臺灣澎湖地方法院廉政暨維護簡訊

105 年 5 月份

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」

問：公務員因生日，獲長官致贈蛋糕，可否接受？另若機關首長生日，部屬合資贈送蛋糕，可否收受？

答：原則：對於與其職務有利害關係者餽贈財物，原則上應予拒絕。（本規範第 4 點前段參照）

例外：但有下列情形之一，且係偶發而無影響特定權利義務之虞時，得受贈之。(本規範第 4 點但書參照)：

1. 屬公務禮儀。
2. 長官之獎勵、救助或慰問。
3. 受贈之財物市價在新臺幣 500 元以下；或對本機關（構）內多數人為餽贈，其市價總額在新臺幣 1,000 元以下。
4. 因訂婚、結婚、生育、喬遷、就職、陞遷異動、退休、辭職、離職及本人、配偶或直系親屬之傷病、死亡受贈之財物，其市價不超過正常社交禮俗標準。

因此(一)公務員獲長官致贈蛋糕，屬長官對部屬之慰問範疇：雖長官與該名 公務員間，有指揮監督關係，係與其職務有利害關係，惟該等行為屬長官之慰問，為本規範所允許(本規範第 2 點第 2 款、第 4 點第 2 款)。

(二) 部屬合資贈送蛋糕給長官，長官可以接受者限於市價新臺幣 500 元以下。(本規範第 4 點第 3 款前段參照)。

從國家角度省思網路安全態度

作者◎楊于勝

美國在網路戰指導及整備作為越發強硬且公開的同時，臺灣在國家安全、政府運作與國防指管機制等諸多面向，均應積極以對，否則網路安全將淪為空談！

2011 年 5 月 31 日，美國《華爾街日報》轉述報導，美國國防部首度正式針對網路駭客攻擊訂定因應策略，認定來自其他國家的破壞電腦之舉，係構成戰爭行為，意味美國得以因此使用傳統軍力報復此類攻擊。儘管美國尚未有針對網路駭客攻擊，進而引發軍事行動，但如何掌握網路安全則著實是一項挑戰。

2015 年 8 月 5 日凌晨的臺灣，支持反課綱的國際駭客組織「匿名者」亞洲支部（AnonymousAsia），對臺灣政府發出最後通牒，限時 48 小時內回應，否則將會全面攻擊民生系統並入侵臺灣網站；該組織 PO 出截圖，說明匿名者確有能力攻擊政府民生系統網站。從已披露的紀錄顯示，「匿名者」三度攻擊並癱瘓國民黨、新黨、經濟部、國民黨臺北市黨部等網站；臺灣維護網路安全之機制，現今已實為一項重要的課題。

網路安全影響深遠

儘管前述「匿名者」亞洲支部對臺灣政府機關的攻擊事件，最後並未造成傷害，然而顯示出臺灣在網路安全維護機制上，仍處於襁褓階段。記憶猶新的是，稍早在 2015 年 4 月，為增強臺灣資安戰力，國安局特考還增加具「資安專長」的技師類組，卻創下無人報考的紀錄？讓關心國安者，不得不對維持網路安全的戰力與能力，抱持著懷疑的態度。

臺灣在許多領域幾乎是以美國馬首是瞻，當然網路安全亦不例外。國軍年度重大演訓在封閉網路攻防的課目中，即是一項被納入的重點，目的在於觀察影響指揮管制機制的程度。軍隊如此，政府運作更需要網路，稍有不慎，影響遍及各行各業。爰此，在前述「匿名者」的攻擊事件消息傳出後，時值颱風接近，乃有網友在相關版面留言，「不要癱瘓醫院或消防局之類的救災系統」或「不要拿老百姓生活依賴的民生系統為目標」，即是體認到一旦攻擊成真，影響深遠。無怪乎美國將「駭客」視同敵軍，規劃以傳統軍力來實施報復。

面對網路攻擊的無遠弗屆，美國國防部刻正以「正視網路文化（cyberculture）變革」來因應網路安全，或許臺灣可作為參考。尤其當美國對中國大陸從不間斷指責「駭客」竊取情資，並準備建立一個號稱全球首創之「網路武器控制協議」，用以規範承平時期不得對電廠、金融、醫院、電信網路等「重要基礎建設」實施網路攻擊，不過其中可關注的重點有三：其一、既然防不了，那就規定遊戲規則，讓損失得以管控；其二、讓被竊取的資訊難以成為駭客攻擊的關鍵資料；其三、在網路間諜活動難以規範下，可能只剩侵犯智慧財產權得以大做文章。

需要改變之思維領域

2015 年 4 月下旬，美國國防部再次公布《網路戰略》(CyberStrategy)，表述美軍從當下到未來，為因應網路戰之行動指導，其五大戰略目標包括：「建立和維護可隨時執行網路空間作戰的兵力與能力」、「確保美國國防部資訊網路與資料安全，以降低任務的風險」、「隨時準備應對美國本土與切身利益遭受顯著入侵式或破壞性之網路攻擊結果」、「建立和維持可行之網路選項與計畫，並運用這些選項來管控衝突升高及適應各階段之衝突環境」與「建立和維持強大之國際友盟與夥伴關係，以遏阻散播威脅與強化國際安全與穩定」。

從戰略目標定義檢視，有明暗兩個部分的意涵。明者直指美國防部網路戰略之

使命，在保護國防部自身網路的相關基礎設施，確保美國避免成為網路入侵與攻擊對象，同時還要有效支援網路空間之軍事行動和應變計畫；暗者則指出相關網路部隊擴充或公私單位的緊密結合，更點名美國將自主選擇方式、時間和地點，來回應所遭遇的網路攻擊。值得省思的是，此發展不僅較美國國防部於2011 年 7 月制定的《網路行動戰略》(Strategy For Operating in Cyberspace）更深入，並與「白宮網絡安全和消費者保護峰會」在 2015 年 2 月所下的結論:「鼓勵私營企業與政府部門加強網路安全合作，共同防止網路安全威脅」有關；無怪乎美國國防部首席資訊官哈沃森（Terry Halvorsen）在 9 月 18 日的一場官方與專業領域人士出席之網路安全峰會（The 6th Annual Billington Cybersecurity Summit)，提出解決網路戰的挑戰與威脅，應重視網路文化三個需要解決問題的面向：紀律（discipline)、經濟狀況（economics）和冒險精神（enterprise)。美國政府早就鋪陳建設一條由國防領軍，並結合產官學的大軍。難道美國國防部是當下才大張旗鼓嗎？答案是否定的，因為早在 2012 年 11 月 20 日公布徵詢發展「基礎網電作戰」技術研究方案時，就已公開呼籲學術界和工業界的專家，積極參與軍事領域之攻擊技術範疇。

臺灣也是高度依賴網路的國家，有雄厚的資訊工業基礎、普及的工程技術人員，再加上大專院所普遍設有相關資訊系所，何愁不能效法成事，但主要的關鍵仍是在於心態！

結語

美國正在打造盟友間的網路安全合作關係，特別是在新版《美日防衛合作指針》中，加入了網路安全合作內容。臺灣若想在新的戰略高地找到立足點，網路安全絕對是一個值得投入，且賦予更多關注的領域。

（資料來源：本文摘自清流雙月刊 105 年 3 號）

安全維護

臺灣澎湖地方法院「危機處理」作業程序說明

壹、危機處理小組成員與作業程序：

一、本院危機處理小組成員：

院長（指揮官）、庭長（副指揮官）、書記官長（執行秘書）、總務科長、民刑事紀錄科長、民事執行處科長、文書科長、人事室主任、政風室主任、資訊室管理師、法警長。

二、本院發生一般危安狀況或陳情請願事件時，法警長應陳報院長及協調相關單位處置，另通報政風室協助處理。

三、若遇有大型群聚、圍堵抗爭、暴力衝突、受刑人庭訊後脫逃或違法之重大陳情請願事件時，法警長除應即陳報院長及協調相關單位妥適因應措施，並通報警察機關及調查單位協助處理。

貳、責任分工及通報機制

一、本院書記官長、相關單位及政風室應協助機關掌握設施及人員可能遭受危害或破壞之各項狀況，將資訊迅速陳報院長知悉處置，協調業管單位採取預防因應措施，政風室同時秉持「迅速、正確、持續、掌握」之基本原則，循政風體系向上陳報。

二、通報資料內容應具備人、事、時、地、物，為何、如何等 7 要件外，應瞭解危害有無擴大之可能與其影響程度，另注意本院有無先聯繫警方支援人力維護機關秩序安全。

法務部廉政署檢舉專線：「0800-286-586」(0800-你爆料-我爆料)。

臺灣澎湖地方法院廉政專線：06-9215222

E-mail：phdged@judicial.gov.tw

檢舉貪瀆專用信箱：馬公郵政 107 號信箱