。

六、結論

保障企業機密資訊是資安議題的最終目標。爲確保安全，把網路資源一視同仁地統統鎖起來是不對的，正確的方式是細心地關注誰有權力看到什麼資料。當企業組織或政府部門逐漸體認到，企業核心價值與公司核心系統內的資訊密不可分時，惟有透過控制——監視從終端下載資訊的方式、屏障——免於被儲存在可攜式或抽取式儲存裝置的不當程式利用來複製到終端上、保護——使您的網路不因無線、藍芽或其他介面而暴露於外界，才能有效免除機密資訊遭盜竊和誤用的危險。誠如資安大師 Bruce Schneier 所言，我們的社會對技術有種崇拜，技術可以解決很多問題，在電腦領域有很多也的確是如此，但是，基本上安全是一個由人產生的問題，所以技術只是很小的一部分，如果安全能隨著組織不斷發展，並能把「安全視爲一種激勵」，和經濟刺激綁在一塊，使安全成爲一種習慣，那這種經濟刺激最終會使電腦網路越來越安全。雖然電腦的安全問題不可能被完全解決，因爲它包含了人的因素，而安全也一直都是一種攻防對抗，惟合理的政策、適切的風險管控，再加以一點刺激，才能在這場對抗中勝出。

（作者任職於國防醫學院）

（本篇摘錄自法務部調查局清流月刊 97 年 3、4 月號）

試論危機預防與保防工作

危機預防乃保防工作的核心，有了充分的準備，才能從容不迫地化解危機。

◎ 許馨尹

前　言

時代變遷，我國在世界潮流中，逐步走向民主開放的社會。從總統直選、政黨輪替、公投入憲等關鍵性議題，獲致歷史性的成果。然而，在民主多元化的發展進程中，仍是工安事件頻傳，經濟犯罪層出不窮，不僅影響國人的生命財產安全，更因民眾自我意識抬頭，爲爭取權益所採取之聚眾陳情、激烈抗爭等手段，造成社會浮動不安。此外，兩岸對立是存在已久的事實，雖然目前雙方學術、經貿或文化交流日趨熱絡，但中共武力犯臺的企圖並無任何改變，尤其在 2005 年 3 月 14 日悍然表決通過「反分裂國家法」（Anti-Secession Law），並即公布施行。此一片面行動撼動了脆弱的臺海現狀，爲未來兩岸間的互動前景投下不可預測的變數。

我們生活在這多元開放的時代，危機無所不在，也隨時可能發生，平時若無危機預防之觀念，臨事又無處置的方法，不能迅速妥善解決問題，將帶來無窮後患，甚或造成重大災難。所謂「明者遠見於未萌，智者避禍於無形」，與其事後「亡羊補牢」，不如事前「防微杜漸」。因此，先知先制的預防乃是保防工作的重點。本文試將危機預防與保防工作結合提出探討。

危機預防與保防工作

「危機」一詞按字典可闡釋爲「生死存亡的緊要關頭」，往往伴隨著緊迫、威脅與不確定性。只要危機一發生，處理不好就會產生危害，組織也將蒙受損失；相反地，若處理得宜，不僅可以減少損害程度，甚至可以化危機爲轉機，其關鍵點即在於是否做好危機管理。學理上將危機管理分爲三個階段：危機預防、危機處理及復原工作。由於我們無法預知危機什麼時候會發生？以何種型態出現？因此，要加強風險觀念，積極做好危機管理，找出安全上的盲點，羅列可能發生的危機項目，未雨綢繆，此即「危機預防」的積極作爲。

「保防」在字面上的意義可詮釋爲「對敵保密，防制滲透」。工作涵括「機密保護」、「安全防護」、「防制滲透」、「保防教育」等四項業務。其要義在於保護國家的安全與利益，針對所有可能的威脅，所採取的一切防制措施；其終極目標，在排除國家安全、政治安全，與社會安定的威脅來源，防止一切外來勢力或本土人民，抑或內外相結合而進行的諜報、顛覆、破壞、恐怖主義等不法活動。

如何做好危機預防與保防工作

「沒有安全，就沒有一切」，既然危機預防是一切安全的基礎，而保防工作又是國家安全的第一道防線，那麼我們應該如何強化呢？以下謹就保防工作的四項業務，探討危機預防之具體做法。

(一)在「機密保護」方面：

韓非子曾說：「事以密成，語以洩敗」。兩國相交，可能因外交官一句不謹慎的話，引起戰爭，或埋下以後殺戮的種子，如果是接受賄賂，出賣情報，情形就更為嚴重。所以為了保障國家安全，人人依法應絕對保守國家機密，於處理機密公務時，更必須採取保密措施，嚴防洩密；發現可疑要即時處理，並檢討改進缺失。唯有養成「人人保密、事事保密、時時保密、處處保密」的觀念，謹言慎行，才能確保機密安全。在個人方面，則要不斷督促自己做到「有要緊之事機，不可輕與人言；有要緊之筆札，不可輕落人手」；此外，慎防表情洩密亦是做好保密工作值得注意的事項。保防工作者要有捨我其誰的沉穩氣度與膽識，以形乎自然的態度來處理機密相關事宜，以免顯露作為而未能達成克敵制勝的目標。

(二)在「防制滲透」方面：

敵諜雖然看不見，但是始終存在。當一個人或一個國家想擴張慾望，或其利益受到危害時，都會用盡各種手段探聽敵情，以求「知己知彼、百戰百勝」。可想而知，在我們國家處境艱難的時刻，我們的生活周遭必然充斥著看不見的間諜，明槍易躲，暗箭難防，對方要探聽機密不會先告訴你，因此謹言慎行最須注意。身處競爭激烈的社會，今日的朋友，也有可能是明日的敵人，因此即使是在親密關係中，仍應保留一點空間，不隨便露出個性上的弱點，不輕易顯示自己的慾望和企圖，培養高度的警覺心是維護自身安全的基本認識，相信只要別人摸不清我們的底細，自然就得不到攻擊的機會。

(三)在「安全防護」方面：

安全是「有備無患」的預防工作，也是「未雨綢繆」的功夫。在做法上，掌握全般並且洞悉危機發生的潛在原因，據以建立預警機制，乃安全防護工作之首要任務。其次，在危機發生前就成立危機處理小組也是必要的準備工作，俾使危機發生時，能自然而然形成一個運作網路，讓每個人都適時扮演適當的角色。此外，除了要定期檢討危機處理標準作業功能，也應要求相關人員熟練操作技能。例如舉行無預警模擬演練，可以讓員工在面對危機時，有經驗可循，也才能臨危不亂、從容應變。相信只要機關內的每一分子都能時時保持高度警覺，處處留心週遭變化，事前做好嚴密無懈的防護及萬無一失的應變措施，發現問題時亦能立即反映處理，必能確保機關物質、器材、設備與人員安全於無虞。

(四)在「保防教育」方面：

「保防即是預防，預防首重宣導」。面對急遽變動的社會，敵人滲透手法不斷翻新，保防工作更要與時俱進。法國大文豪雨果曾說：「世界上只有一種力量強過全球所有的軍力，那就是觀念。」正因為國家安全需要每一分子共同經營，社會每一分子也需具備「保防工作，

人人有責」的觀念，因此從教育著手，使全民經由潛移默化的方式，培養「保防工作就在你我」的觀念，方能建立全民共識，達到「全民保防」的境界。

結　論

所謂「禍常發於所忽之中，而亂常起於不足疑之事」，凡事「豫則立，不豫則廢」，是亙古不變的道理。誠如洛克菲勒所言：「除了掌握自己的事以外，最重要的就是明白別人在做些什麼」。保防工作猶如下棋鏖戰，高手一眼能看出好幾步棋，低手只限一兩步，先知的人才能先發制人。「危機沒有預警，安全沒有假期」，危機預防乃保防工作之核心，有了充分的準備，危機發生時，我們才能從容不迫，冷靜以對。更重要的是，「保防工作從個人做起」並不只是口號，而是需要每一分子共同的努力。倘若全民都能懷有一顆熱忱的愛國心，確立自我保防觀念，則國家安全必能確實獲得保障。

（本篇摘錄自法務部調查局清流月刊 97 年 3 月號）

資訊時代對國家安全的挑戰

如何維護我方敵情系統的完整，應是軍事戰略上的優先考量。

◎ 吳祥億

壹、前言

隨著科技的高度發展，「資訊戰」儼然已成爲 21 世紀之戰爭主流。在資訊戰力整備中之「資訊網路攻擊戰術戰法」運用，因其可達兵不血刃而千里屈人之兵的效果，已形成極重要之課題。尤其，中共近期提出各種數位網路攻擊模式，期以新型態之「網軍」達到「損小、效高、快打、速決」的戰略指導原則，將對我國防思維及現有優勢造成重大衝擊，須密切注意其發展，並研擬因應之道，以確保我國家安全。

綜觀這些年來世界各國對網路戰的研究和實戰情況，網路戰的主要體現在四個方面：駭客攻擊、病毒傳播、通道干擾、節點破壞。最近一段時期，中共軍方媒體對網路戰做了不少評論，認爲網路戰分爲「全球網路戰」和「戰場網路戰」兩種，「全球網路戰」就是國家或集團圍繞和運用電腦網路進行的政治、經濟、文化、科技、軍事等鬥爭；「戰場網路戰」是指戰爭中交戰雙方圍繞和運用戰場互聯網進行的對抗。

這種「戰場網路戰」戰鬥在看不見的網路系統內，「網軍」憑藉有力的「武器」和高超技術，侵入敵方指揮網路系統，隨意瀏覽、竊取、刪改有關資料或輸入假命令、假情報，破壞敵方整體作戰自動化指揮系統，使其做出錯誤的決策，並通過無線注入、預先設伏、有線網路傳播等途徑實施電腦網路病毒戰，癱瘓對方網路，再運用各種手段施放電腦病毒直接攻擊，摧毀敵方技術武器系統；同時運用病毒和駭客攻擊敵國的金融、交通、電力、航空、廣播電視、官方機構等網路系統，攪亂敵國政治、經濟和社會生活，造成社會動盪。

貳、中共駭客侵臺狀況與研析

近年來，中共解放軍運用其「網軍」，陸續入侵我政府與民間部分網站與資訊系統。其攻擊對象甚且廣及世界各國，引起各界高度重視。茲將近幾次大規模的侵害分述如下：

1. 92 年 9 月 3 日：包括 30 多個政府單位及 50 多個民間企業共 88 個機構之電腦，8 月間陸續遭中共駭客透過民間公司網站掩護，進行系統入侵並植入木馬程式。

2. 93 年 6 月 23 日：某政黨黨部網站遭駭客入侵，修改網頁首頁連結，只要民眾進入該黨中央黨部網站，就會被連結至其他預設的網頁。

3. 93 年 7 月 24 日：某官方網站遭中共駭客入侵，不但五星旗占據首頁，還以簡體字寫上「祖國統一，打擊一切分裂，打擊臺獨」等字眼。

4. 93 年 9 月 27 日：某兩個地方政府的網站遭到入侵，被置換首頁並掛上五星旗和不當言論。

5. 94 年 7 月 19 日：某軍方單位網站疑似遭大陸駭客入侵，顯示對外網頁伺服系統有嚴重的系統漏洞，以致於駭客透過系統漏洞登入主機並修改網頁。

6. 95 年 3 月 18 日：政府某部會內部電腦系統遭到中共以木馬程式入侵，竊走機密的高層出訪行程與對外談判資料。

7. 95 年 4 月 25 日：國內數間大專院校、職校、小學，甚至安全業者網站，分別遭到一家名為「海東青」的組織以網路釣魚方式，讓使用者自行輸入個人機密資料。

8. 96 年 1 月 16 日：國軍某 4 個單位內部網站遭中共駭客以惡意程式入侵，竊取不少機密資料，洩密原因在於工作人員以隨身碟任意下載不明網站資料，而使駭客有機可乘。

中共利用資訊偵蒐能力，特別是藉助網軍或坊間駭客的力量，對電腦網站惡意攻擊，企圖竊取我軍事機密，並運用具有電腦專業知識之科技專家，侵入我方網路工作系統，或穿過我設置之防火牆進入網路核心，進而破壞網路或從網上竊取情報，以奪取網路控制權。中共同時研發各類型網路病毒，企圖傳入國軍武器系統或 C4I 指、管、通、情系統中，擬以交互傳播、感染、擴散等方式，侵害我網路系統之軟、硬體設施，使國軍網路系統喪失功能。

參、新一代的資訊戰

一、使用電磁脈衝

電磁脈衝是一種高強度的電波干擾，其產生之高強度電磁脈衝，能夠使半徑數十公里內的所有電子設備癱瘓，對於隱蔽在地下的電子系統，電磁脈衝亦能強烈干擾。 這些奔向地面的電子流，雖然其週期只有「毫秒」，但卻能在目標區地球表面 300 公里範圍內產生強大的電磁脈衝衝擊波，使得電子裝備內部的電晶體、二極體、放大器、積體電路、邏輯電路、微處理器等元件、組件，皆因瞬間超載短路，造成外部完好卻無法修復的永久損壞。同時，電磁脈衝衝擊波涵蓋範圍內的無線電通訊，將因大氣層荷電密度的劇變，對頻率在超高頻以次的波段，產生長達一小時以上的干擾。就整體而論，在電磁脈衝衝擊下，國家的指管通情偵監電腦系統（C4ISR，即指揮、管理、通信、電腦、情報、偵察及偵測）有可能全面毀壞，軍方與民間資訊系統一概癱瘓，整體戰力與運作機制立即破壞。其施行方式即以約 1KT 的核彈頭在 40 公里的平流層頂引爆，所產生的高溫與高壓震波皆無法達到地表，微量的輻射落塵亦被阻滯在平流層內，不會立即飄降下來，因此是「乾淨核爆」，而被攻擊地區的軍民皆毫髮未傷，但國家的整體戰力與運作機制卻被立即癱瘓，賴以為生的資訊通電設施將永久失效。在電磁脈衝攻擊下，國家的運作與軍隊均因資訊化而遭癱瘓，大至雷達小至行動電話統統瞬間失效，致使整個防衛機制變得全盲、全聾、全啞，根本無從有效遏止敵之乘虛而入。

二、運用線上遊戲、MSN、ICQ 等即時通軟體植入木馬程式

時下青少年對於線上遊戲的依存度，可說已到達形影不離的境界；而對於線上遊戲的玩家而言，與對手交換寶物及下載外掛程式，又是不可或缺的動作之一。因此電腦若進行線上遊戲而呈現獨占模式，然後和不明玩家交換寶物時，等於是將電腦處於毫無防護的狀況下傳輸資料，該情形無疑讓電腦系統暴露在病毒的環境之中，很容易被植入木馬程式。另外，機關內部若無實施網路系統與儲存設備的實體隔離，很容易使機關外部原本架設周密的防火牆形同虛設，加上現階段 MSN 等即時通軟體普遍及便利，更淪爲病毒入侵的方便之門。科技的方便，也順道帶來系統性的風險，此爲政府部門所應深切注意的。

三、以網路釣魚方式竊密

網路釣魚（又稱爲 Phishing）已在美國造成嚴重災情。根據美國網路釣魚防範小組（APWG）的統計，釣魚網站平均的壽命長達 6.1 天，也就是說，從開始釣魚到被檢舉關站之間，這些網站通常可以存活將近一周，足以騙取相當多的使用者個人資料；而目前已知存活最長的釣魚網站，則有 31 天，網路使用者不可不多加提防。駭客利用垃圾郵件的管道發送仿效知名網站的電子郵件，引誘無知的使用者進入僞裝的知名或政府網站，藉此騙取使用者帳號、密碼，或姓名、地址、電話等，然後再利用這些帳號及密碼獲取不當資料。由於這種網路犯罪手法較爲新穎，網路犯罪專家估計，第一次收到「釣魚信件」的使用者有 3%會被騙。網路釣魚通常會先寄發垃圾郵件，標題則多半爲「系統更新，請檢查帳號」、「保護帳號，請變更密碼」、「帳號被關閉，請上網重新啓動」等容易吸引使用者注意的字眼，藉以取信於受害者，然後再提供一個僞裝過的連結，誘騙使用者登入假網站輸入個人資料。

四、利用電腦系統佈建

中共駭客將微軟最新作業系統 Vista 破解後，順道植入木馬病毒及惡意程式，並公開於網站供人下載，許多貪小便宜的使用者若安裝破解版之 Vista 系統，每台電腦都有可能成爲中共駭客進入臺灣竊取隱私資料的跳板，此爲另類的資訊(訊息)戰，因爲大部分的破解版 Vista 之皆爲大陸駭客所發行。不可諱言，中共網軍若以此爲資訊戰前的布局，伺機利用 Vista 之普及以悄悄滲入臺灣內部，中共即能輕而易舉地掌握臺灣各種以電腦控制的系統；如果其發動戰爭，中共網軍即可輕易地癱瘓或掌控臺灣電腦系統(諸如：空軍塔台、電達系統、飛彈系統等)，其可不戰而勝，該情況實值得相關單位注意。

肆、資安問題因應之道

一、人員進出管制

資訊管制區內應有適當的進出管制保護措施，以確保只有被授權的人員始得進入。進出管制應考量事項建議如下：(1)來訪人員進入管制區應予適當的管制，並記錄進出時間；來訪人員只有在特定的目的或是被授權情形下，才能進入管制區。(2)在管制區內，所有的人員應配載身分識別標示，並隨時注意身分不明或可疑的人員。(3)員工異動或離職後，應立即更改或撤銷其進入管制區的權限。(4)各樓層的配置說明及內部的電話聯絡簿，應以不讓有心人士循線找出電腦設施的所在地爲原則。

二、網路安全人員內部控管

內部資訊人員爲掌握機敏資料最關鍵的人物，因此單位內部的系統管理者其平時社交生活狀況尤應特別注意。內部控管保密資料的機制如未能有效執行與落實，則非常容易淪爲有心人士介入的弱點，而引發極爲嚴重的後果。

三、小心外聘網路安全人員(維護系統時直接接觸主機)

有些機關的資料輸入與系統維護是委外處理的，在委外過程中要考慮那些資料適合委外，那些資料不適合。其次，若要委外應要考慮如何做，讓資料不易外洩，例如一些資料可用代碼、代號方式儲存。而且可以把資料分成兩部分交給兩個人繕打，或可以把重要的資料挑出自行繕打，以防止資料外洩，這都是資料輸入時要考慮的。另外在輸入資料時，儘量不要把每一項目都告知輸入人員，以提高安全性。近期某科技公司工程師利用公司派他到某政府機構維修電腦時，因該機構承辦人不熟悉系統維護流程而放任外部工程人員進入機房，該工程人員即在無人看管下偷偷拷貝資料，造成資料外流，此皆爲政府部門所應警惕之處。

四、嚴防人員勾串，內神通外鬼

96 年 1 月軍方所屬某 4 個單位因人員以隨身碟任意下載不明網站資料，結果遭中共駭客以惡意程式入侵。姑且不論該事件是否因內部人員之故意，或係單位內部人員的不慎，其內部網站遭入侵已是事實。因此資訊教育應以強化電腦運用、提升資訊系統管理運用能力爲目標，而資訊倫理的教育以及隨身碟的管控，更是單位內資訊安全控管的重點所在；尤其現今病毒發展速度之快，許多看似安全其實充滿危機的動作，常被一般人所忽視，單位內對儲存媒體的控管應該多加重視，才能有效防堵任何可能發生問題的漏洞。

五、嚴守「專網專用」政策

嚴禁國軍網路、戰情網路、機敏網路與網際網路搭接、混用或誤插，此爲網路安全最重要也是最基本的概念；民網應以集中、公開設置爲原則，如有軍、民網資料交換需求，必須設置檢疫區，檢疫電腦僅能單一用途，嚴禁處理公務之網路連接外部網路系統，才能確保專網專用的實質效益。

六、落實網路安全防護機制

由於電腦網路具有開放性、互連性等特徵，易受到電腦駭客、電腦病毒和其他非法攻擊。爲確保網路安全，軍用網路須與網際網路完全隔離，使駭客無法透過網際網路進行攻擊。其次，在軍用網路上傳輸和處理軍事機密資料必須採多層級、多功能等加密措施。再其次，是建構一套完善入侵檢測系統，針對可能危害網路安全事件進行掃瞄並分析網路中各個封包內容，確定所傳輸內容是經授權，並對入侵資訊發出警告及採取隔離網路連接、跟蹤攻擊源、記錄攻擊過程等措施。因此建議：

1. 資訊安全機制：從密碼防護機制、電腦病毒防禦機制等方面去強化。

2. 網路安全機制：從設置網路防火牆、虛擬私有網路(VPN)等技術方面去防護。
3. 系統安全機制：可從弱點掃描、入侵偵測損害預防等機制之建構防護。

七、建構優勢資訊戰力

資訊戰首重「安全」。國家基於當前戰略構想，在考量資訊安全應置網路防護爲優先，故目前資訊戰的重點乃在網路安全防護，且以全方位思考與創意運用爲原則。在發展安全防護機制與系統裝備之外，更應朝向構建自動化、系統化以及資訊化之安全防護系統目標邁進。由被動性的防護進而建構主動性的監、偵能量及反制作爲，同時結合產、官、學、研界力量建立防衛自主能量，俾確保國家在資訊戰場的優勢，以克制中共犯臺企圖。

八、強化網路保防工作

針對電腦病毒戰的攻擊，除迅速對症下藥及清除病毒外，並應以「防火牆」機制，事先劃分若干個封閉「隔離箱」，整個電腦系統即分塊隔離，避免整個系統染上病毒。

爲貫徹多管齊下的預防措施，應運用各種防禦手段，包括：經由對電腦加密防止敵方(或駭客)進行電腦滲透以竊取情報資料；對核心系統和重要用戶的密碼和口令，要嚴格控制知曉範圍，嚴守機密；通過加強管理、監督、檢測、維護等各種技術手段；對敵方實施電磁欺騙和干擾，也可利用一定功率的干擾釋放假信號，擾亂對方的微波探測，誘惑其上當或直接干擾敵方探測設備的正常工作，以達到屏蔽己方的資訊源，保護系統正常工作的目的。

伍、結論

中共近來極熱衷於資訊(信息)戰的發展。在面對中共的威脅下，應如何維護我方敵情系統的完整，應是軍事戰略上的優先考量。除了本身對於信息戰應建構基本正確的觀念，更應於平時即養成資通保密與網路安全之概念。我們從近來各資訊網路遭到入侵的相關例子，可以了解駭客技術已從早期的偷窺、毀壞資料，進步到分散式阻絕服務攻擊等技術，以圍剿目標網站；電腦病毒的散布，亦從個人檔案的傳遞感染，演變至附加在電子郵件的寄發，以擴增影響範圍。此正顯現出資訊戰中最鮮明的一項特質－「科技的進步加速了資訊網路攻擊戰術戰法運用之不斷革新」。網際網路的便利，提供了駭客與病毒入侵之管道，新的犯罪型態及資訊恐怖主義勢將威脅正常的網路用戶。尤其國防資訊系統是敵方駭客最欲遂行網路攻擊及侵入的目標，是故政府各單位應積極研擬有效之資訊網路攻擊及防護戰術與戰法，於癱瘓敵軍資訊網路系統之同時，亦能阻絕使用網路攻擊之敵軍，以充分達到資通支援作戰，確保國家安全之目的。

（本篇摘錄自法務部調查局清流月刊 97 年 2 月號）

監造剋星—工程查核

針對影響大眾安全且具危險性的材料，進行材料檢驗及拆驗確有其必要。

◎ 楊秉蒼

根據「政府採購法」第 70 條規定，機關辦理工程採購應明訂廠商執行品質管理、環境保護、施工安全衛生之責任，並對重點項目訂定檢查程序及檢驗標準；其中，第 4 項規定中央及直轄市、縣（市）政府應成立工程施工查核小組，定期查核所屬（轄）機關工程品質及進度等事宜。爲此，行政院公共工程委員會成立三級品管制度，建立工程施工查核小組作業辦法，以期透過系統化管理，使完成之工程建設品質完善，以達標準與要求。

依行政院公共工程委員會之「工程施工查核小組組織準則」規定，查核小組依職權行使對象之差異可分爲中央（中央查核小組及部會行處局署院查核小組）及地方（直轄市政府查核小組及縣（市）政府查核小組）。查核小組之主要查核項目，得包含：

1. 機關品質督導機制、監造計畫之審查紀錄、施工進度管理措施及障礙之處理。
2. 監造單位之監造組織、施工計畫及品質計畫之審查作業程序、材料設備抽驗及施工查核之程序及標準、品質稽核、文件紀錄管理系統等監造計畫內容及執行情形；缺失改善追蹤及施工進度監督等之執行情形。
3. 廠商之品管組織、施工要領、品質管理標準、材料及施工檢驗程序、自主檢查表、不合格品之管制、矯正與預防措施、內部品質稽核、文件紀錄管理系統等品質計畫內容及執行情形；施工進度管理、趕工計畫、安全衛生及環境保護措施等之執行情形。

在執行層面上，基於整體品質因素考量下，建立工程品質查核五大指標，包含：

1. 環境指標：基地內外及週邊環境整潔、粉塵、噪音及振動。
2. 安全指標：防墜等安全設施（如護欄、開口加蓋）、防止崩塌安全設施、防漏電設備、工地內施工警告設施、圍籬、外部防護網等設施、交通安全措施及危險性工作場所之申請。
3. 強度指標：混凝土、鋼筋、模板、土方、結構體及材料設備檢驗與管制等施工品質。
4. 美觀指標：裝修、雜項、結構體、建築物、構造體、基地內外及週邊等呈現整體美觀感受。（參考文件：設計圖說、施工技術規範、植栽計畫等）。
5. 功能指標：業主需求符合程度、施工成本、經濟性。（參考文件：設計圖說、設計/分析報告、施工技術規範、工程預算書、價值工程研析成果報告書等）。

惟工程結構體外觀無瑕疵或文件紀錄完善，並不能代表材料品質無瑕疵；爲此，行政院公共工程委員會爲進一步確保結構隱蔽處之材料施工品質，規定查核缺失有下列情事之一者，工程應列爲丙等，包含：

1. 鋼筋混凝土結構鑽心試體試驗結果不合格。

2. 路面工程瀝青混凝土鑽心試體試驗結果不合格。
3. 路基工程壓實度試驗結果不合格。
4. 主要結構與設計不符情節重大者。
5. 主要材料設備與設計不符情節重大者。
6. 其他缺失情節重大影響安全者。

至於工程查核成績列爲丙等者（評分爲 70 分以下），機關除應依契約規定處理外，並應爲下列之處置：

1. 對所屬人員依法令爲懲戒、懲處或移送司法機關。
2. 對負責該工程之建築師、技師、專任工程人員或工地主任，報請各該主管機關依相關法規予以懲處或移送司法機關。
3. 廠商有政府採購法第 101 條第 1 項各款規定之情形者，依該法第 101 條至第 103 條規定處理。
4. 通知監造單位撤換監工人員。
5. 通知廠商依契約撤換工地負責人或品管人員或勞工安全衛生管理人員。

當然有人會問，工程在監造監督的情形下，有需要根據政府採購法第 70 條規定，額外訂定工程查核辦法嗎？此舉會不會太勞師動眾，浪費國家政府資源。然根據行政院公共工程委員會 96 年執行列管之三千餘件工程查核案中，發現工程查核列爲丙等案件將近七十件，比例約占查核案件數 2%左右。由此了解工程雖有監造監督承包商，然在無法有效落實全程監造（人力不足），或監造與承包商共生（日久生情）等弊端下，監督不實之案件仍會不斷發生，這也間接證明政府採購法第 70 條規定的必要性。

由上述內容說明了工程推動過程是否接受工程查核監督，就工程品質而言，確實會產生一定程度的監督效果；惟現階段礙於經費及人力的限制，目前僅有公告金額以上（查核金額係工程及財物採購爲新臺幣 5,000 萬元，勞務採購爲新臺幣 1,000 萬元；公告金額係工程、財物及勞務採購爲新臺幣 100 萬元。）的工程才有機會接受工程查核，一般公告金額以下的小型工程，很難有機會監督工程主辦單位、監造單位及承包商。以轟動一時的臺北市養工處瀝青重鋪工程官商勾結案爲例，在案發後，檢調單位於臺北市近四十條道路，進行二百多處鑽心取樣，發現偷工減料道路超過 70%，涉弊道路幾乎遍及大半個臺北市，嚴重影響工程品質。或許道路工程偷工減料，未必會對民眾的生命安全帶來立即性的威脅，如果是擋土牆呢？所以工程小歸小，仍可能存在因小失大的危機，或許未來可依工程屬性的重要程度，進行「選擇性」的工程查核（例如僅查核材料或施工品質），如此可在防不勝防的基礎上，使公告金額以下的小型工程之主辦單位、監造單位及承包商，時時感受工程查核的壓力，這對國內整體營造工程環境之改善，或許會更有「全面性」的助益。

除此之外，目前工程查核已賦予查核委員對已完成結構體進行材料「檢驗及拆驗」之權力，然現階段工程查核案件有進行材料檢驗及拆驗動作者，仍是少數。或許會有人認爲結構外觀無明顯瑕疵(如蜂窩等)，且材料檢驗報告合格，難道品質會有問題嗎？「機會應該不小」；或許會有人不認同，但回頭想想廠商能以不合理的價格低價搶標，那承包商的利潤在哪裡，

關鍵在於「材料」。試想有人可以在不進行任何檢驗的前提下，以目視或經驗得到水泥混凝土抗壓強度、鋼筋抗拉（或降伏）強度及瀝青混凝土的壓實度嗎？既然無法以經驗或目視判別材料品質，又擔心監造不力的危害，因此，針對影響大眾安全且具危害性的主要材料，進行材料檢驗及拆驗確有其必要性，並且查核委員要親送樣品，並監督材料檢驗，才能確保檢驗的有效性，畢竟「道高一尺、魔高一丈」，千萬不可低估承包商的能耐。

（作者是正修科技大學土木與工程資訊系助理教授）

（本篇摘錄自法務部調查局清流月刊 97 年 3 月號）

營建料源不穩，品質堪慮

料源供應不穩定，間接否定營建材料的品質。

◎ 楊秉蒼

一般探討材料品質控制總會探究營建物料之料源問題，若料源供給不穩，材料檢驗品質肯定會出現問題。當然有人會問，現階段營建材料料源品質穩定嗎？「不穩定」。以下謹就國內水泥混凝土、鋼筋、瀝青混凝土及級配等大宗營建材料，說明營建材料之料源出現那些問題。

1. 水泥混凝土：

水泥混凝土係由水泥、骨材（粗、細）、水及摻劑（礦物及化學摻劑）等所構成之複合材料。一旦原料出現狀況，將嚴重影響材料成品品質。現階段水泥混凝土料源以細骨材（砂）的問題最大，尤其在國內河砂限制開採後，砂石來源爲影響混凝土品質之關鍵因素。根據調查國內每年正常砂石需求量爲 6,600 萬立方公尺（砂及石比例約 4：6）；其中，三分之一來自河砂開採，三分之一來自島內陸上砂與地下石，其餘三分之一主要依賴大陸進口。近來大陸禁止砂石出口，臺灣進口砂石量減少 1,200 萬噸，使砂石來源產生不穩定現象，進而影響水泥混凝土成品品質。爲解決砂石缺乏的問題，部分進口商從國外進口軋製砂，殊不知軋製砂可能潛藏之弱帶破裂面，會導致水泥混凝土強度降低（平均降低 1~2 成）；待了解事情嚴重性時，時間已過了 1~2 個月，爲時已晚。

2. 鋼筋：

近年來，在國際經濟大幅成長下，金屬原物料的行情居高不下。以鋼筋材料爲例，民國 90 年鋼筋單價每噸爲 8,000~9,000 元，至民國 96 年鋼筋單價每噸飆至爲 22,000~23,000 元；廢鐵行情亦飆至每噸 13,000 元之譜，至此種下品質不穩的開端。此種不穩定的現象，可由近來發現之鋼筋降伏、抗拉強度的異常及輻射鋼筋等事件，透露出品質不穩的端倪。其中，鋼筋輻射事件發現於苗栗某鋼鐵廠，該廠於 96 年 6 月陸續檢測出少量輻射鋼筋，事不過兩個月該廠又發現高達 2 噸之廢鐵有鋼筋輻射反應，其鋼筋表面輻射劑量高達每小時 150 微西弗，爲自然背景值的 750~1500 倍，創民國 81 年輻射屋事件後之最龐大輻射鋼筋（廢鐵）。其後，原能會根據三家廢鐵供應商提供的資料，追查載運廢鐵之供應商卡車駕駛，但駕駛不願意透露輻射鋼筋從何處收購，甚至誤導方向，最後不了了之。相關官員坦承，經過一個多月追查後，輻射鋼筋來源已陷入膠著。爲此，行政院公共工程委員會於民國 96 年 8 月 21 日發函予各縣市工程主管機關，要求加強查核公共工程使用之鋼筋，是否具有「無輻射污染證明」。如果本事件只是冰山一角，那麼料源品質實在欠缺保障。

3. 瀝青混凝土：

瀝青混凝土係由瀝青、骨材（粗、細）及填充料（石粉）等所構成之複合材料。早在民國 91 年各機關辦理瀝青混凝土再生利用作業要點前，已有承包商於瀝青混凝土內加入刨除再生瀝青混凝土粒料，企圖透過此種壓低材料成本的方式，提高工程得標率。試想發包預算書的材料爲一般瀝青混凝土粒料，但施工卻以再生瀝青混凝土鋪設，如果您是工程監造覺得合理嗎？其實要分辨是否添加再生刨除料，可透過瀝青回收黏度檢驗判斷；然現今多數瀝青混凝土黏度檢驗，多僅針對再生瀝青混凝土檢驗，一般瀝青混凝土則無瀝青回收黏度之檢驗，所以有一段時間承包商之瀝青混凝土得標價，僅爲工程底價的 4~6 成，這就是承包商以不合理價格承攬工程，卻不會虧損的原因。直到民國 91 年在考量環保及料源因素前提下，行政院公共工程委員會規定可以將刨除料添加於瀝青混凝土內，並規定每件工程之再生瀝青混凝土之刨除料，不得添加超過 40%，同時規定養護路面工程部分（每年總工程量），於民國 91 年需達 20%以上、92 年需達 30%以上、93 年需達 40%以上；新闢路段路面工程部分（每年總工程量），民國 91 年需達 10%以上、92 年需達 20%以上、93 年需達 30%以上。此後，瀝青混凝土的得標價漸趨正常，但品質缺失依舊存在。根據公共工程委員會的規定，刨除料添加量不得大於 40%以上，惟現階段國內多數承包商，在砂石料源價格居高不下的情形下，刨除料添加量多已超過 80%，嚴重影響道路使用壽命及工程品質。

4. 級配：

一般工程用級配可分爲河川級配及陸上級配（山級配）。在構築新鋪設道路或回填工程，常須於鋪面底層鋪設一定厚度之碎石級配層襯底。由於河川級配無論品質或潔淨度均優於陸上級配，所以河川級配大多被用於水泥混凝土及瀝青混凝土原料，加上現今砂石料源取得不易，價格居高不下，使得現今道路及回填使用的級配料多爲陸上級配。由於陸上級配含泥量高，所以品質（硬度與級配分布）較河川級配差，加上陸上級配顏色多呈現土黃色，故不法承包商在料源取得困難下，常會於級配料中添加廢棄混凝土塊及轉爐石塊；若非洗淨，否則很難於現場第一時間判別是否爲碎石級配，此現象在級配料源缺乏的情形下，是常見的。此外，於碎石級配料加入轉爐石塊，會因轉爐石之體積不穩定性，產生路面隆起損壞（應靜置一段時間，約 6 個月~1 年以上，才可使用），有時隆起高度可達 30cm 以上，材料品質沒有保障。

由上述四個例子不難理解國內營建材料現階段料源供應，並不如想像中的完善。既然料源供應不穩定，這也間接否定營建材料的品質，這也是現階段營建承包商經營上的困境，值得政府有關單位重視並更積極地防範。

（作者是正修科技大學土木與工程資訊系助理教授

（本篇摘錄自法務部調查局清流月刊 97 年 4 月號）