網路攻擊，精準無形，廉價高效

陸軍中校　宋連海

提　要

資訊與通信科技已是現代生活運行不可或缺的一環，我們仰賴資訊與通信基礎設施治理國家建設、商貿往來以及公民行使自由與權利。同樣地，各國也仰賴其資訊與通信科技之基礎設施，並握有網路攻擊能量以確保必要時可威脅他國網路使用的有效性、可靠性及機敏性，期使能在戰時對敵方國家社會造成癱瘓與停止運作。

網際網路以及與網際網路相連結的智慧型產品已完全滲透你我生活之中，不論是工作聯繫、資訊傳遞、產品設計、商品採購、遠端遙控甚至是軍事行動、武器系統及指揮與管制等，均需仰賴網際網路的迅速與便捷。

準此，有心人士或國家政體也早已利用此一平台，從中獲取個人利益甚至達到政治目的。因此，任何缺乏正確觀念與意識，又沒有相對應技術能力的情況下，任一使用者都會在不知情的情況下暴露在絕高的風險。輕者身敗名裂，重者全軍覆滅。

本文企圖以基礎概念導入，協助讀者擁有自我防護觀念，以確保個人資訊安全。並以近年世界各國遭受的網路滲透與攻擊為例，闡述網際網路帶來科技便利的同時，也帶來史無前例地又難防杜的風險。此外，依現今諸多攻擊與滲透模式預判，未來的網路攻擊將越來越精準與無形，且效益更高，損失更龐大。

關鍵詞：網際網路、網路攻擊、網路滲透、精準攻擊

前　　言

兵法家孫子也沒料到，孫子兵法第十篇「地形」中的「通」、「掛」、「支」、「隘」、「險」、「遠」，談論敵我接觸線、補給要道、險地、高地、要地、隘口等，在當今無疆界的網路空間裡，傳統作戰思維已需與時俱進的大幅調整。

然而，兵者，國之大事。一國網路空間的安全確保，有賴各相關部門共同合作，從定義威脅到制定國家網路戰略，再到教育民眾資安意識以確保個人財產安全等，都必須整體規劃與納入考量。但由於傳統安全的概念係源自於明確的領土、疆界與主權，而網路空間無國界，必須打破舊有思維，以前瞻的概念與他國共同合作，將國家網路戰略提升至全球合作的層級。

自1971年第一封電子郵件產生後，到

1991年起網際網路開放全球使用，至今統計一年約有40兆封電子郵件透過網際網路往來全球的用戶。2013年前，全球共計有30兆註冊的官方網頁。此外，至今全球共有90億項與你我生活相關的產品與網際網路連結，並且，在2020年以前，與網際網路連結的產品預測將高達400億。其中包含車輛、小型電子產品、醫療設備及今天你我都還無法想像出的產品都可能在不久將來誕生。[1]

科技帶來便利，也創造無限可能。生活上的便利包含有，一支智慧型手機在手，其強大的生產力可幫助即使在行動中的使用者於任何時間及地點，進行拍照、製圖、簡報、編輯然後一鍵發送。所有的工作完成或者達成交易，均不需要使用者老老實實地坐在辦公室裡便能輕易完成。由於生活所需均與網路息息相關，因此，也提供了有心人絕佳的平台，透過網際網路及利用使用者的疏忽與無知從中獲取龐大的利益。更有甚者，在國與國的層面，透過網路資訊的傳遞，已經可以完全操弄一國的閱聽大眾、國家政策以及選情逆轉。去年11月的美國總統大選及今年法國總統大選便是絕佳案例。所以，這一便利與無限可能同時也引來極大風險與影響國家安全。

以民間企業為例，全球前500大企業，其中97%曾遭受網路攻擊，而剩下的3%則為遭受攻擊而不自知。也就表示，全球所有企業不論在已知或不知的情況下，均遭受過或大或小的攻擊，無一倖免。而目前有上百個國家政府刻正嚴肅面對這樣的無形黑手。[2]

網路攻擊，精準無形

根據牛津辭典，「網路攻擊」的定義為「駭客對於網路系統的傷害與破壞」。[3]另外，網路辭典的廣泛定義為「對於電腦、電腦系統及電子通信網絡進行破壞、傷害及非法入侵之企圖」。[4]綜合而言，凡是駭客藉由其自身電腦技術能力，對所望對象之電腦系統進行滲透、破壞與入侵，並從而竊取所需資訊。而這些駭客可以是個整天坐在地下室沉迷於網路世界的科技宅男(據文獻記載，全世界最年輕的駭客為美國加州一名5歲的幼童，於2014年成功破解微軟遊戲機XBOX帳號登入系統)[5](圖一)，也可以是受雇於國家情報與安全相關機構的專業人員。透過這些駭客的技術能力，幾乎無所不能的竊取世界各地儲存在伺服器的資訊、自動開啟與遙控遠端攝影機、自動開啟智慧型手機錄音功能以及操控無人駕駛汽車而導致高科技機密資訊

1 P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar (NY: Oxford University Press: 2014),p.2
2 P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar (NY: Oxford University Press: 2014),p.2
3 Oxford, https://en.oxforddictionaries.com/definition/cyberattack (檢索日期：2017年9月18日)
4 Dictionary, http://www.dictionary.com/browse/cyberattack (檢索日期：2017年9月18日)
5 Chris Welch, “5-year-old discovers major Xbox One security flaw, earns big reward”, The Verge, https://www.theverge.com/2014/4/4/5582208/5-year-old-discovers-xbox-one-security-flaw (檢索日期：2017年9月18日)

圖一　圖片來源：最年輕的駭客，5歲的克里斯多福 https://www.theverge.com/2014/4/4/5582208/5-year-old-discovers-xbox-one-security-flaw

外洩、交通癱瘓甚至人員傷亡等。

以下摘要近年全球著名的網路攻擊與入侵事件：

一、Stuxnet(震網)，於2010年首次被發現運用於滲透伊朗核能電廠的電腦系統。震網為一500KB的電腦蠕蟲(程式)，其入侵程序區分三步驟。首先，分析與鎖定採用微軟作業系統的電腦系統，選定有漏洞未修補的系統入侵後，開始自動複製與增生蠕蟲程式。接著針對電腦系統內西門子軟體Step7入侵(此軟體普遍用於工業界電腦系統，如核能廠內的鈾濃縮設施)，然後蠕蟲便取得鈾濃縮設施及核能廠的控制權。若再有外接式硬碟(或俗稱USB及拇指碟)接上受感染的電腦系統，則外接式硬碟也自動感染並散播至其他電腦。此一程式便以這般倍數成長方式快速感染伊朗核能設施，總計共有15座核能廠遭受感染及984座鈾濃縮離心機遭到破壞，此一行動使伊朗整體鈾濃縮效能減損30%。[6]

事件發生後，許多西方媒體均一致認為此一程式是美國國家安全局所撰寫並與以色列共同合作的行動。但至今仍沒有確鑿的證據證實是美國與以色列共同所為。

二、雅虎公司於2016年9月對外證實，該公司伺服器於2013-2014年間遭到「受雇於國家的駭客」(state actors)入侵，共計有15億筆個人資料、電子郵件信箱、電話、地址遭到竊取，是為最大網路信箱入侵與最多人受害的事件。然而，為顧及公司商譽，雅虎公司隱瞞至事發一兩年後才對外公布。這也是網路攻擊事件中，讓受害者無法第一時間因應，持續受害到事件被揭發為止。[7]

三、2014年，聲稱擁有全球6千萬會員大型成人交友網站遭來自泰國的駭客入侵，起因於積欠該網站會員費用而心生報復。共計3百多萬筆個人資料遭竊，其中包含生日、住址、電話、性別、語言、人種、郵遞區號等。駭客並揭露多數會員均為已婚身分，成員有政要、名流與藝人等。[8]

四、另一個神祕又知名的駭客組織「影

6 Michael Holloway, “Stuxnet Worm Attack on Iranian Nuclear Facilities”, Stanford University, http://large.stanford.edu/courses/2015/ph241/holloway1/ (檢索日期：2017年9月18日)

7 Taylor Armerding, “The 16 biggest data breaches of the 21st century”, CSO, https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html(檢索日期：2017年9月18日)

8 Steve Ragan, “Adult Friend Finder confirms data breach 3.5 million records exposed”, CSO, https://www.csoonline.com/article/2925833/data-breach/adult-friend-finder-confirms-data-breach-3-5-million-records-exposed.html (檢索日期：2017年9月18日)

子掮客」(Shadow Brokers)於2016年8月間將幾組自美國國家安全局竊取的網路入侵程式「想哭」(WannaCry)及「永恆之藍」(EternalBlue)，在俄羅斯和烏克蘭大量流竄，波蘭、義大利、德國、美國、法國等國家也發現此病毒蹤跡。此病毒針對電腦檔案加密，也加密主開機磁區，導致電腦完全無法運作。系統重開機後，就會出現勒索病毒畫面，必須依照指示於加密系統付費後，才有可能但又不保證解鎖。(圖二)許多醫院內的電腦系統因此凍結，造成病患就醫延遲甚至危及生命安全。[9]

五、2015年美國索尼製片公司(SONY Picture Entertainment)因推出以戲謔北韓領導人金正恩為題的院線片「名嘴出任務」(The Interview)，遭到北韓駭客組織「和平使者」(The Guardian of Peace)的網路攻擊。駭客將索尼公司內部共計2千億筆(200,000,000,000)機密資訊曝光，其中包含藝人電話號碼、劇本內容、員工個資及5部最新高畫質尚未上映的電影，堪稱企業史上受害最慘重的攻擊事件。[10]駭客組織威脅索尼公司不得上映該影

圖二　勒索畫面　圖片來源：http://www.ksoa.com.tw/news-detail-1653260.html

片，否則將採取更大報復行動。後來索尼公司妥協未上架，但仍在美國前總統歐巴馬公開對北韓嚴厲譴責後，索尼公司改採以線上付費方式下載觀看。

一字外洩，身敗名裂

最近一次大規模網路攻擊是在2017年9月，美國一個最大，歷史最悠久的信用報告機構「易快傳真」(Equifax)對外證實，在7月份時遭到網路攻擊後，共計1億4千多萬筆資料外洩。[11]

上述資料外洩看似並未造成你我生活上直接影響，但其實不然。許多個資遭駭客竊

9 尤嘉禾，< 新型勒索病毒Petya 透過Eternal Blue漏洞擴散中> 《DigiTimes》，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000506136_dfq0c9qa4kynnc5f7e3d0(檢索日期：2017年9月19日)

10 Mohit Kumar, “Bittorrent Invites SONY to release The Interview Movie on Its Paid Service”, The Hacker News, http://thehackernews.com/2014/12/The-Interview-movie-torrent-download.html (檢索日期：2017年9月19日)

11 Equifax Inc.是美國一家消費者信用報告的全球性服務機構，與Experian和TransUnion被認為是美國三大信貸機構。Equifax創立於1899年，是美國三大信貸機構中最年長的機構，它收集並儲存全球超過8億消費者和超過8800萬家企業的資訊，總部位於亞特蘭大，年營業額達27億美元，在14個國家擁有9,000多名員工。2017年9月，Equifax宣布在2017年7月29日遭受網絡攻擊(截至撰稿時，攻擊仍持續中)，有至少20萬名客戶的信用卡信息被竊取。https://zh.wikipedia.org/wiki/Equifax (檢索日期：2017年9月19日)

取後，在層層加密與虛擬伺服器掩護下的暗網 (Dark Web)黑市販售。[12]這些個資遭冒用後可用來向銀行貸款、申請信用卡、刷卡消費、盜領財物、買賣禁品。最終導致原始資料持有人信用破產或身敗名裂，而盜用者仍逍遙法外。

根據統計，在美國每兩分鐘就有一個人的資料因網路攻擊遭外洩。一位在美國俄亥俄州的女士艾咪克瑞伯(Amy Krebs，以下簡稱克氏)，個資於2013年期間遭他人盜用。冒用者在當地向多家銀行開了50多個戶頭，並用克氏身分就醫，以其名字及身分證字號(美國稱社會安全號碼，Social Security Number or SSN)申請信用卡並逍遙自在的消費。克氏因為一通銀行的來電驚覺自己並未在該銀行開戶及申請信用卡。然而，這一連串盜領冒用行為早已持續了半年多。

夢魘並未因此結束，克瑞伯女士報警、蒐證、向各家銀行、雇主、醫院證明自己的身分遭盜用，而各公司機關要求驗明正身的程序與方式不一，且過程曠日廢時。此外，冒用者就醫紀錄也因為受個資保護的情況下，完全無法對克氏公開，使蒐證過程更難上加難。諷刺的是，各行各業當初對冒用者的消費過程卻沒如此嚴苛與刁難，反而是原始身分的受害者要經歷這些苦痛的證明程序。雖然冒用者最終被警方逮捕，但克瑞伯女士為此事奔走，不斷的出庭作證、陳述案情、解釋經過、提出證明，然後同樣程序重覆再重覆，只為了證明自己的清白與洗刷無妄之災。[13]

混淆視聽，操弄政局

除了網路攻擊與滲透竊取個資冒用盜領事件外，透過網路社群媒體傳遞混淆視聽的資訊，也嚴重影響每日的生活，甚至已能操控他國政治與選舉。

根據美國史丹佛大學一篇針對2016年美國總統大選受假新聞操弄影響的學術文獻指出以下幾個事實：[14]

一、62%的美國民眾(台灣57.4%[15])透過網路社群媒體閱讀新聞。

12 只能用特殊軟體、特殊授權、或對電腦做特殊設定才能連上的網路，使用一般的瀏覽器和搜尋引擎找不到暗網的內容。暗網的伺服器位址和資料傳輸通常是匿名、匿蹤的。暗網雖然使用公開的網際網路當作線路，但通常使用非常規網路傳輸協定和連接埠(傳統的網際網路傳輸協議是HTTP/HTTPS，分別使用埠80/443)。有些使用分散式網路架構或層層轉傳來混淆來源，使得第三方難以知悉網路資訊傳遞內容，就算知悉也難以追蹤通訊參與者的真實位置和身分；再搭配全程加密傳輸，即使第三方攔截通訊也難以解析內容。

13 Laura Shin, "'Someone Had Taken Over My Life': An Identity Theft Victim's Story", Forbes, https://www.forbes.com/sites/laurashin/2014/11/18/someone-had-taken-over-my-life-an-identity-theft-victims-story/#352b916b25be (檢索日期：2017年9月19日)

14 Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in 2016 Election", Journal of Economic Perspectives—Volume 31, Number 2—Spring 2017, Stanford, Pages 211–236, https://web.stanford.edu/~gentzkow/research/fakenews.pdf, (檢索日期：2017年9月19日)

二、假新聞(或捏造的謠言)在臉書上廣為流傳的速度比在主流媒體傳遞還快。

三、多數人均輕易取信於假新聞與假消息。

四、當時被廣為討論的假新聞內容多數皆呈現出對總統候選人川普較為有利。

此外，綜合上述幾個事實該文獻也得出一個結論。本次美國總統大選若非受有心人士運用假新聞操弄閱聽大眾，川普是不可能會當選的。文獻更堅定地指出，在其文獻資料庫裡計算出，美國總統大選前有利於川普的假新聞共有115則，在臉書被廣為分享3千萬次。而對希拉蕊有利假新聞有41則，被分享7百多萬次。

今年4-5月間法國總統大選也同飽受假新聞之害，也幾乎在選前扭轉局勢。其中在選前造成重大效應的「假新聞」包含以下幾則：[16]

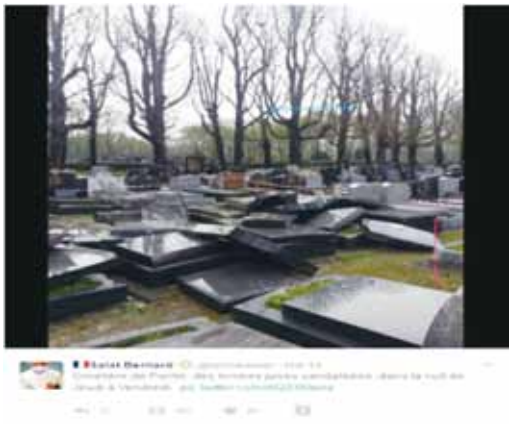
一、候選人馬克宏(Emmanuel Macron)將在法國海外一個馬約特省(French region of Mayotte)成立回教區，這一假新聞對反移民與反回教的選民產生反對投票給馬克宏的效應。

二、猶太教墓園中的許多墓碑遭到毀損與推倒的照片，被假新聞直指對於猶太人的褻瀆。後經證實係因一輛卡車為迴避小車而衝撞進墓園之意外。(圖三)

三、一則「莫斯科當局將協助候選人樂彭(Marine Le Pen)贏得大選」假消息在推特上瘋傳4千次。由於美國總統大選早在法國大選近半年前傳出俄羅斯介入，因此，此一消息便成功在法國發揮效應。

四、400個推特帳號轉傳「蓋達組織表態支持候選人馬克宏」。回教激進份子支持候選人負面效應，其負面效應可想而知。

另外，法國總統候選人樂彭陣營在選前甚至將游擊戰法運用在網路上，透過大量影音及照片對敵陣營進行飄忽、閃躲與重點打擊。[17]顯見這樣超越以往透過電視、報紙及廣



圖三　推特的發文與照片
圖片來源：http://www.bbc.com/news/world-europe-39495635

15 中華傳播學會，〈新聞媒體在臉書-社群編輯的引言框架研究〉《國立政治大學華傳播學會》， http://ccs.nccu.edu.tw/word/HISTORY_PAPER_FILES/315822017.pdf (檢索日期：2017年9月19日)

16 BBC News, “Fact-checking fake news in the French election”, BBC, http://www.bbc.com/news/world-europe-39495635 (檢索日期：2017年9月19日)

17 Mark Scott, “In French Elections, Alt-Right Messages and Memes Don’t Translate”, The New York Times, https://www.nytimes.com/2017/05/04/technology/french-elections-alt-right-fake-news-le-pen-macron.html (檢索日期：2017年9月20日)

播等傳統作為，網路攻防戰已成為現今高度數位化的社會重要的政治操弄手法之一。

一語外洩，全軍覆滅

除混淆視聽外，廣受全球及我行政機關與軍事單位使用的即時通訊軟體「LINE」，擁有全球4.7億用戶，已是每日工作聯繫與資訊傳遞必備工具之一。[18]究其原因，一方面是因各機關體制內提供的平台必須經過重重行政程序申請與核准，既不便又耗時。另一方面是傳送檔案大小不受限外，即時又便利。因此也造成多數人尋求體制外的管道作為業務聯繫用，卻嚴重忽略了架設於「不明地點」的主機伺服器，完全將個人資料、業務聯繫、公務資訊暴露於他人手中。[19]此外，擁有10億用戶的中共通訊軟體微信(WeChat)，許多人平常付款、轉帳、醫院掛號、發表文章和照片，都靠微信傳達分享。日前有外媒稱用戶聊天內容全遭中共監控，最近微信也發出聲明表示，用戶的個人資料和私人聊天內容，若有需要將被提供給中共當局。[20]

綜合上述美、法國大選及通訊軟體普及的研究，顯示幾件應警覺的事實：

一、網路資訊針對閱聽大眾宣傳，恰與中共三戰中的「輿論戰」及「心理戰」不謀而合，中共透過對我閱聽大眾常接觸的媒體、報紙、雜誌、社群軟體等平台，一點一滴傳遞統戰思想，讓盲目的民眾自然而然地吸收從而受影響。

二、我軍事單位及人員，早已透過即時通訊軟體業務聯繫多年，這些資訊經過有心人士悉心排列組合後，便可對我單位士氣、戰力、位置、編裝、任務甚至對於長官的信仰與埋怨等輕易拼湊出全貌。

三、任何持有智慧型手機的人，均能在自己的手機上編輯一則謠言、呼籲、請求、募款與假消息，然後一鍵發送給任何一位朋友(或群組)。且LINE空間裡最常發生的就是「不經查證，盲目轉發」。假消息與謠言之多，罄竹難書(圖四)。在不明究理轉發之後，就開始產生一傳十，十傳百倍數成長的傳遞效應。輕則造成食安恐慌，商家困擾或單位主管出面澄清，重則恐因洩密造成國破家亡，全軍覆滅。

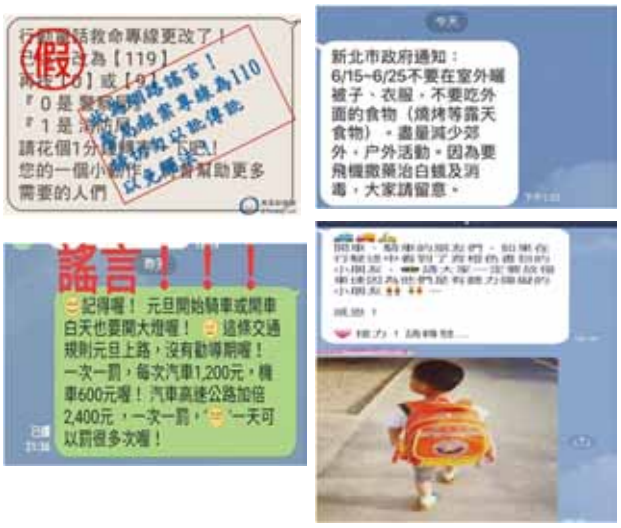
兵馬未動，網攻先行

當北韓導彈試射屢次失敗時，究竟是因為技術工程上的缺陷還是其他原因所致？雖然美國當局從未公開表示針對北韓試射進行任何干擾，但根據美軍現役或退役部隊官員及卸任國會議員的證詞與來自美國重要盟友的資深官員公開聲明表示，美軍正在積極地

18 蘇文彬，〈LINE推出滿3週年，家族App全球下載次數破10億〉《iTHome》，http://www.ithome.com.tw/news/88944 (檢索日期：2017年9月20日)

19 LINE官方聲明稿表示，其伺服器地點未曾公布。 http://official-blog.line.me/tw/archives/35059580.html (檢索日期：2017年9月20日)

20 新聞，〈微信遭全面控制！用戶資料會傳回中國政府〉《自由時報》， http://news.ltn.com.tw/news/world/breakingnews/2196590 (檢索日期：2017年9月20日)



圖四　網路謠言，無奇不有。多數人完全不加查證直接轉發，傳遞無效資訊既沒意義，也構成生活上無謂的騷擾，甚至對社會造成負面效應

採取這種網路攻擊的策略。前英國外交大臣今年告訴英國廣播公司，他非常堅定地認為美國通過網絡方式多次成功地阻斷了北韓飛彈測試並使之失敗。此外，澳洲新南威爾士大學網絡安全中心教授格雷格奧斯丁(Greg Austin)表示：「美國政策明確地制定網絡能力來使敵方彈道導彈失效。」[21]

此外，美國海軍退役將領亞契梅西(Rear Admiral Archer Macy retired)於2015年在華府智庫國際戰略與研究中心參加「2015飛彈防禦研討會」時表示，防禦計劃必須能足以因應區域內彈道飛彈打擊的能力，這些能力包括阻止發射，干預飛行，影響航道直到目標選定，以及破壞它所攜帶的彈頭，並使其失效。[22]目前，美國國防部正在開發各種不同方法來實現這些效果。主要手段就在於美國國防部正在積極開發技術，透過網路攻擊手段使導彈發射失效，干擾飛彈飛行路線或導航系統，甚至摧毀彈頭。另一位專家表示，飛彈發射過程中有很多事情可能出錯。所以即使美國利用網路攻擊讓北韓飛彈失效，這一切過程是無法從飛彈外部得知內部控制系統出了問題。而且北韓也永遠無法證實是美國所為。[23]

這被美國視為可與傳統彈道飛彈防禦系統結合使用，又能節約數億美元成本，既廉價又高效的措施。(圖五)

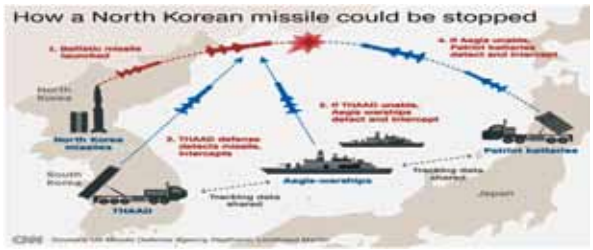
相對地，窮兵黷武的北韓也握有相當程度的網路攻擊能量，堪稱名列世界前10名。[24]根據一份國營國防技術分析報告指出，北韓的網絡攻擊具備擊潰美國太平洋司令部電腦網絡的能力。據國防科技與質量局(Defense

21 Joshua Berlinger” Could the US take out North Korea's missiles before launch?”, CNN, http://edition.cnn.com/2017/04/18/asia/cyber-missile-defense-north-korea/index.html (檢索日期：2017年9月20日)

22 CSIS, “2015 Missile Defense”, CSIS, https://csis-prod.s3.amazonaws.com/s3fs-public/event/151204_full_spectrum_transcript.pdf (檢索日期：2017年9月20日)

23 Will Worley, “North Korea's failed missile test could have been caused by US cyber-attack, expert suggests”, Independent, http://www.independent.co.uk/news/world/asia/north-korea-missile-test-fail-us-cyber-attack-barack-obama-kim-jong-un-intervention-a7669686.html (檢索日期：2017年9月20日)

24 Apdf, “Decoding North Korea’s Cyber Warriors”, APDF Magazine, http://apdf-magazine.com/decoding-north-koreas-cyber-warriors/ (檢索日期：2017年9月20日)



圖五　傳統飛彈防禦體系，多重部署避免攔截失效，但須耗資數億美元
圖片來源：CNN網站，http://edition.cnn.com/2017/04/18/asia/cyber-missile-defense-north-korea/index.html

Agency for Technology and Quality〉報導，美國國防部最近一次模擬顯示，北韓平壤若發起全面網絡攻擊有可能對美國本土電力系統造成損害的同時，也有能力癱瘓美國太平洋司令部的指揮中心。而美國太平洋司令部下轄四個指揮部，計有美國海軍太平洋艦隊，美國空軍太平洋指揮部，美國陸軍太平洋指揮部和美國海軍陸戰隊太平洋指揮部。因此，司令部一旦遭受網路攻擊而癱瘓，則美軍在太平洋各軍的指管與用兵將面對嚴峻的挑戰。

國防科技與質量局也指出，平壤的網絡攻擊能量與技術在網路駭客領域極富聲譽，2013年一次針對南韓大規模襲擊事件之後，韓國三大銀行，其附屬公司，三家電視台等，共計感染了大約4萬8千台電腦。總計這次襲擊造成約7.56億美元的損失。[25]上述這些網路攻防，你來我往，堅決否認外，而整過程並未有任何武裝軍事人員與敵接觸與戰鬥。

缺乏意識，引狼入室

綜合上述所有入侵與攻擊事件的發生，其肇因多半始於使用者在沒有分辨電子郵件真假前，就點擊了信件內所附上的連結或附件。一旦點擊或開啟附件，便自動透過惡意程式開啟遠端連線、開啟使用者電腦後門或者植入病毒程式。智慧型手機在這種攻擊模式下，手機將可能被自動開啟錄影或錄音功能，或者手機內資料庫自動外洩。有心人士一旦握有你的私密檔案、照片或資料，便能對你進行勒索、脅迫與利用。

這樣的手法稱為「釣魚郵件」(Spear Phishing或Phishing mail)，一封來自假冒使用者所熟知的上司、同事、親朋好友之名的寄件者，已吸引人的標題或檔案內容誘發使用者查看附件或是點擊信中連結，攻擊行動就此生效。

而企業內員工通常都是促成網路攻擊的主因，以釣魚郵件方式誘騙使用者點擊的成功機率高達40-50%，而眾多網路攻擊手段中，採釣魚郵件方式佔了95%。就是因為缺乏安全意識與經驗，輕易接受陌生郵件邀請、開啟附件與點擊不明連結等。根據統計，在網路社群平台上，僅有24%的人會完全拒絕陌生人的邀請，只有36%的員工有自信分辨釣魚郵件。而在企業界，僅有39%的

25 Maha Hamdan, “NK hackers could disable US Pacific Command- Report”, LinkedIn, https://www.linkedin.com/pulse/nk-hackers-could-disable-us-pacific-command-report-maha-hamdan (檢索日期：2017年9月20日)

員工在企業內接受每年超過一次的資安防護意識訓練。[26]

此外，避免安裝不明來源的應用程式(APP)、未授權的軟體及瀏覽可疑網站。根據媒體報導，中國大陸江蘇省消費者協會公布調查顯示，市面上有大量手機應用程式未經用戶同意便可自動獲取個人資訊。隨機實驗顯示，隨機測試 100 多個 APP，就有 79個可獲取定位許可權，甚至有 14 個可以監聽電話和掛斷電話。另外包括定位、獲取手機資訊、日曆、相機、錄音、讀寫手機記憶體、系統設置、後台彈出介面等 8 項內容，手機自動默認勾選，可以在安裝時自動獲取許可權。這些許可權獲取是在不知不覺中完成的，消費者甚至完全看不到許可權設置，軟體就已經自動安裝完畢。[27]

在各種服務要求註冊帳號密碼時，務求不同服務使用不同帳號密碼，避免同一組密碼運用於多個服務的註冊帳號上，並且提高密碼複雜度以外，還要能時常更換。要做到這點確實不易，但卻是 最基本的自保方式之一。

觀念為先，技術墊後

接連不斷爆發的資安事件，攻擊目標已從商業組織延伸到政府機關、基礎設施，嚴重威脅國家安全與百姓生命安全。迫使各國政府均採取行動以制定更嚴苛的安全措施因應資安即國安的時代。以美國政府為例，2016年7月公布重大資安事件發生準則，並指派聯邦調查局、國土安全部、國家網路調查聯合行動小組，做為重大資安事件的主要執法、調查單位，以有效對抗各種突如其來的資安威脅。而國土安全部則負責回應相關行動，如提供受害單位必要技術援助以確保其資產不致受損或協助控制損害。至於情報相關支援，則由直接隸屬美國總統的國家情報總監負責相關統籌。[28]

趨勢科技調查指出，國人使用多種裝置上網，喜歡瀏覽社交網站、網路新聞及影片，但資安防護的意識不足，台灣名列全球惡意網站造訪的第5名。國人喜歡上網尋找娛樂內容、與親友聯絡、搜尋資訊，連帶使得面臨的資安風險大增。分析全球造訪惡意網站的國家地區，美國以29%位居第一位，其次為日本的16%，第3名之後大致約4%左右，依序為法國、澳洲、台灣、義大利、中國、印度。台灣人口僅有2,000多萬，但在造訪惡意網站的全球排名上卻能和法國、澳洲、印度、中國等大國平起平坐。皆因許多

26 Daniel Humphries, “Phishing Scams: Why Employees Click and What to Do About It”, Software Advice, http://www.softwareadvice.com/security/industryview/phishing-scams-report-2015/ (檢索日期：2017年9月20日)

27 林厚勳，〈中國多款知名APP遭爆暗藏後門，定位竊聽樣樣來〉《科技報橘》， https://buzzorange.com/techorange/2017/08/24/iqy-illegal-monitor/ (檢索日期：2017年9月20日)

28 陳文義，〈美政府首度發表重大資安攻擊回應準則〉《iThome》， http://www.ithome.com.tw/news/107364 (檢索日期：2017年9月20日)

民眾頻繁使用社交網站、網路新聞、影片，駭客便藉熱門新聞議題、關鍵字搜尋、影片散布惡意程式或釣魚連結，以社交網站、即時通訊做為散佈的管道。民眾資安意識未提高之下，誤觸資安地雷。即便瀏覽器、防毒程式已提出警告，仍有民眾不以為意，顯示資安防護意識不足。[29]

美國國防部及各軍種近年對外舉辦漏洞偵測比賽，以美國空軍為例，為獎勵高手，賽前共募集3百萬美金吸引國內外白帽駭客高手協助挖掘漏洞。視漏洞嚴重性頒發獎金，個人最高可獨得1萬5千美金。[30]

而我國民間資訊技術與駭客能量充沛，若能考慮善用民間力量，與之交流、合作、取經甚至也提供有利條件商請技術單位對我行政機關與軍事單位實施漏洞掃描與偵測並及時修補，亦能有效防杜重大攻擊事件在出其不意下發生而措手不及。

結　　語

科技帶來的生活便利，以及我們重度仰賴資通科技的情況下，我們已無法回到過去白紙黑字的平面媒體時代。面對當今設計精緻、攻擊精準、行跡匿蹤、猖狂散布的網路攻擊行為，使用者必須時時刻刻心存懷疑，在填寫個人資料或系統要求提供個資前，必須小心檢視來信者或發送者的真實身分，同時以交叉驗證的方式求證。

在國安與軍事作為上，仍以明確定義威脅優先，再制訂國家網路安全戰略以指導軍事作為之模式推展。然後再加強對於資訊安全教育的深度與力度，勝於限制與封鎖便利的服務。

雖然在網路空間敵暗我明，難以察覺，但「勝兵先勝而後求戰，敗兵先戰而後求勝」，我們當善用民間資源軍民合作，預先創造有利態勢，以求先勝而求戰。

作者簡介

宋連海中校，陸軍官校86年班、美國海軍資料系統軍官班88年班、美國陸戰隊遠征作戰高級班92年班、新加坡營級情報軍官班94年班、美國陸戰隊通信初級軍官班97年班、美國陸戰隊指揮參謀學院100年班、國防大學戰略研究所103年班。曾任排長、連長、學員隊長、教官、美國華府智庫大西洋理事會訪問研究員。現任國防大學海軍學院陸戰隊中校教官。

29 蘇文彬，〈趨勢：愛上網、資安意識不足，台灣名列全球惡意網站造訪第5名〉《iThome》，http://www.ithome.com.tw/news/91276 (檢索日期：2017年9月20日)

30 Jared Serbu, “In DoD first, Air Force launches bug bounty open to foreign hackers”, Federal News Radio, https://federalnewsradio.com/air-force/2017/04/in-dod-first-air-force-launches-bug-bounty-open-to-foreign-hackers/ (檢索日期：2017年9月20日)