失控的手機

2017 年印度及 2018 年澳洲國防部均嚴禁手機安裝微信 App；2019 年 2 月英國軍事智庫 RUSI 警告，如果讓華為參與 5G 行動網路，猶如開了「隱藏後門」。處於通訊軟體稱霸、人手一機的年代，楚門的世界是否危言聳聽？民眾要如何防範隱私外洩？

〈資安法〉上路！建構資通安全新時代

／國家文官學院政風室主任及兼任副教授　李志強

《資通安全管理法》(下簡稱:〈資安法〉)於108年1月1日上路，《公務機關所屬人員資通安全事項獎懲辦法》也同步實施。依據該等辦法，全國公務機關必須訂定資通安全維護計畫、資安事件通報及應變機制，違反者，資安人員最重將遭到記一大過的處分。

前言

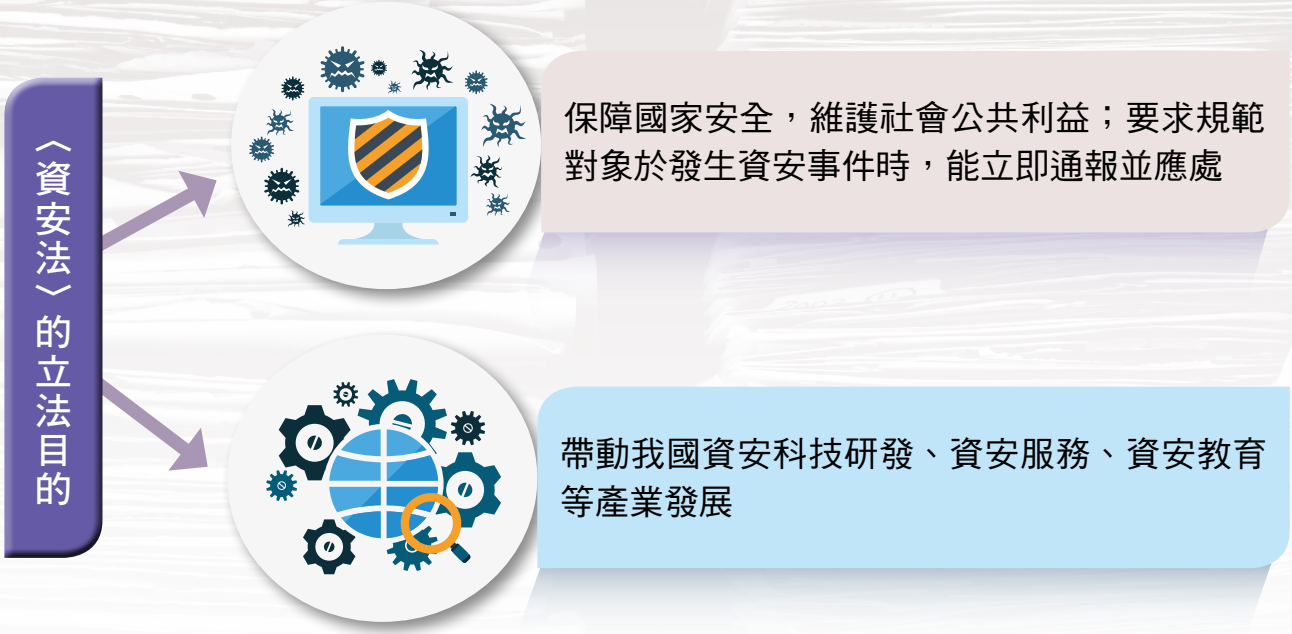
當大家透過手機或電腦享受網路便利的同時，駭客也無時無刻伺機入侵，輕者個人資料外洩，重者公司商業機密遭竊，甚至有政府機關因而停擺，可見資訊安全已是刻不容緩之議題。

由於缺乏一套以風險管理為基礎，規範整體資通安全的專法，行政院參酌先進國家立法原則，並考量我國社經環境與法規制度，研訂〈資安法〉草案，於 107 年 6 月 6 日總統華總一義字第 10700060021 號令制定公布，行政院另於同年 11 月 21 日訂定發布《資通安全管理法施行細則》、《資通安全責任等級分級辦法》、《資通安全事件通報及應變辦法》、《特定非公務機關資通安全維護計畫實施情形稽核辦法》、《資通安全情資分享辦法》及《公務機關所屬人員資通安全事項獎懲辦法》等 6 種配套規定，且已自 108 年 1 月 1 日施行。

有鑑於各界面對上路不久的資安新法，一時恐難探究竟，故本文歸納分析之，期能提供各界參考遵行。

資通安全管理法架構

（108 年 1 月 1 日施行）



〈資安法〉相關重點

一、立法目的

為因應網際網路及其他資通科技快速發展與普及，〈資安法〉的立意即是加速建構完善的國家資通安全環境，以保障國家安全，維護社會公共利益，並建立以風險管理為核心的機制，要求規範對象於發生資安事件時，能立即通報並應處。另一目的則盼此帶動我國資安科技研發、資安服務、資安教育等產業發展。在此說明，法條中所稱「資通安全」，係指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。而所謂「資通安全事件」，則指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

二、規範對象

〈資安法〉規範對象分為兩大類，其一是公務機關，係指依法行使公權力之中央、地方機關（構）或公法人，但不包括軍事機關及情報機關；另一對象則是特定非公務機關，此限於關鍵基礎設施提供者、公營事業及政府捐助之財團法人，並不及於一般民眾。前述所稱關鍵基礎設施，指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大

資安法規範對象包含公務機關與特定非公務機關，後者包含關鍵設施提供者、公營事業及政府捐助之財團法人，不及於一般民眾。（圖片來源：行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1280）

影響之虞者，例如電力、交通、金融、醫療、水資源、通訊傳播、緊急救援等系統或網路。

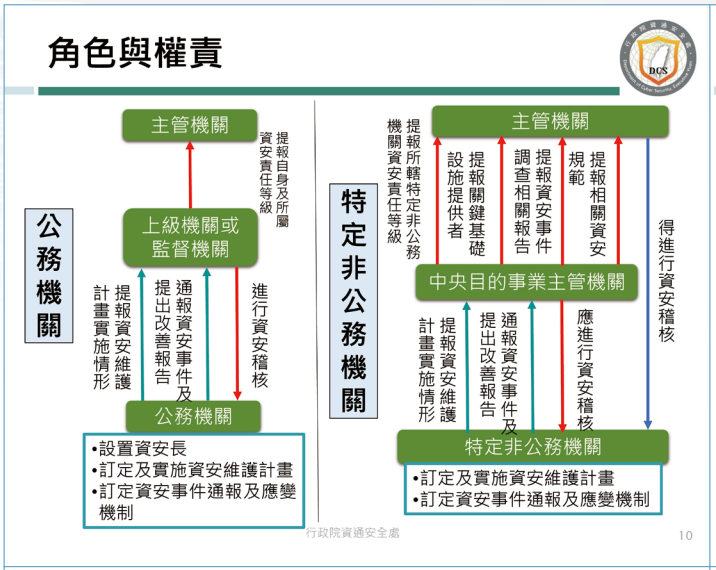
提醒注意者，依據〈資安法〉第 9 條規定，公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

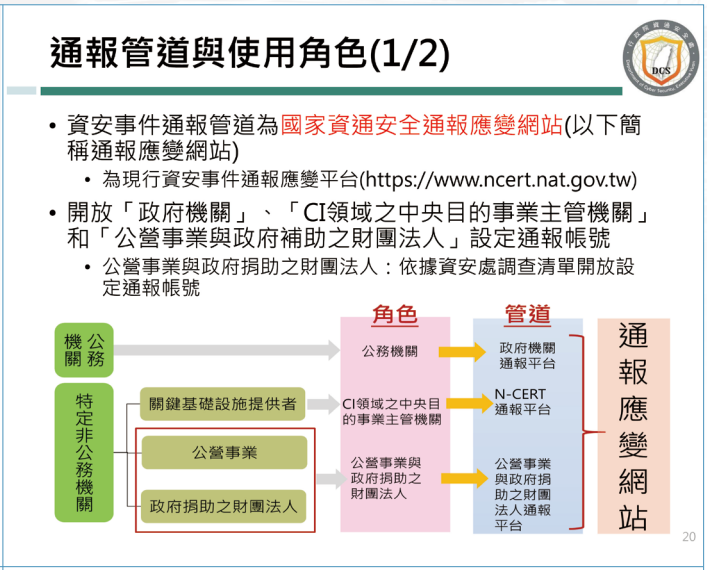
三、應行義務

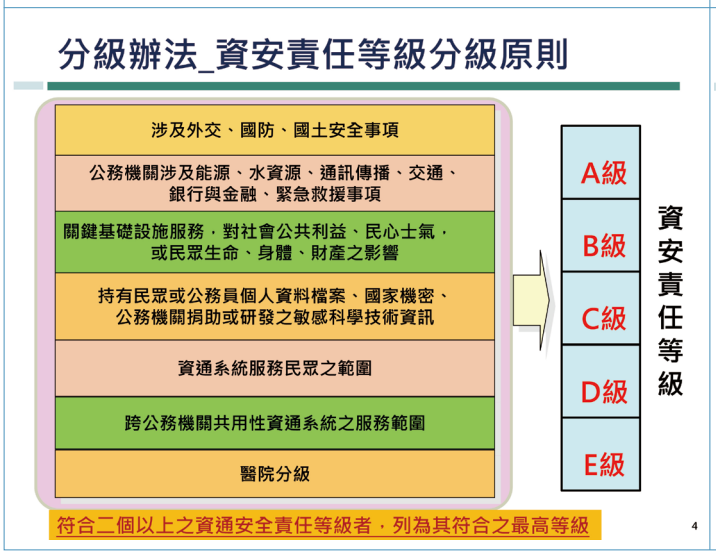
〈資安法〉乃就公務機關、特定非公務機關兩種規範對象分別訂定其相關義務。在公務機關資通安全管理部分，於本法第 10 至 15 條設有明文，重點有公務機關應符合其所屬資通安全責任等級之要求，並考量所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，而《資通安全管理法施行細則》第 6 條則明確列舉資通安全維護計畫應包括之 13 點必要事項；由機關首長指派副首長或適當人員兼任資通安全長，負責推動及監督機關內資通安全相關事務設置；每年向上級或監督機關提出資通安全維護計畫實施情形；稽核其所屬或監督機關之資通安全維護計畫實施情形，受稽機關有缺失或待改善者，應將改善報告送交稽核機關及上級或監督機關，有關改善報告之內容，在《資通安全管理法施行細則》第 3 條明列 4 項必要事項；為因應資通安全事件，應訂定通報及應變機制，當知悉資通安全事件時，除

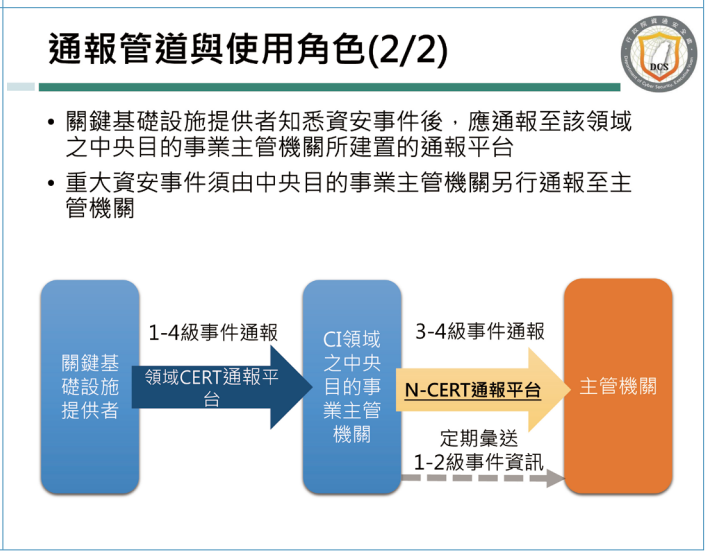
應通報上級或監督機關外，並應通報主管機關，另應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；所屬人員對於機關之資通安全維護績效優良者，應予獎勵。

另在特定非公務機關資通安全管理部分，於本法第 16 至 18 條予以規範，重點首先是中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知；關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫，並向中央目的事業主管機關提出資









資安法分別就公務機關與特定非公務機關明文規定相關義務，並將資通安全責任等級劃分為 5 級，依據不同等級規範應辦事項。（圖片來源：行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/HandoutDetail?lang=zh&seq=1280）

通安全維護計畫實施情形，有缺失或待改善者亦應提出改善報告，而中央目的事業主管機關應辦理稽核；關鍵基礎設施提供者以外之特定非公務機關，比照前述規範訂定、修正及實施資通安全維護計畫，中央目的事業主管機關得要求其提出資通安全維護計畫實施情形，並得辦理稽核；特定非公務機關為因應資通安全事件，應訂定通報及應變機制，於知悉資通安全事件時，應向中央目的事業主管機關通報，並提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。

此外，依據《資通安全責任等級分級辦法》，公務機關及特定非公務機關之資通安全責任等級，係根據業務所涉機敏程度及有無涉及關鍵基礎設施為判斷標準，並將資通安全責任等級由高至低，分為 A、B、C、D、E 等 5 級，且就不同等級在管理面、技術面、認知與訓練等面向，分別規範其應辦事項。

四、相關罰則

〈資安法〉第 19 條規定，公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。

第 20 條明文，特定非公務機關若未依本法訂定、修正或實施資通安全維護計畫；違反資通安全維護計畫法定必要事項；未向中央目的事業主管機關提出資通安全維護計畫之實施情形；未訂定資通安全事件之通報及應變機制，或違反法定必要事項；未向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告；違反有關通報內容之規定，有上述情形之一者，由中央目的事業主管機關令限期改正，屆期未改正者，按次處新臺幣（下同）10 萬元以上 100 萬元以下罰鍰。

另為強化通報機制，第 21 條明定，特定非公務機關未通報資通安全事件，由中央目的事業主管機關處 30 萬元以上 500 萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

結語

由上可知，不論是公務機關或者特定非公務機關，均須界定資通安全責任等級及訂定資通安全維護計畫，方能依法推動資通管理，現雖定有相關法令可供遵循，然而法條內容錯綜複雜，若未瞭解法規、審慎訂定並落實執行，恐失立法美意。申言之，各機關首要之務即是釐清資通安全責任等級及核心業務，因兩者均攸關資通系統之後續安全管理，可說牽一髮而動全身。透過本文，希望協助公務機關及社會大眾認識這套資安專法，並共同為建構完善的國家資通安全環境攜手努力，以避免自身及國家權益遭駭。

LINE來 LINE去，LINE出問題

／鍵盤 007

根據 iThome 於 107 年 3 月間的報導，LINE 用戶已突破 1,900 萬，每天使用 LINE 進行語音通話人數也突破 700 萬，毫無懸念地，LINE 已成為臺灣最主要的社群通訊軟體。舉凡學生喜歡用 LINE 溝通，老師用 LINE 教學分享、指導課業，公務機關亦起而效尤，隨手建立公務群組，藉此橫向連繫、有效溝通。但是每天使用的你，知道它也存在一些「黑歷史」嗎？每天 LINE 來 LINE 去到底會不會出事？其他通訊軟體像是 WhatsApp、Instagram 會不會比較安全？這些疑問從來就沒有消停過！

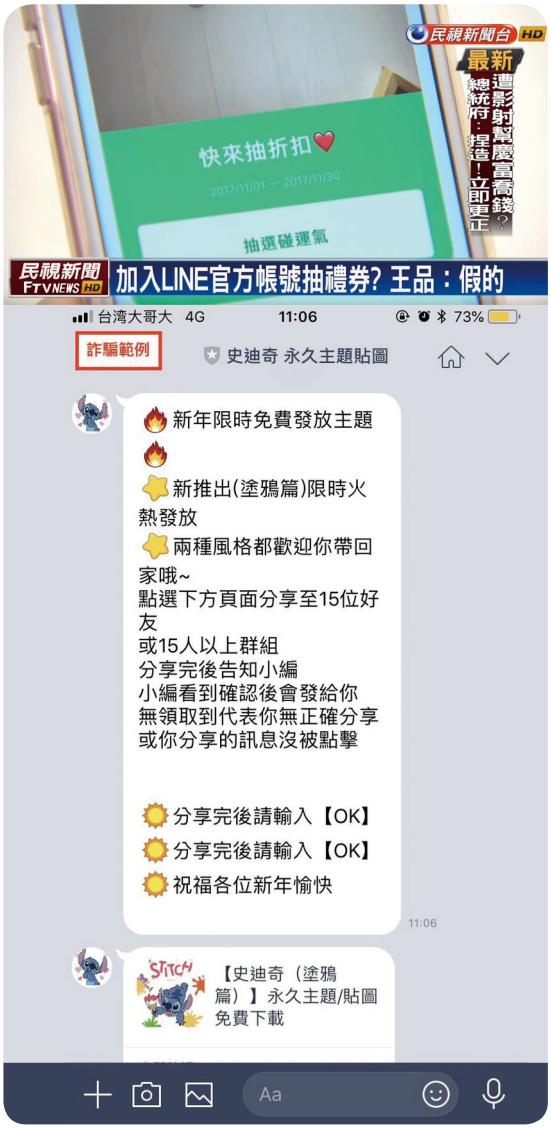
LINE 近期議題

東森新聞於 2018 年 11 月 29 日報導「手誤傳錯群組，潘姓員警被依過失洩密罪送辦，檢方給予緩起訴處分」，內容陳述 2017 年間偵辦擄人勒贖案的潘姓員警，原本要傳「偵辦進度報告」給負責調閱監視器的同事，卻誤傳到反年金改革的群組「台灣憤怒鳥」，該案檢方於 2018 年給予緩起訴處分，需繳交公庫 3 萬元。

LINE 最常遇到的態樣，當屬詐騙集團竊取個資及財務等問題。趨勢科技所屬「資安趨勢部落格」曾指出詐騙集團善於偽造「瘋傳 7-11 限時發送 100 元禮券」、「FamilyMart 送全家千元禮券」等等詐騙帳號，吸引民眾加入好友或點選釣魚網站連結。據趨勢科技防詐達人調查，臺灣前 15 大 LINE@ 詐騙帳號受害品牌店家，以臭跩貓詐騙貼圖排名第一，共有將近 150 組詐騙 Line@ 帳號；而被發現的詐騙帳號中，1/2 為假貼圖，1/4 則透過假冒如星巴克、王品、中油、全聯、7-11、全家等店家假優惠名義引誘消費者上鉤。

其他通訊軟體，像是 WhatsApp、Instagram 等亦存在類似資安風險，例如 iThome 亦指出 WhatsApp 於 2018 年 10 月才修復一項漏洞，該漏洞允許使用者於視訊通話時，讓駭客有機會操控手機程式。

此外 LINE 也成為假訊息散布平台，長輩、朋友間都用 LINE 轉傳不實消息，例如「菌類不能和茄子一起吃」、「柿子加優酪乳會中毒」等，另 107 年 9 合 1 大選之前，LINE 更成為攻擊各候選人的大平台，常有人轉傳「韓國瑜造勢現場發走路工 1,500 元」、「陳其邁辯論會帶耳機」等攻訐候選人不實訊息。



詐騙集團以偽造各種免費貼圖、優惠和抽獎，吸引消費者加入好友或點選釣魚網站，導致民眾財物損失或個資外洩。（圖片來源：截自民視新聞，https://youtu.be/vvNP8WPxlIY；LINE@ 生活圈，http://at-blog.line.me/tw/archives/75713444.html）

LINE 潛藏風險

總結上述各項議題，我們得知 LINE 本身存在許多資安風險，可約略將之分為「操作風險」及「軟體風險」，分述如下：

一、操作風險

1. 如前述案例所載，使用者於公務上可能同時與多群組人員聯繫，稍有不慎，易誤傳公務相關文件予不相干第三人，即使 LINE 具備「訊息回收」功能，也難得知第三人是否已知悉內容。

2. 許多人使用 LINE 未了解軟體具備之功能，像是 LINE 聊天室的「相簿」、「儲存至 Keep」功能等，可將檔案上傳雲端，若不善用而隨意儲存在手機目錄、相簿內，一旦手機誤植木馬軟體等，手上資料恐遭外洩。

3. LINE 若設定不當，允許陌生人加為好友，讓有心人士有可趁之機，偽冒熟識、家人，誘騙點選連結進行 APT（Advanced Persistent Threat）攻擊或交付資料等，均可能引發資安風險。

4. 公務機關人員為求跨部會聯繫提升效率，往往建立許多群組，群組成員間彼此也未必熟識；又尚未在 LINE 群組裡指定管理者時，任何成員均可邀請他人進入該族群內；倘若誤加入非此公務相關人員，將滋生公務資料外洩疑慮。

二、軟體風險

1. LINE 可隨意轉貼及點選任何網址，若是該網址潛藏惡意代碼，手機極可能被植入惡意程式，導致機敏資訊遭竊。

2. LINE 建置雲端資料庫能儲存用戶或群組對話內容及檔案，但若 LINE 公司遭駭客入侵，即可能洩漏用戶或群組之檔案及對話內容，即使循司法調查管道，亦因 LINE 屬國外公司而增加偵辦難度；此外，使用者在通訊過程中亦存在遭 LINE 公司側錄對話內容之風險，故以國安角度考量，確實不宜在機敏公務上使用。

風險防制

一、安裝訊息加解密軟體

若 LINE 群組人員欲傳送公務資料，請務必安裝第三方加解密軟體，例如資通電腦與國家中山科學研究院研發之「ME 通訊

ME 通訊軟體介紹。（圖片來源：截自資通電腦網站，https://www.ares.com.tw/products/ncsist/?_ga=2.250067718.1418945601.1549964666-605880405.1549964666#lineme）

軟體」，透過該軟體對訊息、檔案加密後，再以 LINE 傳送，避免訊息誤傳或訊息遭他人擷取之資安疑慮。

二、「LINE」群組中建立管理人員

透過設定群組管理人，可統籌管理群組成員，必要時可將不適合人員踢出群組，以確保該群組談話內容不外流。

三、持續更新 LINE 版本

LINE 近年持續進行「資安漏洞回報獎金計畫」，用於挖掘軟體漏洞等各項缺失，並於後續版本中修補漏洞，故當 LINE 跳出新版本（電腦版）要求更新時，務必持續更新，避免遺留漏洞給駭客趁機攻擊。

四、安裝防毒軟體

由於 LINE 可傳送各項超連結網址、檔案、圖片等，甚至許多使用者亦安裝 LINE 電腦板，往往給駭客可趁之機，誘騙使用者下載檔案、開啟連結，最終再植入木馬程式。因此若加裝防毒軟體，就可讓防毒軟體進行初步篩選，降低中毒機會。

五、不隨便加好友、加官方帳號

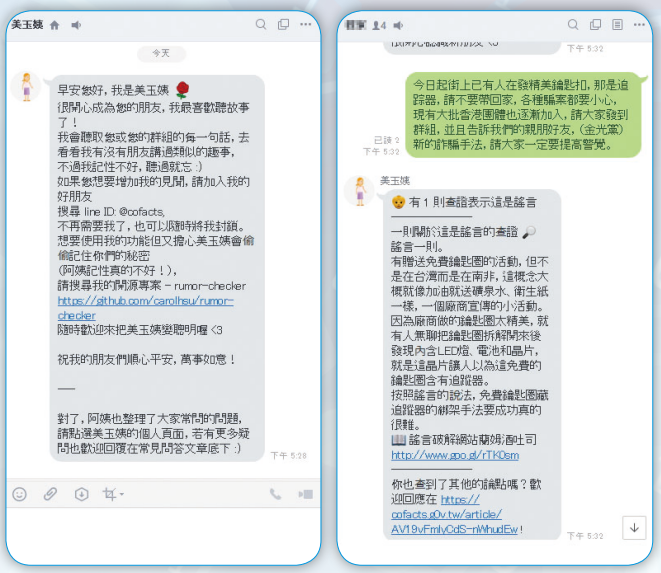
不隨意加陌生人為好友，可點選 LINE「設定」中的「好友」設定，關閉「自動加入好友」、「允許被加入好友」功能，即可避免被色情業者、陌生人士誘騙。另網路上常常充斥各種假官方帳號，建議可利用「趨勢防詐達人」、「刑事局 165 APP」，先查證該帳號是否為「官方正版」後再加入。

LINE「好友」設定。

刑事局 165 反詐騙 APP 和趨勢防詐騙達人。（圖片來源：Google Play，https://play.google.com/store/apps/details?id=tw.gov.cib.app.fraud165&hl=zh_TW；趨勢科技防詐騙達人網站，https://www.getdr.com/）

假訊息防制

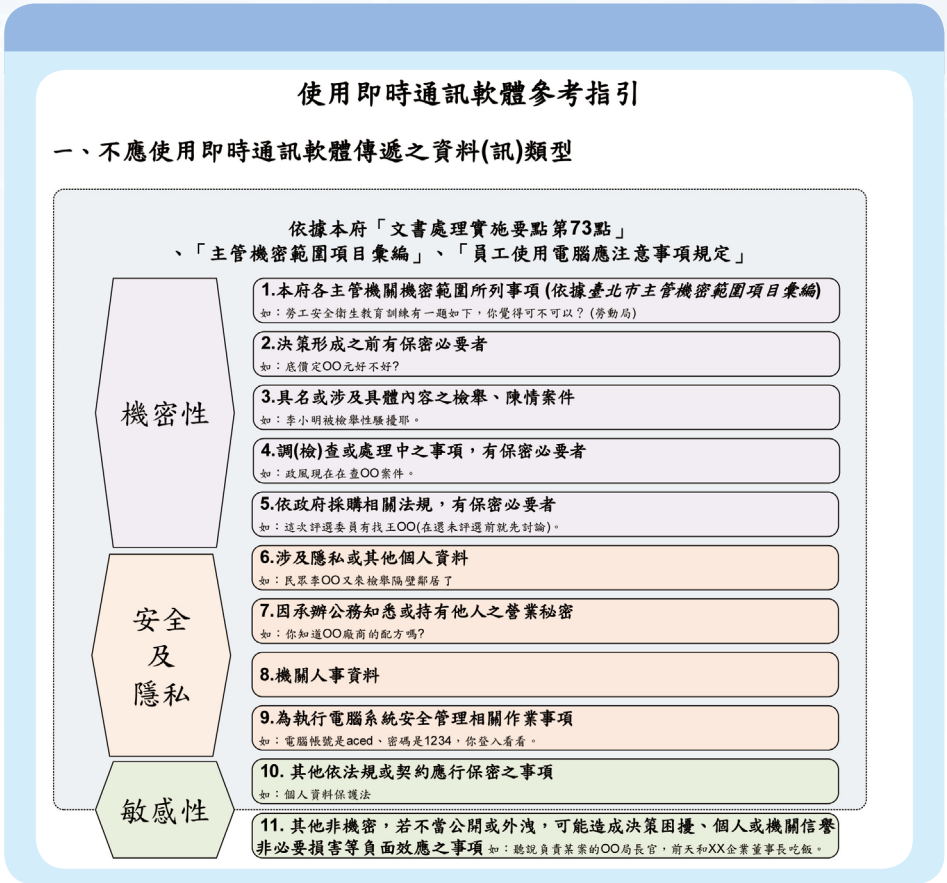
雖然坊間已有不少假訊息查證平台，像是 LINE 帳號「真的假的」、網站「MyGoPen」等，但迄今最方便、最受歡迎的查證管道，當屬「美玉姨」LINE 聊天機器人。使用者僅需將「美玉姨」加入聊天群組，即可以提問方式丟出訊息，讓「美玉姨」直接查證該訊息是否真實；惟「美玉姨」系採擷取使用者訊息並傳送至資料庫查詢運作方式，公務群組若加入「美玉姨」恐有資料外洩之虞。



LINE「美玉姨」及謠言查證結果。

結論

LINE 在臺灣儼然成為生活不可或缺的一部分，公務機關也常藉此開設公務群組，期以「行動辦公室」增進行政效率，然而在享受便利的同時，我們也要明白使用 LINE 所必須承擔的資安風險，盡可能不要在 LINE 上處理公務，倘仍須處理公務，務必考量 LINE 使用上的安全性。您可透過安裝加解密軟體、調整 LINE 操作等預防方式，在最低的風險下，方能享受 LINE 帶給我們的便利。



公務機關透過 LINE 增進行政效率的同時，務必考量 LINE 的安全性。圖為臺北市政府針對 LINE 之使用，所訂定的參考指引。（圖片來源：臺北市政府資訊局，https://doit.gov.taipei/News_Content.aspx?n=6CB3401DAD37F659&s=3284900CC421A8E1）

保密到家：以智慧型手機App為例

／劉俊偉

只要有資訊設備，就會有資安風險。根據國家通訊傳播委員會行動通訊市場數據顯示，截至 2018 年底行動電話用戶數已達 2921 萬戶，智慧型手機已成為現代科技資訊之主流，人人甚至機不離手。然而，除了常見的手機病毒與木馬惡意程式外，使用者更易忽略手機內潛藏之危機— App 行動應用程式，對於此程式之資安管理尚在萌芽階段，並未能掌握風險。您可知當我們在享受便利時，惡質企業也同時在分享你的隱私？

行動應用程式潛存風險

一、App 行動應用程式資安檢測回顧

2017 年由行政院及所屬部會、機關設置的行動 App，共有 144 個潛藏高度資安風險。從清查結果顯示，其中被檢測出有 6 項資安弱點的政府 App 更高達 6 件。國發會當即通知相關機關於期限內完成改善，否則立即下架，以提升資安防護。另 2018 年行政院消保處抽測市面 15 款熱門應用 App 資安檢測，包括線上購物、線上支付、線上訂票及保險業類等，初測結果全數未通過，揭露出不論是政府或私人企業開發之 App 都存有不少的資安風險，顯示手機資安風暴正在成形。

二、手機品牌製造來源分析

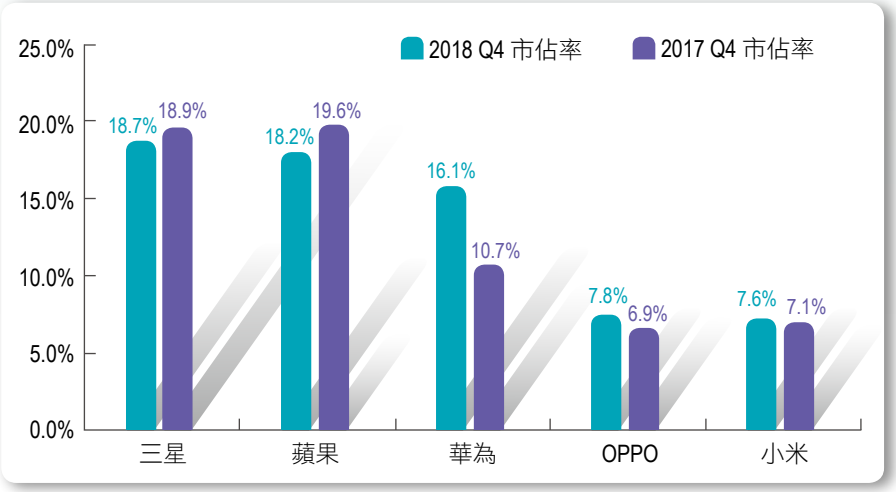
中國大陸手機品牌在全球市占率持續提升，根據 IDC（國際數據資訊有限公司）發布 2018 年第 4 季調查報告顯示，全球智慧型手機出貨量統計為 3.7 億支。依全球手機出貨量來看，目前排名前 5 大的手機品牌，三星仍穩居第 1，市占率達 18.7%，居於榜首。蘋果排名第 2，市占率達 18.2%。原排名第 2 的中國大陸手機品牌華為，受美國打壓影響，市占率降為 16.1%。第 4、5 名，分別為 OPPO、小米，市占率為 7.8% 及 7.6%。綜觀整體數據，陸牌手機已透過低廉價格與豐富功能之特

使用者在下載 App 時，因注意以下事項：

1. 避免安裝來路不明或不需要的 App，只信任安裝來自可靠來源的行動應用程式。
2. 密切注意程式所請求的存取權，不隨意提供非必要隱私權限。
3. 將行動裝置的作業系統更新到最新版，因為更新版本通常也會對漏洞進行修正。
4. 注意 App 實際發揮的功能與請求授予權限項目是否相符。
5. 參考其他使用者的評論，判斷此應用程式的安全性及可用性。

資料來源：行政院消保處

性，漸次拓展全球消費市場，且諸多款式均能支援「北斗衛星導航系統」。該系統於去（107）年 5 月上線，除可提供移動、即時定位和導航，進一步發展智慧城市、物流、自動駕駛等商用外，更透過系統功能性，進行各項情報之蒐集。因此，手機製造來源亦是造成國家資安威脅之一。



2018 第 4 季全球智慧型手機市占率統計，排名前 5 大的手機品牌為：三星、蘋果、華為、OPPO、小米。（資料來源：IDC 國際數據資訊有限公司）

行動資訊服務應有認知與作為

一、周延法律規範與檢測

根據 106 年 7 月 28 日修正之《行政院及所屬各機關行動化服務發展作業原則》，為規範各機關提供之行動化服務應通過經濟部工業局訂定之相關資安檢測規定：「各機關開發之行動化服務應符合個人資料保護法及行政院訂定之政府資通安全管理等相關規定，並通過經濟部工業局訂定行動化應用軟體之檢測項目，始得提供民眾下

華為手機是 2018 第 4 季全球手機出貨市占率第 3 名，而其餘如 OPPO、小米也分別名列第 4、5 名，顯示陸牌手機已透過低廉價格與豐富功能，逐漸拓展至全球消費市場。（Photo Credit: Kārlis Dambrāns, https://www.flickr.com/photos/janitors/16103979223/in/album-72157650786478488）

北斗衛星導航系統可提供移動、即時定位和導航，有利於各項情報之蒐集，去年 12 月中國衛星導航系統管理辦公室宣布開始提供「全球服務」。（圖片來源：中新社／達志影像）

工研院透過內部公告系統通知，1 月 15 日起全體員工禁止使用華為手機、電腦等，國家實驗研究院後跟進公布訊息。（圖片來源：工研院，國家實驗研究院，https://www.narlabs.org.tw/xmdoc/cont?sid=0J0163168622771674 93&xsmsid=0I148622737263495777）

載使用」。其次，為建立績效及資安檢測管考機制：「各機關發展行動化服務應建立績效管理機制，定期檢討服務成效。行政院所屬二級機關應於每年 12 月 31 日前彙整其所屬機關（構）之績效及資通安全檢測報告，送國家發展委員會進行管考」。基此，上揭所增列之官方 App 資安檢測規定，均必須經資安檢測通過後方能上架，同時，亦透過經濟部工業局將檢測服務納入共同供應採購契約，進而讓各個政府機關依需求採購 App 資安檢測服務，確保政府 App 資安防護健全。

二、縝密手機來源管控

根據美國眾議院情報委員會（House Intelligence Committee）早在 2012 年便曾發表報告指出，建議美國企業不要採

國軍對大陸廠牌手機嚴格禁止帶入營區，並於採購契約中明定禁用；另對於其他廠牌智慧型手機，亦需加裝限制功能的軟體，維護資安。（圖片來源：截自東森新聞，https://youtu.be/qfMkoSde1QA；TVBS 新聞，https://youtu.be/6csqXToZ6sw）

用中國大陸業者華為（Huawei）和中興（ZTE）的設備與服務，也要求政府機構直接將華為與中興踢出採購名單。2014 年時華為品牌即被禁止參與美國政府的競標案。對此，美國眾議院軍事委員會在去年 5 月公布 2019 年「國防授權法」（NDAA）法案細節，明確禁止任何美國政府機關使用華為或中興等大陸公司所生產的「高風險」科技產品。

鑑此，美國國防部亦在國家資安風險考量下，認定大陸政府可能會追蹤使用華為或中興通訊設備的美軍行蹤，例如獲悉軍事基地行動，或掌握軍隊何時在基地外集結，故要求軍中販賣部停止販售（或下架）華為、中興通訊兩家陸企製造的智慧型手機。我國軍方在採購方案中亦有明文規定，嚴禁使用中國廠牌的智慧型手機。

結語

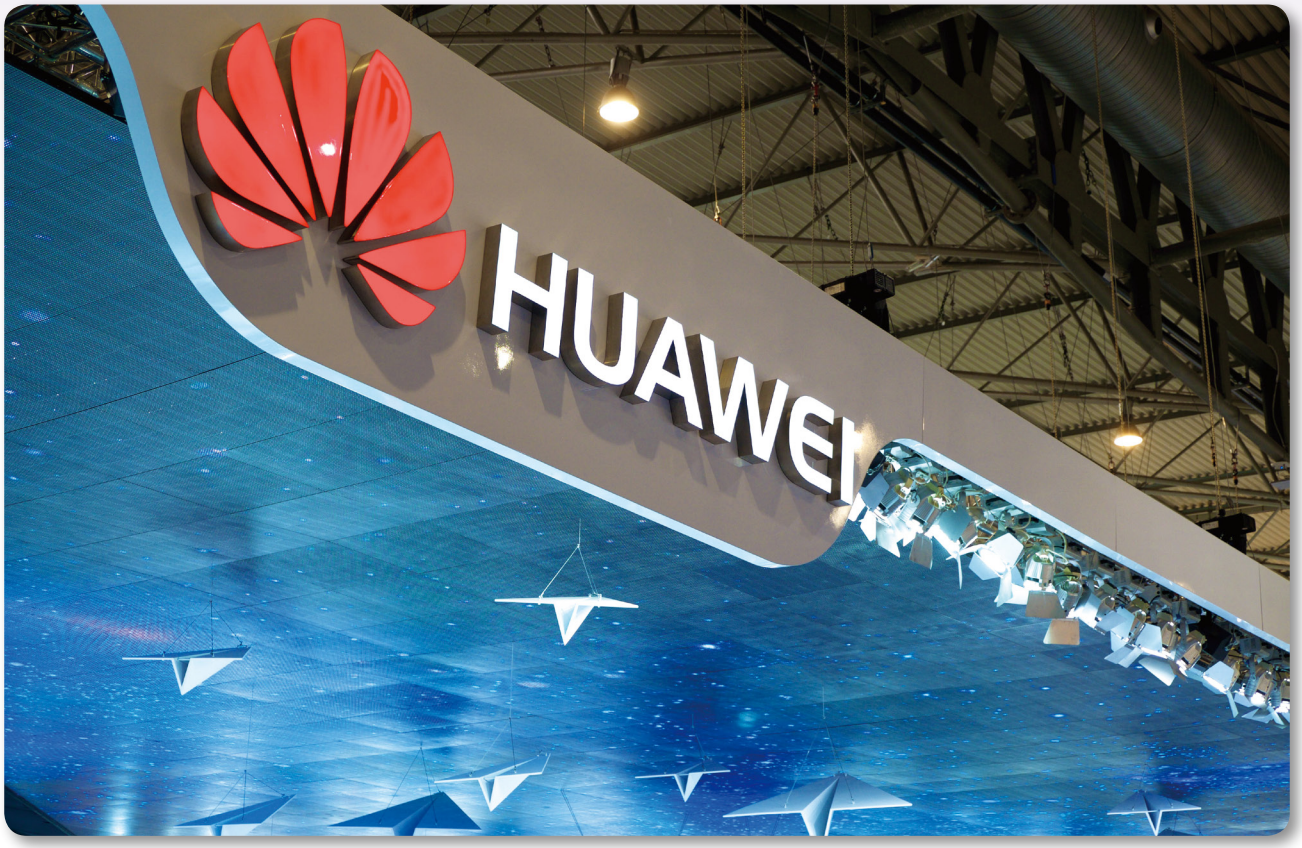
智慧型手機的普及，雖大幅提升日常生活的便利性，但行動裝置卻因防護措施的不健全，已成為全世界政府頭痛的問題。丹麥 TV2 電視臺在 2015 年製作的紀錄片《手機不設防》（Addicted to My Phone），如實闡述了 App 所潛藏之危機與風險，數位世界正以前所未見的速度快速擴張，這意味著網路威脅與攻擊目標也正在各地迅速蔓延。美國總統川普於 2018 年底簽署《網路安全與基礎安全署》法案，將網路安全事務的管理拉高到聯邦層級。歐盟更於今（2019）年 2 月研擬禁用大陸 5G 設備，將修改網路安全法以因應即將鋪天蓋地的網路威脅。因此，智慧型手機的防護與檢測，對我國安而言，更是不容忽視之課題。

紀錄片《手機不設防》，揭露手機與 APP 所潛藏的資安風險及危機。（圖片來源：截自世界公視大展 youtube，https://youtu.be/HnRsvhUuRgw）

手機個資
如何被竊取？

／法務部調查局資通安全處　雷喻翔

美國眾議院情報委員會數年前就曾公布調查報告，指「中國大陸廠商華為通訊所生產的設備，存在追蹤郵件、擾亂美國通訊系統的可能性」，此後阻止華為向美國通訊企業供應相關設備。



華為的通訊電子設備，可能被蓄意設計開後門漏洞，屢遭各國以國家安全考量拒絕採購。（Photo Credit: Kārlis Dambrāns, https://www.flickr.com/photos/janitors/16103977343/in/album-72157650786478488）

延燒國際的資安新聞

華為（Huawei）總部位於中國大陸深圳，以網路通訊設備起家，後來跨足智慧手機市場而闖出名號，近期卻屢遭各國以國家安全考量拒絕採購，指華為的通訊電子設備，可能被蓄意設計開後門漏洞，懷疑北京可能藉此非法收集境外國家用戶的通話內容；去年 10 月彭博社（Bloomberg News）報導，亞馬遜（Amazon）在 2015 年曾打算收購一家串流視訊伺服器業者，但在評估其產品安全中發現其上游的伺服器供應商超微電腦（Super Micro），疑似在組裝過程中遭植入中國間諜晶片，此外蘋果（Apple Inc.）也曾發現相似情形而終止和超微電腦的合約。

究竟我們所使用的通訊設備是否能夠守住使用者的隱私？高舉資訊安全大旗而拒某些通訊品牌於門外是否合理？

什麼是通訊設備？

通訊設備是個廣泛的名詞，從最上游的基地台、路由器、交換器，到使用者終端設備—也就是手機，都是通訊設備的

範疇。每個設備都是由極為精密的硬體（Hardware）晶片、使用者應用程式的軟體（Software）以及中介軟硬體的韌體（Firmware）所組成，任何一個環節都需要數十名至上百名的工程師通力合作才得以使其功能正常運作。正因為其複雜度之高，若在系統埋入具有特殊用途的系統模組，不正如在樹林中藏起一片落葉般難以察覺？

什麼是除錯模組？

程式開發階段由於系統還未穩定，研發工程師 RD（Research & Development）通常需要在原本的功能模組中另外加入除錯模組（debug module），當系統發生問題時能夠蒐集當下的資訊以便日後的分析。以智慧型手機為例，相信讀者一定有這樣的經驗：原本正常使用的手機卻突然毫無預警的關機、總是無法正常啟用某一個應用程式等，因此每間系統商都需要專門進行測試的人員，品質保證工程師 QA（Quality Assurance）應運而生。

除錯模組所扮演的角色就是在問題發生的當下盡可能地蒐集手機系統內的資訊，從手機 IMEI 識別碼、作業系統版號、系統時間、當下系統的記憶體快照等等全部蒐羅，藉由這些資訊讓 RD 可以詳細判讀系統狀態。除錯模組會將所蒐集的資訊存放在手機的內存空間中，等到 QA 完成了所有檢測項目後一次擷取在這過程中所產生的除錯資訊，再將這些重要的資訊傳遞予 RD。為加快軟體開發進程，通常 QA

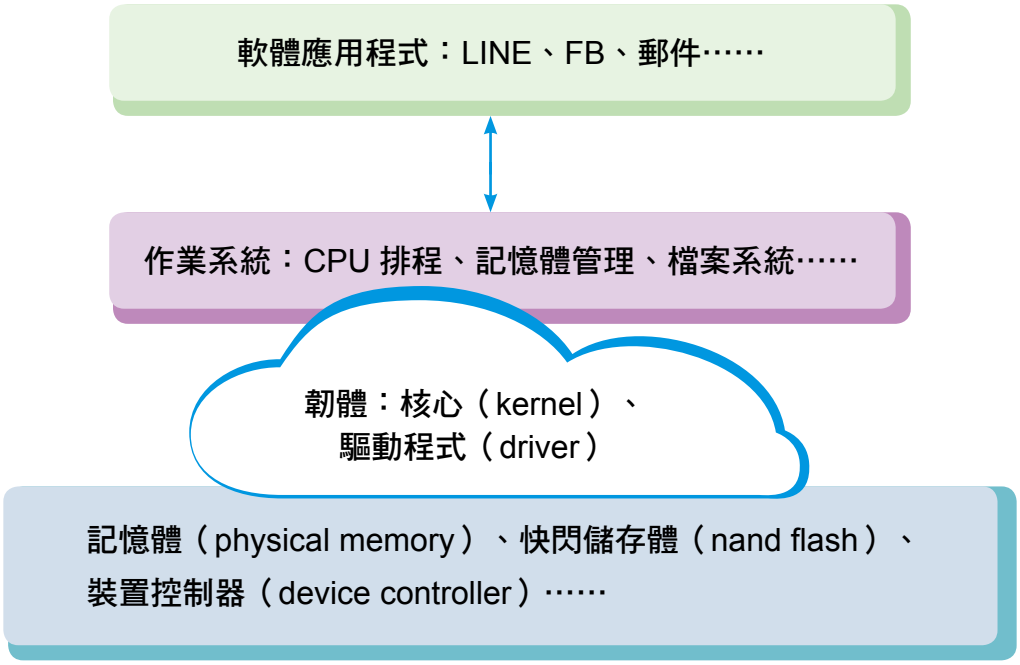
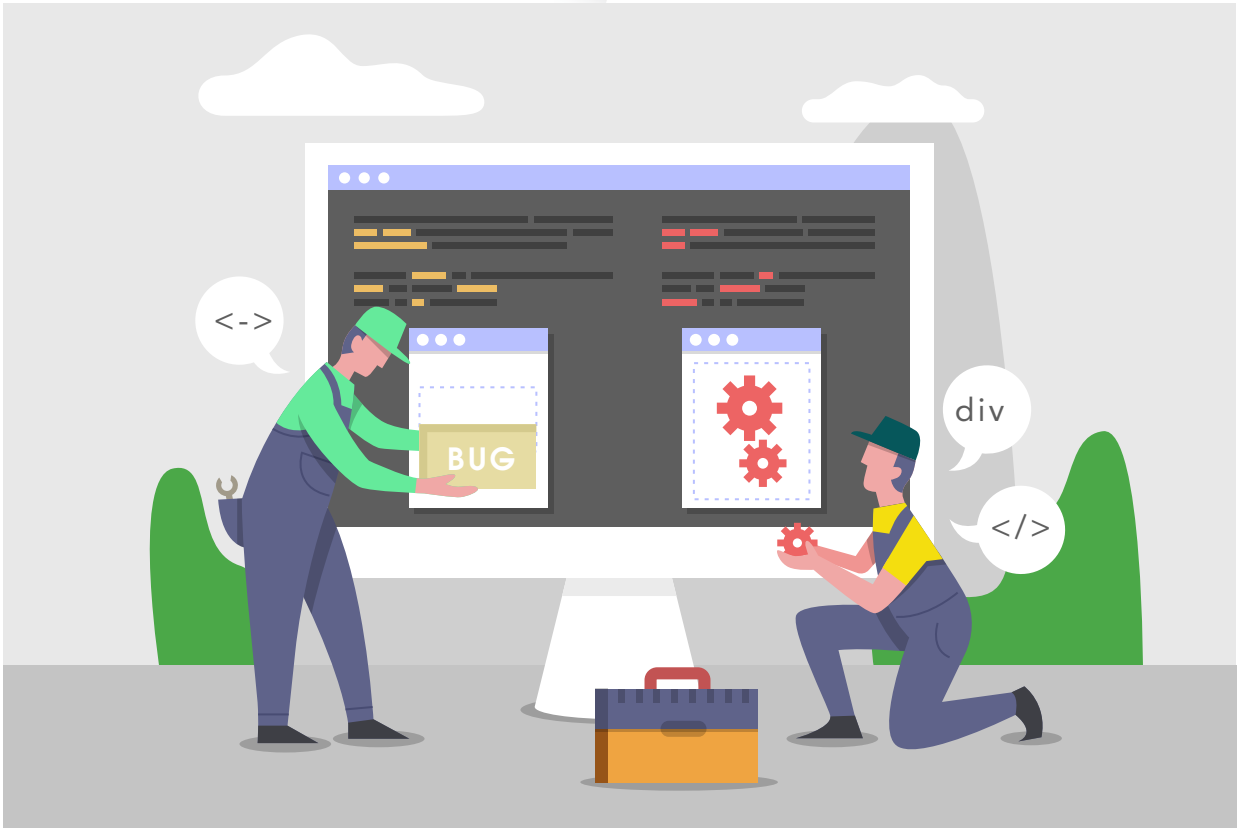


圖 1　通訊設備的基本組成



智慧型手機的系統開發，會經由 QA 檢測完項目後一次擷取除錯資訊，傳送給 RD 掌握問題並解決。

所測試的手機會配載網路 SIM 卡。網路狀況隨著位置的不同各有所異，有時候臺北、高雄兩地所產生的問題就是不同，所以 QA 必須機動性地全臺移動甚至全世界移動。進階版的除錯模組可以在問題發生的當下馬上將資料傳回某一台伺服器，RD 得以第一時間便掌握到系統發生的問題。

當除錯模組化身惡意模組

敘述至此，您是否已聯想到前述的行為跟惡意的駭客在手機中所埋入的後門程式有何分別？其實兩者本質相同，都是將系統中的資訊回傳至特定伺服器的程式碼，差別在於寫程式碼的工程師其主觀意念，究竟這個模組是為了幫助產品的開發，讓其達到盡善盡美的地步？抑或是藉以竊取手機使用者的個人資訊？

正常情況下，除錯模組只限定於開發階段，一旦產品達到上市的品質其將被移除，此模組將不再自動回報相關系統資訊。試著想像一個情境，如果某手機開發商收到一批訂單，從而知道該批下單的手機將用於其他國家的機敏機關，若該手機開發商所處的國家有意從中打探其他國家的內部訊息，那麼在開發過程中於動輒十幾萬行的程式碼中埋入一組惡意模組，似乎也不那麼令人意外。

或許讀者心中有所疑惑：「現在市面有許多應用程式可以找到哪些程式做了你不預期的行為，找到之後將之移除不就行了嗎？」然而系統程式的組成分為韌體及軟體，如果惡意的模組是寫在軟體應用程式層級，可以較為容易地發掘出惡意程式，但如果是寫在韌體之中，那麼事情就不是那麼簡單了。除錯模組是寫在韌體中的核心（kernel），即為程式最底層與晶片介接的部分，無法單獨分離出來，其隱密性不言可喻。

手機是如此，路由器、交換器甚至基地台亦是如此，原本立意良善的除錯模組究竟是為了開發所需或是別有用心僅在一念之間，然而只要是牽涉到機敏議題，為了資訊安全起見，在考慮購置通訊設備的過程中宜三思而後行。

手機、路由器、交換器甚至基地台，都可能因為植入惡意程式的除錯模組而導致資安危機。

Clear Current
15 min

your text goes here #hashtag

Seeing is Believing：「同溫層」效應

／吳旻純

Like Comment Share

在實際的社交群體互動中，你是否覺得找到志同道合、心靈契合的朋友並不容易？但當你打開臉書等社群網站平台時，許多相同興趣及背景的臉友卻熱情地張開雙臂迎接你！此即現代智慧人類的「虛擬生活圈」，在虛擬網路世界尋找自我、尋求認同，進而獲得假性肯定，只接受單一訊息，活在自主性阻斷某些訊息的「同溫層」舒適圈。

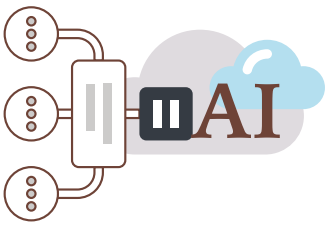
何謂「同溫層」效應？

「同溫層」效應（Echo Chamber Effect）也稱為迴聲室效應、過濾泡泡（filter bubbles），係指社群網站紀錄用戶的使用歷程（瀏覽、按讚、分享、互動等），利用大數據分析導入演算法，依據使用者偏好傳送相關消息，完全阻絕無興趣、負向的訊息，產生一種特定性強化之機制。長時間處於認知制約的氛圍下，每個人越來越封閉在特定社群，只看自己所認同的事實，相信自己所想相信的理念，但一旦跨出認知舒適圈，接觸到真實世界時，自然產生認知衝突，自我建構價值隨之崩潰。

實際上「同溫層」效應在 2016 年因為川普當選美國總統而成為討論話題，選舉過程中，川普的言行跟企業家背景並沒有提高他的選情，而對手希拉蕊擁有高度政治奧援，相對選情穩定樂觀。但川普這種非典型的政治人物，卻透過網路聲量扭轉形勢。

同溫層效應在 2016 年美國總統選舉時成為討論話題，川普透過網路與社群軟體的發散，贏過擁有高度政治奧援的對手希拉蕊。（Photo Credit: Gage Skidmore, https://www.flickr.com/photos/gageskidmore/albums/with/72157674671637971）

紀錄用戶
使用行為



大數據概念
導入演算法

特定強化
同溫層發散

圖 1　同溫層效應擴散歷程

圖 2　同溫層效應之資安危機

「同溫層」效應對資訊安全之影響

每天打開臉書、YOUTUBE 等社群網站平台，開心接收想要的訊息，觀看喜愛瀏覽的影片，深陷在自己打造的舒適圈，其實也讓自己處於資安的危機圈。社群網站會記錄使用者選取、按讚、觀看、分享等行為，進而依據數據分析傳送特定訊息，以灌輸或強化用戶認知與行為，成為另一種行銷策略。但是此種大數據演算機制卻可能被有心人士利用成為資安漏洞（圖 2），當社群平台業者利用收集的數據傳送相關訊息或影音給用戶，駭客可能利用時下當紅議題，製作關鍵字名稱，卻是將內容嵌入惡意廣告或連結，借助平台自動演算跟同溫層效應，致特定使用者點取而被駭或植入惡意程式。

正視「同溫層」效應之危機及策略

同溫層效應的發散可能造成個人認知及資訊安全危機，而面對不同的危機，應正視問題並採取適當的策略，將損失及損害降至最低。

一、個人認知危機

當落入同溫層舒適圈時，若遭遇與自身認知矛盾或是不利的資訊，會產生極不

舒服之感，而這會破壞大腦的穩定狀況，因此會下意識地想要消除這樣的狀態，自主地選擇忽略與過濾掉不被我們所認同的資訊，或用自身偏好的認知去解釋，將資訊合理化。一旦處於這種排除異己，自我感覺良好的氛圍，持續只接收想要的資訊，無法接觸到相反立場的意見，將自動被邊緣化成特定群體，產生難以適應真實社會價值的困難感。

二、資訊安全危機

因為使用者網路使用行為的偏好，透過平台演算機制，放大同溫層效應，使用者不知覺留下使用軌跡，除了變相成為業者置入性行銷的對象，也可能因此洩漏個資，變成駭客攻擊的對象；甚至成為有心人士傳遞特定意識形態、錯誤訊息之手段，以誤導民眾，達到政治或經濟目的。

當落入同溫層舒適圈時，若是和自身認知矛盾或不利的資訊，會破壞大腦的穩定狀況，進而下意識地選擇忽略或過濾掉不被認同的資訊，或將資訊合理化。

落入同溫層效應中，可能造成個人認知與資訊安全危機，不但容易洩漏個資、成為駭客或有心人士攻擊的對象，也可能導致被邊緣化，難以適應真實社會價值。

三、面對同溫層效應之應對策略

（一）擴大取得資訊的管道

網路社群網站或影音平台已經成為許多民眾獲取資訊的主要管道，但由於客製化演算法會隨著時間優化，與本身同溫層意見相左之訊息幾乎不會出現，導致個人認知越來越同化，無法融入真實社會氛圍。所以要脫離同溫層舒適圈最好的方法就是增加取得資訊之管道，尤其是與自身立場不同的意見管道。例如不要專注在單一社群媒體，除了臉書，還可以選擇各類新聞、雜誌等平台，接受多元觀點，來打破本身築起的認知高牆。

（二）聆聽多面向的意見

聆聽不同面向的意見可以修正扭曲的偏好認知，建構更全面的社會價值。因此不妨觀看批評你的留言、閱讀朋友貼文上的評論及養成分享前先閱讀內文等網路習慣。

（三）培養良好網路使用習慣

在使用社群網站平台時，先確認訊息內容的正確性，不要隨便點選置入廣告或連結，以免洩漏個資或被植入惡意軟體，並定期更新系統軟體，提高資訊安全防護力。

結論

身處網路資訊時代，多數的訊息來自於社群網站或平台，我們可以自由選擇自己想要觀看的內容，但也選擇性地忽略不同於己的意見，導致觀點過於狹隘單一。因此所產生的同溫層效應可能會帶來個人認知及資訊安全危機。應正視問題核心，透過擴大取得資訊管道、聆聽多元意見及培養良好網路使用習慣的策略，進而建構更全面的社會價值和包容的社會氛圍。

圖 3　脫離同溫層效應之策略