從風險管理觀點探討惡意 APP 應用程式對國軍之影響－以智慧型手機為例

作者／曾柏元中校

提要

一、智慧型手機日益普及化，加以安裝擴充功能(APP 應用程式)已成為趨勢，雖增添國人許多的便利性，卻常在操作上產生必然之風險，成為網路駭客的工具，無形間引發資安事件。

二、從 2019 年世界經濟論壇中公布年度《全球風險報告》指出，「大規模數據詐欺與竊取」及「網路攻擊」分別被列為排名之第四與第五位，國人無意識網路攻擊手法之氾濫，已直接對軍隊、社會以及國家造成極大風險，實在不容小覷。

三、在 2019 年 3 月蔡總統參加臺灣資安大會指出「資安就是國安」。然而，身為國軍的一份子，應時時警惕自我，勢必將成為中共網軍攻擊對象。因此，在資安風險管理更須落實。

四、本文試藉 APP 應用程式的風險分析，使國軍更能重視智慧型手機軟體下載的危害與防制，再從官兵需求與資安管理上，尋求適切的平衡點。

關鍵詞：風險管理、APP 應用程式、智慧型手機、資訊安全。

前言

近年來，智慧型手機和 APP 應用程式(Application, 以下簡稱 APP)[1]對資訊產業的發展與應用上，可說是越來越廣泛與普及，尤其現今只需運用智慧型手機，便可輕易提供個人多元性之服務，確實給予國人增加不少便利性。相對「水能載舟 亦能覆舟」，此話意旨兩者之間，有「正面」與「負面」的影響程度。

根據資安公司賽門鐵克在 2017 年指出，我國個資外洩全球是第五，亞洲則為第一。另外，《華爾街日報》一篇專欄〈你的 App 正在監視你(Your Apps Are Watching You)〉中，透露出 iPhone 和 Android 作業系統遭受惡意應用程式入侵，使用者在隱私權易被竊取與濫用，以致於發生身心與財務上之損失。[2]本文希望從上述資安事件報導，從風險管理角度去觀察國軍在 APP 的運用，再藉由風險分析、評估與管控等手段，將資訊管理風險(Management Of Information Risks)降至最低。

---

[1] 行動應用 App 指一種設計給智慧型手機、平板電腦和其他行動裝置使用之應用程式，本文中亦簡稱「行動應用 App」。

[2] 〈台灣個資外洩亞洲之冠〉，《今週刊》，https://www.cna.com.tw/news/firstnews/201909130056.aspx，2017 年 5 月 18 日，(檢索日期：民國 108 年 11 月 20 日)。

風險管理與 APP 應用程式之關聯性

面對資訊化時代，下載 APP 應用程式已成為無法回頭的趨勢，卻也帶來「資安風險」存在於國人日常中。況且國軍身為社會一份子，勢必也會面臨此相關議題，必定也將它列為高風險的管理重點。

一、 風險與風險管理的意涵

從 20 世紀 30 年代開始風險(Risk)概念就已逐漸萌芽，直至 80 年代末被學界重視進而廣泛運用。[3]依據韋氏字典(Webster's unabridged dictionary, 1970)對風險[4]所下之定義，係指「傷害、損害或損失的機會」，進而歸納出「風險」的核心意義：不確定性、發生的機率、事件的影響。再者，從 2002 年丹尼爾(Daniell)學者的解釋認為，我們是位處在風險高升、劇烈變動的世界。[5]說明人們隨時隨地都處於風險之中。因此，確認「可接受」之風險就顯得格外重要。

然而，風險管理(Risk Management)於 1931 年由美國企業管理協會(The American Management Association, AMA)保險部門首先提出，但至 1957 年美國保險管理協會(The American Society of Insurance Management, ASIM)才開始凸顯風險管理的觀念與重要性，[6]其中敘述風險管理流程與規劃，著重於事前的預防。另外，可從 2004 年英國副首相辦公室出版的風險管理《技術手冊》中，它將風險管理定義為控制風險的作法與步驟，包括辨識風險、評估風險、發展處理方案、監督風險及記錄風險等相關作法，[7]其主要原因在於達到三項作用：

(一)是損失事故發生前，預防損失。

(二)是損失事故發生時，能夠減輕損失。

(三)是損失發生後，彌補損失。[8]

因此，從以上闡述中可理解風險管理的重要性，而本次研究內容以資安風險為主，諸如駭客入侵、電腦病毒、資料外洩等。使國人瞭解「萬物皆連網，萬物皆可駭」的道理，漸以重視資訊安全管理，進以降低資安事故發生性。

二、 智慧型手機與資訊安全風險

TeamT5 杜浦數位安全公司執行長蔡松廷認為:「資安是一種風險管理，沒有絕對的安全，

---

[3] 陳嘉智，〈風險管理理論綜述〉，《經濟綜述》(廣東廣州)，第 6 期，華南理工大學工商管理學院，2008 年 6 月，頁 278。

[4]「Risk」一詞源起根據法國的語源學字典，弗朗索瓦·埃瓦爾德(Francois Ewald)將詞追溯到法文"Risque"，並將它置放於海上貿易。指的是海上航行與活動可能發生之險難(例如風暴)。劉傑雄，〈風險的基本概念〉，http://webcache.googleusercontent.com/search?q=cache:6avcNTdiRmQJ:laukithung.com/pdf/a9.pdf+&cd=28&hl=zh-TW&ct=clnk&gl=tw，2007 年 5 月 27 日，(檢索日期：民國 108 年 11 月 20 日)。

[5]〈風險管理基礎理論與文獻探討〉，http://140.119.115.26/bitstream/140.119/35505/6/32804106.pdf，(檢索日期：民國 108 年 11 月 20 日)。

[6] 胡智明，〈奠基於遊戲樹理論之戰場風險管理〉，《致遠資管學刊》(臺南縣)，第 2 期，致遠管理學院知識管理與出版中心，民國 97 年 7 月，頁 79。

[7] 魏秋水，〈風險移轉模式之建構〉，中華大學科技管理研究所博士論文，民國 97 年 7 月，頁 13。

[8] 張琴、陳柳欽，〈風險管理理論沿襲和最新研究趨勢綜述〉，《河南金融管理幹部學院學報》(中國河南省)，第 5 期，河南金融管理干部學院，2008 年，頁 23。

也沒有永遠攻不破的系統。」[9]此句可鏈結至智慧型手機近期所面臨的高風險威脅，例如：透過簡訊、電子郵件、網頁瀏覽、藍牙、記憶卡等途徑產生資安風險。此外，再以丹麥 TV2 電視臺在 2015 年製作《手機不設防(Addicted to My Phone)》的紀錄片為例，內容中介紹一款免費手電筒 APP 是由丹麥大學生所製作，權限設定與臉書相同(可獲取得相片、簡訊、話筒、全球衛星定位系統(Global Positioning System, GPS)定位等訊息)，上架後供路人下載試用。[10]發現受試者輕易接受隱私條款，成為資安受害者，從案例中闡述惡意 APP 所潛藏危機與風險。[11]筆者則以 2018-2019 年惡意 APP 所導致資安事件，證實智慧型手機、APP 與資訊安全風險三者間的關聯性。(如表一)

表一 2018-2019 年智慧型手機 APP 應用程式資安問題

項次	報導者	報導時間	報導內容	資安性質
1	紐約時報	2018 年 1 月	Google Play Store 應用商店已超過約 2 百多款的應用程式與遊戲 APP，可將手機麥克風開啟對背景進行監聽行為。	授權與連線管理
2	騰訊社會研究中心、DCCI 網際網路數據中心	2018 年 1 月	《2017 年度網絡隱私安全及網絡欺詐行為分析報告》在影音娛樂、資訊閱讀、網路遊戲和常用工具等手機應用程式，成為越界隱私的重災區。	敏感性資料保護
3	新華社	2018 年 1 月	手機應用軟體存在侵犯使用者個人隱私的問題，工信部信息通信管理局約談百度、支付寶、今日頭條等公司，要求企業立即進行整改。	敏感性資料保護 授權與連線管理
4	華爾街日報	2018 年 7 月	Google 允許第三方開發者存取數以百萬計 Gmail 使用者的電子郵件資料。	授權與連線管理
5	中消協	2018 年 8 月	《APP 個人信息洩露情況調查報告》，超過八成受訪者都曾收到推銷電話或簡訊的騷擾，約有 1/3 的遭遇信息洩露後，均會「自認倒霉」。	敏感性資料保護
6	Google 工程部副總裁史密斯	2018 年 12 月	Google 啟動「閃光燈計畫」，稽查第三方開發商，結果發現 Google+應用程式介面存有重大漏洞。	敏感性資料保護
7	德國之聲中文網	2019 年 3 月	GDI 基金會研究員報導，位於深圳的深網視界科技有近 260 萬筆中國新疆自治區的個資外洩；資料庫數據顯示居民近 670 萬筆坐標定位。	敏感性資料保護

[9] 鄭閔聲、陳虹宇，〈指尖上的防衛戰〉，《今周刊》，https://www.businesstoday.com.tw/article/category/154768/post/201907310022，2019 年 7 月 31 日，(檢索日期：民國 108 年 11 月 20 日)。

[10] 〈「同意條款」不設防？小心手機 APP 洩個資〉，《TVBS NEWS》，https://news.tvbs.com.tw/local/687768，2016 年 11 月 20 日，(檢索日期：民國 108 年 11 月 20 日)。

[11] 〈保密到家：以智慧型手機 App 為例〉，《清流月刊》(新北市)，第 20 期，法務部調查局，民國 108 年 3 月，頁 15-19。

8	卡巴斯基	2019 年 8 月	「時代週刊」將 CamScanner 掃描程式，列為最好用的手機程式之一，但內含有「Trojan-Dropper. AndroidOS. Necro. n」木馬病毒，可被用來播放侵入式廣告，或替使用者註冊付費服務等。	身分認證 付費資源控管

資料來源：作者蒐整。

針對上述相關資安報導，發覺惡意 APP 主要在竊取「敏感性資料保護、身分認證、授權與連線管理安全與付費資源控管」等「權限」[12]。此現象勢必會對現今社會造成資安管理上的衝擊，顯然也會對國軍的資安問題造成影響與挑戰。凡此種種，皆突顯「資訊安全與犯罪」已是全球性須即刻處理的重大議題。

三、 國軍官兵在 APP 應用程式之運用

在 2017 年資策會產業情報研究所調查顯示，國內 APP 使用者行為有 63%的民眾，下載數都維持在 15 個以內，且主要分布類型於「通訊(77.9%)」、遊戲(64%)、網路購物(46.2%)、交通運輸(40.7%)、照片與視訊(40%)」等項次為主。[13]另財團法人臺灣網路資訊中心公布「2018 年臺灣網路報告」中，強調我國在行動上網率位居亞洲國家第三名(76.9%)，且智慧型手機是主要的上網行動裝置。[14]上述報導顯示，我國在智慧型手機與 APP 的運用上均維持較高的使用率，舉凡食、衣、住、行、育、樂都需仰賴它，已成為國人民生必需品。

然而，國軍身為社會一份子，部隊官兵廣泛下載 APP 應用於個人休閒或部隊事務上，也是常有耳聞之事，例如像通訊類、地圖交通類、購物類、影音類與遊戲類等，是各級單位無法制止與防範。下述針對目前軍隊主要下載 APP 運用實施概述。

(一)通訊類

以社群、通訊為主要，在於訊息的傳遞，在平時回報制度、建立互助通聯機制等，發佈最近動態與臉書打卡，例如：LINE、WhatApp、微博、Facebook。

(二)地圖交通類

運用在部隊移防訓練之路線勘查、現地戰術地形偵查。例如：Google 地圖、Waze、樂客導航王。

(三)購物類

可隨時在營區內選購商品，添購於連隊事務運用。例如：蝦皮購物、momo 購物網、國軍福利讚 APP。

---

[12] 「權限」依照保護層級，可以分為正常(Normal)、簽名(Signature)和危險(Dangerous)權限，其中危險權限涵蓋應用程式需要涉及用户私人訊息的資訊或資源的區域，或者可能會影響用户儲存的資訊或其他應用程式的操作，例如通訊錄、相機、地理資訊、錄音、簡訊等等。

[13] 〈【APP 使用者調查】遊戲、網購、交通運輸 APP 崛起〉，《MIC.產業情報研究所》，https://mic.iii.org.tw/IndustryObservations_PressRelease02.aspx?sqno=466，2017 年 3 月 29 日，(檢索日期：民國 108 年 11 月 14 日)。

[14] 〈台灣手機購物比例偏低，剁手族都跑去哪下單？〉，《數位時代》，https://www.bnext.com.tw/article/51904/10-percent-taiwenese-consumer-shopping-on-mobile，2019 年 1 月 11 日，(檢索日期：民國 108 年 11 月 15 日)。

(四)影音類

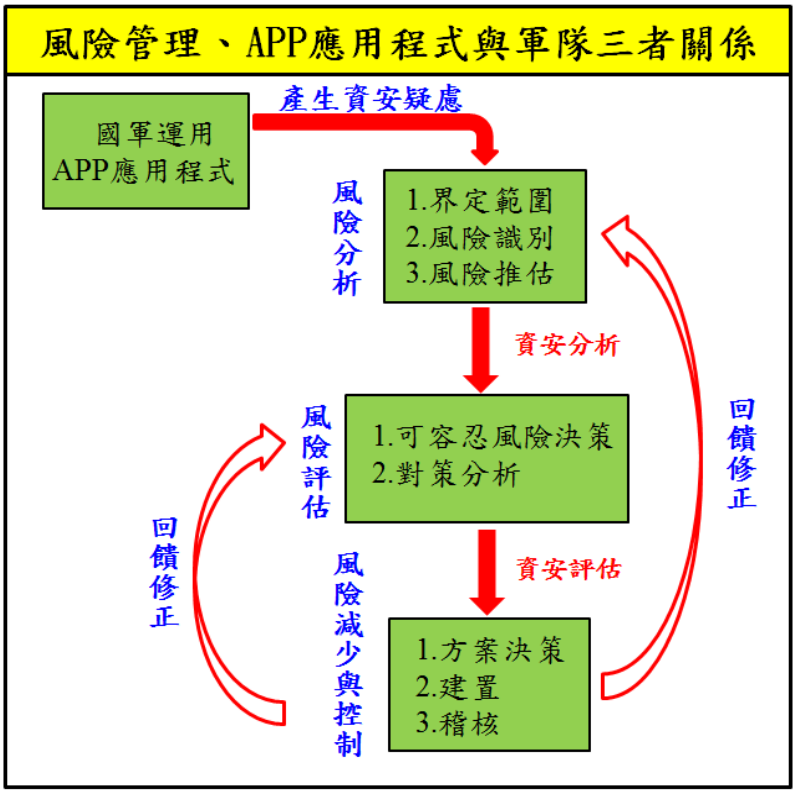
在營區內下載影片或音樂，供官兵放鬆心情或學習等，例如：Youtube、優酷、愛奇藝。

(五)遊戲類

現今遊戲設計類型多種(角色扮演、休閒、策略等)，可配合營區內之零碎時間，以娛樂自我和紓解壓力。例如：Pokémon GO、Garena 極速領域、從零開始的魔王。

綜合上述國軍官兵應用情形，可見均來自於它的實用性、獨特性與創新性，且可滿足官兵生理與心理需求，視為正面影響。反之，若從風險管理角度觀察，一旦官兵下載惡意 APP 應用程式，可能將會衍生出眾多負面問題，更易造成國安議題。因此，須先行判斷風險管理、APP 應用程式與軍隊三者之關係，在分析當前所隱藏之資安風險，以防制可能遭遇之各種災害。(如圖一)

圖一 風險管理、APP 應用程式與軍隊



資料來源：作者繪製。

「APP 應用程式」對國軍資安保密之安全威脅

在 2019 年世界經濟論壇(World Economic Forum)發布年度《全球風險報告》指出，「大規模數據詐欺與竊取」及「網路攻擊」分別被列為第四及第五位。[15]間接說明 APP 已開始對國家、社會至軍隊都造成極大風險，實在不容小覷。

一、「APP 應用程式」主要應用介紹

[15] 〈新型態網路戰 我們準備好了嗎？〉，《經濟日報》，https://money.udn.com/money/story/5628/3815461，2019 年 5 月 16 日，(檢索日期：民國 108 年 11 月 20 日)。

在應用程式市場中若不衡量中共極權制度管理，全球最大行動 APP 商店(Application Store)應屬「App Store」與「Google play」(如圖二)，兩項分由智慧型手機中的 iOS 與 Android(安卓)作業系統獲取。通常取得各項 APP 的途徑，下載流程是經由：確認官方市集→閱讀介紹與評論→閱讀授權原則→獲取 APP 程式運用。以下針對「App Store」與「Google play」各性質實施簡介。

(一)App Store 與 Google Play 介紹

1.「Google Play」

為 Android 作業系統所開發的數位化應用發布平台，它為官方應用商店，其中包括數位媒體商店。Google 為維護整體系統的安全性及完整度，只要通過 Google 許可，才能在產品裝置上安裝 Google 服務框架和 Google Play。

圖二 App Store 與 Google Play 圖示

資料來源：作者繪製。

2.「APP Store」

是屬於 iOS 系統內建，由於 iOS 系統不支援「第三方軟體」，若要開發新型應用軟體須經由 Apple 公司審核。使用者要下載或購買 APP，需登載「Apple ID」此帳戶以做識別，是為安全保護之一環。

3.「Google Play 與 App Store」下載方式

(1)開啟「Google Play」(或 App Store)下載。→(2)請由 Android OS 終端的「Google Play」(iPhone、iPad 和 iPod touch 上開啟 App Store)→(3)瀏覽或搜尋要下載的 APP→(4)按一下該 APP。→(5)然後按一下「購買 APP」。(如有價格)，請按一下「取得」，然後按一下「安裝 APP」。

(二)「Android」與「iOS」對 APP 審認差異比較

App Store 與 Google Play 分別屬於不同作業系統，相對兩者在 App 審核機制會有所差異。由 Google 所主導之 Android 為開放源代碼，在審查時間僅需數小時即可審認通過，審核方式以採取自動掃描。然而惡意軟體可輕易避開安全審查，趁虛而入的機率較高，易造成使用者資安風險，例如「隱私與安全」，主要在於開放權限問題。[16]

[16] 〈要求多餘權限？小心 app 竊取個資〉，《新頭殼》，https://newtalk.tw/news/view/2018-01-06/109553，2018 年 1 月 6 日，(檢索日期：民國 108 年 11 月 20 日)。

反之，iOS 的 App Store 對開發商限制性較強，在上架前須逐一進行安全掃描，審查耗時甚鉅，且會監控程式原始碼，以防範惡意程式上架。此外，APP 必須使用 Apple 公司中央控管的憑證進行簽章，不可使用第三方憑證。因此，罕有惡意程式。[17]但從 2019 蘋果開發者大會(WWDC)中，經營高層提到每週審核的 10 萬個 APP 中，高達四成無法上架，其中多數是因資安疑慮。[18](如表二)

再者，根據學者 Mamdouh Alenezi 於 2017 年在電機電子工程師學會所發表之研究顯示，高達約八成的 Android 系統手機 APP，都過度獲取授權，要求使用者運作時，同意取得非必要之權限，[19]上述驗證 Android 系統的審查機制較為寬鬆。另外，從環球網路及端點安全廠商 Sophos 在其 2020 年威脅報告中顯示：「在過去的一年中，我們已經觀察到犯罪分子針對智慧型手機所有者使用的移動攻擊類型的多樣性和可變性。」，而最大風險是惡意軟體。[20]其中，說明確實存有風險性的許可授權類型，更以具開放性的 Android 系統被監視的風險性最高，佔比達 89%；iOS 系統則佔比達 39%。以上說明兩個系統雖均審核，但都可能遭惡意軟體上架，並沒有所謂的 100%安全系統。

表二 iOS 與 Android 差異性

名稱	iOS	Android
作業系統	類 UNIX 當作基礎的作業系統	Linux 為基礎的作業系統
發布平台	App Store	Google Play
內容規定(含分級)及審查	已訂定內容規範供外界實施參考，並且事先逐一審查 APP 及分級，上述共區分為 5 個級別。(不允許應用程式、4+、9+、12+與 17+)	已訂定內容規範提供外界實施參考，不事先審查 APP 程式，開發者須自行分級。且須經由主動檢舉才會啟動機制，較屬於被動審查。分級別為 4 級。(年齡成熟度不限、低、中、高等)
屬性	封閉性	開放性
開放性	否	開放第三方市場
自律機制主要爭議	事先審查 App 的效率低落	若發覺有惡意、技術上、擅自使用盜取資料、遠程操控或盜版的 APP 上架，會主動實施刪除，但也因時間耗費過長常遭反應。

資料來源：楊佳學，〈讓自律先行，分級從網路素養做起行動應用程式(App)強制分級可行性評估〉，《NCC NEWS NATIONAL COMMUNICATIONS COMMISSION》(臺北市)，第 7 卷第 6 期，國家通訊傳播委員會，民國 102 年 10 月，頁 14。

[17] 黃建隆，〈行動裝置 App 之安全導覽〉，《財金資訊季刊》(臺北市)，第 79 期，財金資訊股份有限公司，2014 年 7 月，頁 38。

[18] 〈導入 APP 資安檢測 打造企業安全防護牆〉，《商周》，https://www.businessweekly.com.tw/focus/indep/38870，2019 年 7 月 11 日，(檢索日期：民國 108 年 11 月 20 日)。

[19] 〈手機 App 資安黑洞！讓蝦皮和 YouTube 讀你的簡訊和通訊錄，你也按下「同意」了嗎？〉，《獨立評論》，https://opinion.cw.com.tw/blog/profile/463/article/7961，2019 年 4 月 18 日，(檢索日期：民國 108 年 11 月 20 日)。

[20] Zak Doffman, “Google Confirms Play Store Security Threat: Here's The Fix-But Does It Make You Safer?” https://translate.google.com/translate?hl=zh-TW&sl=en&u=https://www.forbes.com/sites/zakdoffman/2019/11/10/google-confirms-play-store-security-threat-heres-the-fixbut-does-it-make-you-safer/&prev=search, (2019/11/20).

二、APP 應用程式潛在風險與分析

不論是 iOS 或 Android 作業系統，下載 APP 擴充功能已是智慧型手機必備生活條件，凡是接收郵件、閱讀新聞、使用地圖系統或造訪社交網站等各項活動運用，均可能發生「隱私」與「方便」間的選擇，間接引發其他潛在的資安風險。

(一)APP 應用程式之風險分析[21]

APP 的資訊架構，相較傳統系統更為複雜，且承載更多機敏性資料，舉凡如個資、交易(通訊)資訊與 GPS 定位等等，以上均為時下最常應用的資訊。但常因使用者對安全認知有限，且企業開發商均以程式功能性為優先考量，資安管控易遭受忽略，就易引發資安風險，而經評估潛在風險因子，大致分述「人」、「物」與「網路環境」實施探究：

1.「人」的風險

據統計人是資安防護鏈中最弱的一環，意旨是「操作風險」，就是操作或管理之疏失，[22]人們因 APP 的「功能需求」與「免費機制」導致慾望難以控制。加上開發商可蒐集使用者需求訊息，順勢推出瀏覽器與遊戲等，形成完整的產業鏈，進而誘導實施下載。若一旦未詳閱程式使用條款，即按下同意，將會成為「提供免費軟體之名，行獲取權限之實」。上述說明大多數人的資訊安全意識都太過於薄弱以求方便，卻往往造成無法挽救之風險。

2.「物」的風險

主要是指惡意軟體，亦是「軟體風險」。因為 APP 漏洞問題複雜且變化性高，其實跟網路釣魚攻擊類似，駭客可以利用社群媒體來散播惡意軟件，以社交工程手法，誘騙使用者下載安裝手機應用程式，並同意特定存取功能，進而竊取手機資料。例如：2018 年 1 月，網路公布手機間諜軟體 Skygofree，該軟體就能記錄周遭聲音、側錄鍵盤及竊取裝置上的 LINE、WhatsApp 或 Facebook 之訊息記錄。[23]

3.「網路環境」的風險

依據學術研究預測，至 2020 年全球有五百億筆資料在網路中流通，藉由網路空間交換、取得及蒐集資料。[24]說明網路世界中，已沒有絕對隱私，例如：許多應用程式常會設置與臉書(Facebook)帳號連結的功能，便於快速登入。此種登入方式可能帶來風險，包括個資被第三方應用程式取得、個資用途不明、遭駭客入侵。[25]

---

[21] 何謂風險分析：透過系統化方式，尋求業務流程相關之資訊資產於風險準則中所定義的風險評估條件，並用「定性」方式得出資訊資產風險等級。參考〈法務部及所屬機關資訊安全風險評鑑管理規範〉，《植根法律網》，民國 105 年 11 月 15 日，http://www.rootlaw.com.tw/LawContent.aspx?LawID=A040090021044500-1051115，(檢索日期：民國 108 年 12 月 19 日)。

[22] 陳姿陵，〈運動手環 APP 洩漏你的行蹤〉，《清流雙月刊》(臺北市)，第 15 期，法務部調查局，2018 年 5 月，頁 45。

[23] 〈手機間諜軟體分析—以 Skygofree 為例〉，《MIFR》(臺北市)，第 1 期，財團法人台灣網路資訊中心，民國 107 年 2 月，頁 12。

[24] 陳鈺津，〈網路沒有距離，也沒有祕密〉，《清流雙月刊》(臺北市)，第 18 期，法務部調查局，2018 年 11 月，頁 55。

[25] 〈App 採臉書帳號 資安業者：蒐集個資三大風險〉，《大紀元》，http://www.epochtimes.com/b5/19/3/1/n11081706.htm，2019 年 3 月 1 日，(檢索日期：民國 108 年 11 月 20 日)。

從上述可知「風險」均屬於內部的攻擊威脅，則有人為的非授權存取與破壞、系統存在的漏洞利用等。但其中隱藏許多資安，漏洞與後門程式，是可輕易產生隱私安全問題。從 360 網際網路安全中心發布《2018 中國手機安全生態研究報告》指出，目前約有 89.69%的 APP 都具有濫用使用者通訊錄權限的情況。[26]從比例得知獲取過度權限是為高度風險。再者，從政府管理機制探究，手機內建 APP 是歸屬國家通訊傳播委員會(National Communications Commission, NCC)所管控；商業性 APP 則由經濟部工業局管理，以上兩者性質均概同，卻分屬兩個不同單位控管。因此，易造成權責與督管不清疑慮，就易造成風險升高的因素。

(二)APP 應用程式之風險評估[27]

從樊國楨、林樹國與朱潮昌在 2008 年《資訊安全風險評鑑》的研究報告顯示，說明駭客會運用各項「工具、技術與方法」等手段構成威脅，也因威脅等級不同，相對影響衝擊也不相同。[28]現行在 APP 應用上符合以上三項要素，進而產生眾多風險因子，包括惡意軟體複雜性高，且連帶效應迅速發酵，加以威脅模型難建立，一旦缺乏聯防機制，隨時可能肇生資安事件。就以平時生活為例，此句是平時使用者最常提出疑問？

使用者：『我明明是使用相機，為什麼除了存取相機權限外，還夾帶要存取麥克風、GPS 定位、撥打電話、聯絡人等等……的權限，真是奇怪要求？』

但往往此情形卻無人理會。不僅是國內如此，中共亦是如此。在 2019 年第一季「淨網 2019」專項行動中，大陸共監測發現 1670 款 APP 應用程式中，分別列出 10 款超越取得權限(如表三)，收集用戶信息行為。若藉由大數據或雲計算[29]等運算模式，就可判斷該員生活習性或其他用途，[30]假使受中共當局取得管理權限，勢必監視範圍可能擴及至人民或特定人士的日常生活。

表三 2019 年「Google Play Store」上的百大熱門免費應用程式

編號	APP 名稱	過度範圍用戶權限								
		讀取使用者手機狀態和身份	訪問攝像頭進行拍照	收集精準的位置(GPS)	開機時自動啟動	允許應用程式錄製音頻	允許應用程式建立藍牙連接	讀取簡訊或彩信	讀取聯繫人數據或通話紀錄	其他

[26]〈不要讓個人資訊通過這樣的方式向外洩露了〉,《每日頭條》, https://kknews.cc/tech/9pkp5o8.html，2019 年 3 月 14 日，(檢索日期：民國 108 年 11 月 20 日)。

[27] 何謂風險評估：A.依「風險接受準則」評估「風險分析」之結果，以決定需要管控的資訊資產。B.「風險分析」之結果值高於「可接受風險等級」之資訊資產，應列為「風險處理」之對象。參考〈法務部及所屬機關資訊安全風險評鑑管理規範〉,《植根法律網》, 民國 105 年 11 月 15 日，http://www.rootlaw.com.tw/LawContent.aspx?LawID=A040090021044500-1051115，(檢索日期：民國 108 年 12 月 19 日)。

[28] 楊欣哲、彭勝寶，〈延伸型攻擊樹分析法以評估網站安全風險之研究〉,《資訊管理學報〉(臺北市)，第 21 卷第 1 期，中華民國資訊管理學會，頁 9。

[29] 雲計算(Cloud Computing)，是分散式計算技術的一種，其最基本的概念，是透過網路將龐大的計算處理程式自動分拆成無數個較小的子程式，再交由多部伺服器所組成的龐大系統經搜尋、計算分析之後將處理結果回傳給用户。〈雲計算〉,《MBA 智庫百科》, https://wiki.mbalib.com/zh-tw/%E4%BA%91%E8%AE%A1%E7%AE%97，(檢索日期：民國 108 年 11 月 20 日)。

[30] 〈真相了！為什麼很多手機 APP 要獲取我們的通訊錄、位置？〉,《每日頭條》, https://kknews.cc/tech/rz9q5xx.html，2017 年 5 月 15 日，(檢索日期：民國 108 年 11 月 20 日)。

1	電視優化大師(2.9.1)	v		v						v
2	雪球股票(11.17)	v			v	v	v			
3	免費小說大全(3.8.9.3012)	v		v	v	v	v	v	v	
4	桌面批量卸載(4.2.5)			v	v				v	v
5	LED Disco(0.812)							v		
6	K&A LOVING STORY(2)							v	v	v
7	錢聚易(1)		v					v		v
8	WiFi 萬能鑰匙(4.3.56)		v					v		v
9	金太陽(5.4.0)		v			v		v	v	v
10	棗莊智能交通(1)		v							
統計		3	4	3	3	3	2	6	4	6
備考	其他部分：1.允許程序禁用鍵盤鎖；2.允許程序重新啟動其他程序；3.允許程序打開內部窗口，不對第三方應用程序開放此權限；4.查閱敏感日誌數據；5.修改/刪除 SD 卡中的內容；6.獲取使用者設備上已知帳號列表。上述統計均為 1 項，因此不納入項次考量。									

資料來源：〈廣東警方曝光 10 款超範圍收集用戶信息 APP〉，《每日頭條》，https://kknews.cc/society/o3aozvm.html，2019 年 4 月 29 日，(檢索日期：民國 108 年 11 月 20 日)。

表四 App 權限風險評估表

項次	風險項目	風險內容	衝擊(影響)(1~3)	威脅發生的可能(1~3)	風險等級		
					高	中	低
1	訊息	存取即時訊息。	3	3	v		
2	通訊記錄	存取在裝置中 Skype 或其他電話語音 App 進行通話的歷程記錄。	3	3	v		
3	網路攝影機	啟用和使用裝置上的相機。	3	3	v		
4	GPS-位置	啟用和使用 GPS 或其他位置尋找功能。	3	3	v		
5	連絡人	存取連絡人、人員或通訊錄。	3	3	v		
6	麥克風	啟用和使用裝置上的麥克風。	3	3	v		
7	帳戶資訊	存取任何帳戶資訊。	3	2	v		
8	行事曆	存取個人行事曆。	2	2		v	
9	檔案系統	存取個人存取權的檔案和資	2	2		v	

	(SD 卡存取)	料夾，並讀取或寫入所有檔案。					
10	電子郵件	存取電子郵件帳戶的電子郵件及帳戶資訊。	2	2		v	
11	允許提高權限	允許 APP 以系統管理員權限執行，而無需先提示使用者。	2	2		v	
12	應用程式診斷	取得有關其他執行中 APP 的診斷資訊。	2	2		v	
13	藍牙	啟用和使用您的裝置與其他裝置之間的任何藍牙連線。	2	2		v	
14	Wi-Fi	啟用和使用您的裝置、網際網路和其他裝置之間的任何 Wi-Fi 連線。	2	2		v	
15	有線連線	啟用和使用任何有線連線，包括您的裝置、網際網路與其他裝置之間的乙太網路、USB 和序號通訊。	2	2		v	
16	近距離無線通訊	啟用和使用任何在您裝置與其他裝置之間的近距離無線通訊(NFC)連線。	2	2		v	
17	本機系統服務	在以最大權限執行的電腦上安裝服務。	2	2		v	
18	視訊媒體櫃	存取裝置上視訊媒體櫃中的任何視訊檔案。	2	2		v	
19	圖片媒體櫃	存取裝置上圖片媒體櫃中的任何圖片檔案	2	2		v	
20	音樂媒體櫃	存取裝置上音樂媒體櫃中的任何音樂檔案。	1	1			v
21	動作	啟用和使用裝置上的加速計或其他動作感應功能。	1	1			v
22	可修改的 APP	允許使用者修改 APP。	1	1			v
23	通知	存取出現於控制中心的通知	1	1			v
24	封裝服務	在機器上安裝服務。	1	1			v
25	封裝寫入重新導向相容性 Shim	允許 APP 在 APP 的安裝資料夾中建立、修改或刪除檔案。	1	1			v
26	工作	存取 Outlook 及其他工作追蹤 APP 中的工作清單。	1	1			v
27	未虛擬化資源	寫入在解除安裝時未清除的登錄項目和檔案。	1	1			v
28	語音辨識	啟用和使用任何語音辨識硬體。	1	1			v
29	自訂安裝動作	安裝其他軟體。	1	1			v
30	臉部辨識	啟用和使用任何臉部辨識硬體。	1	1			v

31	指紋辨識器	啟用和使用任何指紋辨識器硬體。	1	1			v
備考	1.風險容忍度＝中度風險以下予以容忍。 2.風險等級與回應 (1)高度風險(R=3)：管理階層需督導所屬研擬計畫，並提供資源，予以處理。 (2)中度風險(R=2)：需明定管理階層的責任範圍，作必要監視。 (3)低度風險(R=1)：予以容忍，依現行步驟處理。						

資料來源：〈App 權限〉，《Microsoft》，https://support.microsoft.com/zh-tw/help/105 57/windows-10-app-permissions，(檢索日期：民國 108 年 11 月 17 日)。

經由筆者對 31 項風險項目進行風險評估，可識別各等級潛在風險來源，得到屬於高等風險為 7 項、中度風險為 12 項、低度風險為 12 項。以下針對高風險安全威脅實施分析，進行提出風險降低之建議與改進說明。(如表五)

表五 APP 安全威脅分析

編號	弱點	威脅	威脅描述	建議及改進措施
1	獲取手機識別碼	不安全身分認證	可以確定使用者手持的手機型號，開發者可通過大數據統計軟體的下載量與實際的安卓使用量，進行使用者適配。	1.增加資安宣導要項。 2.針對惡意軟體發布資安通報。 3.建立資安聯繫管道。 4.避免安裝來路不明或不需要的APP。 5.密切注意程式所請求的存取權。
2	獲取存儲空間	不安全資料儲存	獲取手機的存儲空間，衡量手機空間，便於下載、保存圖片視頻和取得敏感性資料。	
3	獲取相機和錄音	網路監聽	獲取相機、錄音功能，取得啟用攝像頭、錄音功能的權限，可竊聽動態。	
4	獲取 GPS 定位	定位追蹤	獲取定位資訊被列入危險許可權，例如使用導航程式時，使用者會開啟全球定位系統，GPS 功能開啟後可追蹤所在位置。	
5	獲取通訊錄權限	通訊錄權限	開啟通訊錄權限，可讀取、獲得編輯/刪除或得到聯繫人名單權限。	

資料來源：作者編製。

從上述得知只要獲取相關權限，就可任意操控帳號，其中暗藏個人隱私問題，使用者就成為網路術語「裸奔」狀態，就算遭 Google Play 或 App store 下架，若使用者無法從裝置中直接刪除，仍有面臨攻擊之風險。[31]

因此，國軍是為社會一份子，在軍隊開放智慧型手機同時，也使上述風險逐漸增加。相對也會對國軍造成影響，國防部應試想中共是否運用資訊罅隙，實施各項網路滲透與攻擊，面對如此安全危機困境，應想盡解決之道，避免擴大情蒐空間，防止未來軍事機密遭受窺視，這將會損及國家安全與利益。

[31]〈惡意 App 年下載量達 3 千萬次！Google 與業者共組「防禦聯盟」強化掌上資安〉，《數位時代》，https://www.bnext.com.tw/article/55385/google-android-app-defense-alliance，2019 年 11 月 7 日，(檢索日期：民國 108 年 11 月 14 日)。

三、共軍運用惡意 APP 對國軍作為蠡測

在 2012 年美國眾議院調查報告指出，顯示部分中共資訊廠商背後均有軍方背景，[32]透過廠商合作提供軍事需求，稱之為「供應鏈攻擊」，[33]並以此作為戰爭工具。若從 APP 資安上加以分析，也可被視為一種「網路攻擊」，分別為「竊取」或「破壞」。以上皆有共同公式：攻擊(Attack)＝動機(Motive)＋方法(Method)＋弱點(Vulnerability)。

想必中共對臺動機企圖相當明顯，但並非絕對以武力犯臺，其實「資訊戰」(Information Warfare)[34]也是方法之一，且更易融入生活之中。從 2014 年 11 月我國前國安局長李翔宙已說明中共正研製惡意 APP，以竊取特定目標敏感資訊。[35]另據 2015 年 10 月美資安業者 FireEye 也表示，中共的惡意程式假冒智慧型行動裝置 APP，已成功竊取國人個資。[36]加以近期積極發展人工智慧科技，例如大規模蒐集個資、生物特徵數據及數位監控等，透過訊息收集、宣傳與心理暗示等行動，影響國人的認知、態度與行為。

從 2019 年 6 月美國國防部副部長在印太戰略會議上表示：「2020 年，中共百分之百會用資訊戰打臺灣」，[37]此項明確表達未來所應面臨資訊險境。筆者依據美國國防大學資訊戰權威李比奇(Martin C. Libicki)在 1995 年指出的資訊戰是以許多不同形式的聚集[38]作為釋義，針對符合 APP 實例之「情報戰、心理戰與網域戰」進行分析。

(一)情報戰－蒐集數據資料庫

中共對情報戰是以「隱蔽戰線」為主，而現今的資訊時代中，諜報戰的管道與來源更加多元，APP 就是其一。從美國智庫彼得森國際經濟研究所(Peterson Institu te for International Economics)研究報告指出，中共「抖音」應用程式就疑似蒐集大量個資與民間資訊，已對美國造成國安問題，[39]另智庫研究員碧安寇提(Claudia Biancotti)則認為看似無害的抖音，卻可能是中共在全球人工智慧競賽中的特洛伊木馬。[40]

---

[32] 陳鈺津，〈網路沒有距離，也沒有祕密〉，《清流雙月刊》(台北市)，第 18 期，法務部調查局，2018 年 11 月，頁 55。

[33] 〈林宏達闇黑部隊入侵 無聲的國安危機〉，《財訊》，https://www.wealth.com.tw/home/articles/21383，2019 年 7 月 10 日，(檢索日期：民國 108 年 11 月 15 日)。

[34] 「資訊戰」包括戰時和平時任何用來影響敵方資訊系統、資訊作戰應用在所有作戰步驟、所有軍事行動範圍和每一層級戰爭。Joint Chiefs of Staff, Joint Pub 3-13: Joint Doctrine for Information Operations (Washington, DC: Joint Chiefs of Staff, 1998), p.vii.

[35] 〈國安局證實中共「網軍」多達 18 萬人〉，《新頭殼 Newtalk》，https:// Newtalk.tw/news/view/2014-11-20/53852，2014 年 11 月 20 日，(檢索日期：民國 108 年 11 月 18 日)。

[36] 〈國安局保密手機 藍綠不敢用〉，《中國時報》，https://www.chinatimes.com/newspapers/20151022000424-260102?chdtv，2015 年 10 月 22 日，(檢索日期：民國 108 年 11 月 14 日)。

[37] 〈台專家：資訊戰導致內戰 中共欲「讓台灣亂」〉，《大紀元》，http://www.epochtimes.com/b5/19/6/23/n11341256.htm，2019 年 6 月 24 日，(檢索日期：民國 108 年 11 月 20 日)。

[38] 資訊戰區分為七種形式：指管戰(command-and-control warfare,C2W)；情資戰(intelligence-based warfare, IBW)；電子戰(electronic warfare, EW)；心理戰(psychological operations, PSYOPS)；經資戰(information economic warfare, EIW)；駭客戰(hacker warfare)；網域戰(cyber warfare)。」彭錦珍，〈現代化發展趨勢下的資訊社會與資訊戰〉，《復興崗學報》(臺北市)，第 86 期，國防大學政治作戰學院，民國 95 年，頁 45。

[39] 鄭鈞元，〈應用系統面臨多元資安風險之教戰手則（上）〉，《叡揚 e 論壇》(臺北市)，第 84 期，叡揚資訊，2016 年 10 月，頁 26。

[40] 〈「抖音」是中共的網路間諜？談短片 App 資安爭議〉，《鳴人堂》，https://opinion.udn.com/opinion/story/12061/3973187，2019 年 8 月，(檢索日期：民國 108 年 11 月 20 日)。

舉例說明：獲取軍方特定目標人員之 APP 授權，可推估日常習性及活動意義，若更取得 GPS 定位資訊、通訊錄、簡訊、錄音等資料，可研判部隊動態，例如演訓、基地等。

(二)心理戰－散播假訊息誤導

我國國安局在 2019 年 5 月 2 日就已向立院提出:「中共假訊息心戰之因應對策」之報告，且引述瑞典哥德堡大學研究報告，指出我國深受外國假訊息攻擊頻率最高的國家。主要藉由社群媒體轉發、LINE 群組流傳，採用「行銷與心理學」對策，使國人產生認知混淆，最終影響決策。例如 2018 年中共力推惠台 31 條措施，大量運用網路宣傳戰以同名的 APP、網站、臉書等媒介，強力推銷對臺政策資訊。[41]此舉動表示中共已進階至「認知領域」攻擊，[42]企圖達到不戰而屈人之兵。

舉例說明：透過真假混合的「假新聞」，透漏軍方負面議題，維持新聞議題的熱度，建立民眾對於議題的負面印象，且對於特定族群表達負面觀感。

(三)網域(路)戰－虛擬空間戰場

網路戰主要依賴於硬體與軟體，其特性在於突然性、隱蔽性、不對稱性和代價低、參與性強等特點。[43]因此，虛擬網路空間是目前各國相繼爭取的戰場，正符合智慧型手機與 APP 的應用。中共近年在習近平領軍下，相繼設立「中央網絡安全和信息化領導小組」，此點顯示中共高層已將網路安全及發展視為重點。相對在發展同時，勢必我國會受到影響，況且國內是屬於資訊開放之環境，衝擊性應該會較大。

舉例說明：2014 年的俄羅斯併吞克里米亞島模式，就是最佳之案例。

除上述可見中共已開始對我國採取軍事威脅外，他國也面臨相同困境，如 2017 年底印度政府及 2018 年澳洲國防部均嚴禁手機安裝微信 APP，[44]印度更要求駐紮邊界之部隊，須刪除微信、微博及 Truecaller 等 42 款由大陸研製的手機應用軟體。[45]上述實例已分析當今戰爭型態已有所改變，可從軍事至非軍事、前方至後方，平時至戰時，僅需運用網路各種手段實施誤導、錯亂、阻絕、封鎖等作為，就可以達到「致人而不致于人」之原則。

然而，我國處於資訊網路發達的時代，人手一機已是常態亦是強項，相對也是弱點。想必國軍官兵亦是如此，從上述 2019 年「Google Play Store」的百大熱門免費應用程式中不難發現超越「權限」問題，一旦下載惡意 APP 必會造成資安影響。因此，應不斷提醒在下載 APP 同時，需針對 APP 內容加以審認，且勿輕易同意認可。

---

41 〈中國網路宣傳戰整合再升級，台灣怎麼應對？〉,《聯合新聞網》, https://www.gvm.com.tw/article/60402，2019 年 4 月 6 日，(檢索日期：民國 108 年 11 月 21 日)。

42 〈新新聞-北京資訊戰裂解台灣：讓你覺得中國好棒棒、愛台灣沒前途〉,《風傳媒》, https://www.storm.mg/article/1261729，民國 108 年 5 月 10 日，(檢索日期：民國 108 年 11 月 18 日)。

43 陳良駒、范俊平、謝佳容,〈網路作戰安全與管理主題實證探索之研究-使用 GHSOM 技術〉,《資訊管理學報》(臺北市)，第 23 卷第 1 期，國立臺灣大學商學研究所，民國 105 年，頁 99-128。

44 〈保密到家：以智慧型手機 App 為例〉,《清流月刊》(新北市)，第 20 期，法務部調查局，民國 108 年 3 月，頁 15-19。

45 〈APP 曝資安危機 別把手機當麻吉〉,《青年日報》, https://www.ydn.com.tw/News/267148，2017 年 12 月 5 日，(檢索日期：民國 108 年 11 月 20 日)。

國軍應有之資安風險防制與作為

2019 年 3 月蔡總統參加臺灣資安大會強調「資安就是國安」，說明數位化已成為趨勢，身為保衛國家的國軍勢必會遭受資安的威脅與挑戰，因此需加以重視資安風險的管控作為，就如同國防部副參謀總長李廷盛中將工作指導中所強調「資訊安全即是軍紀安全」。

一、執行風險評估，建立聯繫管道

從風險管理角度分析，其實資訊安全工作是無法達到「零風險」的境況。但國軍若能先期完成 APP 風險分析與評估，透過系統化分析尋找風險與威脅嚴重等級，就能降低風險。例如：智慧管理系統-APP 會竊取個人權限，可能帶來隱私威脅，藉由其一、聯繫管道(資安研討會)，將威脅趨勢提供給官兵；其二、加強資訊軟體之管理。

再者，單位應建立資安專責聯繫管道，完成內(外)部溝通聯繫機制，彼此整合、共享威脅情報，且平時多關注相關資安新聞、漏洞。若發生資安事件可立即尋求協助，以求事件之快速排除。以下為建立聯繫管道之建議事項。

(一)資安舉報管道

提供部隊內(外)人員各類舉報途徑，例如電子郵件、網站與電話等，提供之管道愈多元，愈能提升處理時效與辦理效能。

(二)設置專責編組

因部隊講求編制，若能在各連營級採取任務編組方式，採取專責人員，針對 APP 軟體舉報案件實施審慎檢視真實性。

(三)提供檢舉獎金

若部隊發現官兵使用可疑之 APP 軟體，可藉由反映機制向上呈報，而建議予以核發檢舉獎金獎勵。

若能建構良好資安機制，提供完善的威脅防禦與集中化的掌握與監控能力，使官兵都能提高 APP 使用警覺性，主動發掘風險徵候即時向上反映，方能確保機密不外洩之危機。

二、強化資安政策，加強法令宣教

2019 年 11 月 3 日我國立法院已三讀通過「陸海空軍刑法部分條文修正草案」現役軍人如果捏造或「傳述」軍事上之「不實訊息」[46]。其中法規之第 72 條條文，明確說明如果傳播方式是以廣播電視、電子通訊、網際網路或其他傳播工具，得加重刑責二分之一。APP 運用也包含在內，例如社群媒體，LINE 或 Facebook 等。國軍應運用各場合將新修訂之條文進行宣導，以提升宣教之廣度、深度和速度，避免以身試法。

[46] 現役軍人如果捏造或「傳述」軍事上之「不實訊息」，處 3 年以下有期徒刑、拘役或 30 萬以下罰金；如果是以廣播電視、電子通訊、網際網路或其他傳播工具散布不實訊息，加重其刑最重判處 4 年 6 個月以下有期徒刑、拘役或罰金 45 萬。對於所謂「軍事上」的不實訊息，國防部曾作出解釋，範疇包括軍事上的人事、情報、作戰、後勤、武器編裝、軍備等。〈立院三讀 軍人網傳軍事假訊息得加重其刑〉，《中央通訊社》，https://www.cna.com.tw/news/firstnews/201911050033.aspx，2019 年 11 月 5 日，(檢索日期：民國 108 年 11 月 20 日)。

(一)廣度

定期舉辦資安宣導巡迴講習，以座談會方式雙向互動交流，且透過網路擴展宣教，結合臉書粉絲專頁、官方網站與數位學習平台等媒介，予以拓展廣度與分眾資安宣導。

(二)深度

藉由深度溝通方式，可區分議題內容，針對 APP 運用實施集體智慧協作模式，可從網路問題蒐集來源或鮮活案例、態樣資料進行比對，再藉由彙整組合，以達到活化資安宣教之目的。

(三)速度

各單位應落實辦理各項資安事件，以提升偵測與反應速度；另透過資安通報及資安應變程序等各項演練，提升事件應變速度。

藉由上述三項重點，就可建立國軍官兵「守規守分」的觀念，唯有官兵個人具備完善的資安警覺及高度的保密習性，才能夠確保國軍的整體安全。

三、認識駭客(網軍)趨勢，提高資安意識

在傳統的資安威脅中，駭客主要經由電子郵件、檔案或網站安裝惡意程式等作為傳播途徑。現今亦運用所謂的「隱藏管道」，從 2016 年起發現駭客已從惡意軟體藉由供應鏈，滲透至部分 Android 手機，國軍須擺脫以往傳統想法有所新的認知，以強化部隊在「作業面」與「管理面」執行。

(一)作業面

國軍落實國軍資安政策規範及標準化作業程序，按程序、步驟、要領，藉由計畫(Plan)、執行(Do)、檢查(Check)、行動(Act)稱之謂「 PDCA 循環程序」實施檢驗，以降低資安風險威脅。

(二)管理面

APP 程式種類繁多，且區分各種類型，除管制國軍智慧型手機自動化管理系統(MDM)，進營區切勿圖求便利自行關閉，避免會議場所遭 APP 程式竊聽、定位回傳情事。

國軍係維護國家安全的第一道防線，尤其面對中共網軍無孔不入的網路攻擊及竊密蒐情，全體官兵於營內應貫徹網路實體隔離的觀念及落實個人保密作為，幹部則依資訊安全檢管要項，加強保密檢查強度及密度，防範洩密違規情事。

四、培育資安人才，降低資安風險

國軍現今已完成全志願役轉型，單位須以提升資安人才數量為目標。因為現代戰爭趨勢發展，資訊戰不僅是前哨戰，更可能成為作戰致勝的關鍵因素。因此，部隊不能僅單純依賴資安防護軟體或解決方案，更需投入必要時間進行適當的資安培訓。

現行可配合部隊教學點提供多元資源(資通訊科系大學)，針對有興趣之官兵培養第二專長。再者，能否鏈結證照班隊完成證照獲取，在連隊中以「資安扎根」為重點，將相關資安

知識與觀念、傳承國內外成功資安經驗。符合美國紐奧良杜蘭大學(Tulane University)資深資安分析師 Mark Liggett 所述：「合格專業人才的缺乏，是企業中最常聽到的資安問題….讓更多各行各業的新鮮人能夠培養這方面的能力….有效管理資安問題，並降低攻擊風險的重要關鍵。」[47] 因此，部隊若能有效培育資安人員，就可為單位達到以下幾點：

(一)確保連隊瞭解資安重要性。

(二)提升單位資安威脅的意識。

(三)分析 APP 應用管理之策略。

(四)提出連隊資安弱點建議事項。

培育人才確實不易，但若能重視整體網路安全中，相信必能發揮資安警覺及危安預警功能，建立堅固的安全防線，唯有部隊官兵都自我要求，恪遵資安規定，才能建構出一道堅若磐石的安全網。

結論

「安全是一切的基礎，沒有安全就沒有一切」，這句話耳熟能詳，不僅適用在資訊安全的領域，更提醒國軍面臨智慧型手機與 APP 應用程式的普及，雖提升日常生活的品質，但惡意軟體問題與防護機制的不健全，往往看似免費的背後，卻付出慘痛的教訓，也就是「隱私權問題」。上述查驗手機惡意軟體的恐怖程度，絕不亞於電腦病毒軟體，並且現已成為全球性議題，面臨網路環境衝擊之課題。

況且，文內舉例數則手機資訊外洩的案例，其代表網路上是沒有距離，同時闡述 App 所潛藏的危機與風險。因此，身為國軍的我們，平時切勿貪圖一時便利或僥倖，在各類型之 App(社群媒體、通訊軟體)談論敏感公務或傳輸公文資料等，方能確保機密不外洩，降低資訊安全的風險威脅。

參考文獻

一、 黃建隆，〈行動裝置 App 之安全導覽〉，《財金資訊季刊》(臺北市)，第 79 期，財金資訊股份有限公司，2014 年 7 月。

二、 陳姿陵，〈運動手環 APP 洩漏你的行蹤〉，《清流雙月刊》(臺北市)，第 15 期，法務部調查局，2018 年 5 月。

三、 陳鈺津，〈網路沒有距離，也沒有祕密〉，《清流雙月刊》(臺北市)，第 18 期，法務部調查局，2018 年 11 月。

[47]〈趨勢科技 2019 年 Capture The Flag (CTF)網路攻防搶旗賽起跑資安〉，《趨勢部落格》，https://blog.trendmicro.com.tw/?tag=%E8%B3%87%E5%AE%89%E4%BA%BA%E6%89%8D，2019 年 8 月 28 日，(檢索日期：民國 108 年 11 月 20 日)。

四、〈APP 的度量衡—資安檢測標準的剖析〉,《科學發展》(臺北市)，第 553 期，科技部，2019 年 1 月。

五、〈使用者風險認知對遊戲類 In-App 廣告點擊意願影響之研究〉,《人文社會科學研究〉(屏東縣)，第 10 卷第 2 期，國立屏東科技大學人文暨社會科學院，2016 年 6 月。

六、楊欣哲、彭勝寶,〈延伸型攻擊樹分析法以評估網站安全風險之研究〉,《資訊管理學報〉(臺北市)，第 21 卷第 1 期，中華民國資訊管理學會，2013 年 1 月。

七、彭錦珍,〈現代化發展趨勢下的資訊社會與資訊戰〉,《復興崗學報》(臺北市)，第 86 期，國防大學政治作戰學院，民國 95 年。

八、鄭鈞元,〈應用系統面臨多元資安風險之教戰手則(上)〉,《叡揚 e 論壇》(臺北市)，第 84 期，叡揚資訊，2016 年 10 月。

九、陳良駒、范俊平、謝佳容,〈『網路作戰安全與管理主題實證探索之研究－使用 GHSOM 技術』〉,《資訊管理學報》，第 23 卷第 1 期，中華民國資訊管理學會，民國 105 年。

十、〈「同意條款」不設防？小心手機 APP 洩個資〉,《TVBS NEWS》，https://news.tvbs.com.tw/local/687768，2016 年 11 月 20 日，(檢索日期：民國 108 年 11 月 20 日)。

十一、〈下載 App「隱私權限」要注意！超過 250 款遊戲應用程式會偷偷監聽手機〉,《自由電子報》，https://today.line.me/TW/pc/article/2zwgm6，2018 年 1 月 2 日，(檢索日期：民國 108 年 11 月 5 日)。

十二、〈個資恐被看光光，杜奕瑾：別用中國 App 和設備〉,《科技新報》，2019 年 3 月 5 日，https://technews.tw/2019/03/05/ptt-father-said-dont-use-chinas- everything/，(檢索日期：民國 108 年 11 月 2 日)。

十三、〈破千款 Android App 違規蒐集個資，連拒絕授權都沒用〉,《科技新報》，https://technews.tw/2019/07/10/thousands-of-android-apps-takes-personal-data-even-though-deny-permissions/，2019 年 7 月 10 日，(檢索日期：民國 108 年 11 月 6 日)。

作者簡介

曾柏元中校，陸軍軍官學校90年班、陸軍步兵學校正規班339期、國防大學陸軍指揮參謀學院101年班、國立政治大學戰略與國際關係研究所。曾任排、連、營長、教官。現任國防大學教官。