現代公民核心能力課程計畫

現代科技與公民生活

子計畫一 現代科技面面觀

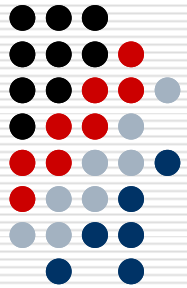
第 4 週 資訊科技與社會變遷

大葉大學電機系 陳木松

中華民國101年3月14日

chenms@mail.dyu.edu.tw

04-8511888-2167



科技的衝擊、迷思、省思

- ✓ 科技文明的演化史
- ✓ 現代科技何去何從：衝擊、迷思、省思
- ✓ 科技的正面影響：網路科技、運輸科技、能源科技等
- ✓ 科技的負面影響：酸雨、溫室效應、廢棄物汙染、水汙染等
- ✓ 科技擴大人際間的矛盾與衝突：人際互動減少、社會疏離感增加、資訊及技術被不正當的使用
- ✓ 現代科技與公民生活
- ✓ 建構科技時代的公民核心能力與素養

資訊倫理

- 科技的本質在於人類運用科學、知識、創意和資源，以解決所面臨的問題，改善生活環境的行動。可以說科技是人類生存的一種手段，也是社會變遷的主要動力。
- 資訊科技的發達，為人們的生活帶來前所未有的便利，卻也引發影響健康、環保、取代人力、非人性化、現實與虛擬混淆、侵犯資訊隱私權、智慧財產權、電腦犯罪、數位落差等問題。
- 對於這些問題，除透過科技保護技術和現行的法律來加以防範及懲處之外，還需要一套社會自主的規範機制，也就是「資訊倫理」。所謂倫理(ethics)指的是定義個人或群體行為的道德標準，而資訊倫理 (computer ethics)就是和資訊相關的道德標準。

科技引發倫理的爭議

- 我們是否有權利決定孩子生長於單親父母或同性戀的家庭裡？我們是否有權利決定孩子的性別？
- **網路中我們是否有權私自轉寄他人信件，造成隱私的傷害？我們是否有權利未經許可大量寄送商業性的垃圾郵件，造成收件人的困擾？**
- 動物可能作為基因工程的器官移植、藥物、實驗品等生產的工廠，人類謀求利益是否有權利控制動物的生存主控性？
- **因商業的利益所趨，就能在廣告中誇大產品的功能，隱瞞產品的負作用，造成消費者權利受損？**

科技的負面影響

1. 環境與生態問題
2. 科技戰爭
3. 科技犯罪
4. 地球資源過度使用
5. 精神文化的危機

電腦犯罪

- 社會變遷在帶來便利改變的同時，也可能製造出新的社會問題或社會脫序的現象。
- 例如：網際網路的發明帶來許多便利，但也衍生網路犯罪的問題。
- 為了維護使用者的權益，政府必須制定法律（如刑法之妨害電腦使用罪），約束不法的行為，個人也應建立**資訊倫理**的觀念，遵守法律並學習尊他人。

電腦犯罪的手法

- 積少成多：這種手法最常出現在金融機構，美國就曾經發生過某個銀行的行員在為客戶計算利息時，將美分 (cent) 之後的小數點金額轉入秘密帳號，舉例來說，假設計算利息的結果為123.4567美元，那麼付給客戶的利息將為123.45美元，剩下的0.0067美元就轉入秘密帳號，金額雖然很小，但累積成千上萬個客戶後，就能得到可觀的數目。
- 冒用身份：有心人士利用交談、窺視、翻看資源回收筒、便條紙、社交操縱等方式盜取合法使用者的帳戶與密碼，然後入侵系統，或利用合法使用者暫時離開電腦卻忘了登出系統，伺機入侵系統。許多公司已經意識到冒用身份的問題，因而開始教育員工注意相關細節。

電腦犯罪的手法

- 偽造資料：除了電腦已經存在的資料可能遭到竊取、竄改或破壞之外，事實上，資料來源的正確性也是不容忽視。舉例來說，假設售票系統的輸入人員向客戶收取全票的費用，然後在將訂票輸入電腦的同時卻設定為優待票，就能盜取全票與優待票之間的差價。
- 阻斷服務攻擊 (DoS attack，denial of service attack)、分散式阻斷服務攻擊 (DDoS attack，distributed DoS attack)：DoS的攻擊者會在瞬間發送大量的網路封包，癱瘓被攻擊者的網站及伺服器，諸如Yahoo!、亞馬遜、CNN.com等知名網站均曾遭到DoS而癱瘓；DDoS的破壞力比DoS更為嚴重，攻擊者會先透過Internet將「殭屍程式」植入大量電腦，然後同時啟動這些被控制的電腦，對被攻擊者的網站及伺服器啟動干擾指令，進行遠端攻擊。

電腦犯罪的手法

- 軟體炸彈 (software bomb)：軟體炸彈在進入系統的當下並不會立刻發作，而是在系統符合特定時間或特定邏輯的情況下，才會開始破壞系統或資料。舉例來說，電腦病毒就是屬於軟體炸彈的一種，知名的米開朗基羅病毒每逢系統時間為3月6日就會發作，摧毀硬碟資料，這種以時間做為發作條件的軟體炸彈又稱為時間炸彈 (time bomb)。至於以邏輯做為發作條件的軟體炸彈則又稱為邏輯炸彈 (logic bomb)，例如公司的離職員工因為心存不滿而撰寫某個程式，令它一搜尋到擁有者為其主管的檔案就予以刪除。

電腦犯罪的手法

- 程式後門 (back door)：這是依附於合法程式的非法指令，在合法程式執行完畢後，會留下一個秘密入口，有心人士可以利用它入侵系統。有些程式設計人員在開發需要認證程序的程式時，會在程式中留下「後門」，以方便在除錯階段時，能夠獲得特殊權限或迴避認證程序，而當「後門」被不懷好意的程式設計人員做為迴避認證程序的途徑時，就可能對系統造成威脅。
- 利用漏洞入侵：所謂漏洞指的是軟體設計或設定不當，導致有心人士利用漏洞取得電腦的控制權，因此，即時修正軟體漏洞是很重要的。
- 暴力入侵 (brute force attack)：這種攻擊方式很簡單，就是執行一個入侵程式，不斷嘗試所有可能登入系統的帳戶與密碼，直到登入為止。

電腦犯罪的手法

- 冒用主機 (spoofing)：攻擊者假冒成合法的主機，以獲得被攻擊主機的信任，進一步存取其服務與資源，這種攻擊方式往往能夠成功欺騙封包過濾型的防火牆。
- 網路監聽 (sniffing)：這是利用傳輸媒介具有廣播的特性，以監聽他人的資訊，舉例來說，10Base2或10Base5 Ethernet網路相同區段內的資訊會在同一條同軸纜線上傳送，有心人士只要將自己的網路卡設定為全部接收模式，就能接收到所有在這條傳輸媒介上傳送的資訊。
- 惡意程式 (malware)：泛指不懷好意的程式碼，除了前面提及的殭屍程式、程式後門、軟體炸彈之外，還有電腦病毒、蠕蟲、特洛伊木馬、間諜軟體/廣告軟體、釣魚軟體、垃圾郵件等，第14章有詳細的介紹。