漫談關鍵基礎設施保護

華梵大學資訊管理學系特聘教授 朱惠中

前言

「關鍵基礎設施(Critical Infrastructure, CI)」，係泛指一個國家為了維持民生、經濟與政府等相關公私部門之合作運作而提供之基本設施與服務，其中包括實體的環境、設備及以資通訊為基礎之系統，為重要社會基礎功能所需之基礎建設。諸如：公民營電信、電力、能源、水資源、農業、金融、醫療、交通、緊急救助及政府設施等。而「關鍵基礎設施保護(Critical Infrastructure Protection, CIP)」，則代表保護關鍵基礎設施(CI)之政策與作為，另因「關鍵資訊基礎建設(Critical Information Infrastructure, CII)」，為支持關鍵基礎設施(CI)所需之資訊系統，關鍵資訊基礎設施保護(Critical Information Infrastructure Protection, CIIP)，則是保護關鍵資訊基礎設施(CII)之政策與作為。

2001 年美國發生舉世震驚的 911 恐怖攻擊事件，恐怖組織利用網際網路做為指揮通訊工具，以民航機分別衝撞位於紐約的世貿大樓和華府的五角大廈，造成慘重傷亡並癱瘓美國國土防衛及金融體系。在此震撼全球的事件之後，世界各國無不思考國家關鍵基礎設施安全之防護；然而隨著網際網路科技的日新月異，業已提高了攻擊行動的不可預測性，也暴露出關鍵基礎設施的弱點。因此，如何規劃更完善的防護計畫以面對愈來愈多的挑戰與威脅，如何強化資通訊安全的認知與教育訓練，已成為各國亟需面對的課題。

我國行政院體察世界已開發國家的規劃與發展後，深覺我國應與國際先進國家接軌，更因 2017 年世界大學運動會(世大運)將於我國舉行，為求能讓世大運順利進行，早於民國 103 年 12 月 23 日頒布「國家關鍵基礎設施防護指導綱要」，其目的在建立各機關風險評估之觀念與技能及撰擬防護計畫之能力，並藉由舉辦演練來驗證上述防護策略及部署是否到位，進而提升關鍵基礎設施的持續營運韌力及深化國家關鍵基礎設施之防護能量。

「關鍵基礎設施」被攻擊案例彙整與分析

經綜整及分析近年來全球各主要國家遭受關鍵基礎設施的攻擊，可將驅動或執行對關鍵基礎設施的攻擊者，分為以下 5 類，並略述於次：

一、 國家情治機構或專業組織(Nation State)

(一) 運用國家的資源對敵方工業控制系統(ICS)或數據採集與監控系統(SCADA)之資產進行攻擊。

(二) 美國與以色列雙方政府合作，發展 STUXNET 病毒，破壞伊朗核武發展相關設施與環境，將國土安全的攻防首次提升到了網路攻擊層級；另如真實紀錄片《零日網路戰》中揭露美國、以色列秘密合作一項名為「奧運計畫」的網路病毒行動，而這個超級病毒，也被資安領域專家稱為「網路世界裡的佛地魔」，是一個不能說的名字等案例，均屬此類。

二、 被攻擊組織之內部人員(Insider)

(一) 組織內部之成員，因不滿工作環境或待遇及原先期待的目標與理念不同所採取的報復行為，因彼等熟悉基礎設施的資產及其系統之弱點，並具有較高資料存取權限，故對關鍵基礎設施的威

脅與破壞甚大。

(二)　前美國中情局職員史諾登，因報國理念加入美國中情局，惟日後發現政府監控人民情資的內幕，與其當初為國服務的精神與理念不符，便在香港把美國「稜鏡計劃」(PRISM)的資料透漏給英國衛報及美國華盛頓郵報，引起全球震驚並遭到美國通緝，最後只好逃到俄國尋求庇護，即為此類。

三、　國際犯罪組織(Organized Crimes)

(一)　就關鍵基礎設施的觀點而言，國際犯罪組織成員係利用「惡意軟體」來進行有關金融領域的網路犯罪行為，與傳統所進行的自殺攻擊、販毒、爆炸等暴力行為或恐怖攻擊不同，此類犯罪組織的核心目標為金錢，其方法為雇用第三方犯罪組織的成員，針對關鍵基礎設施的資產進行恐嚇與勒索，以達其目的。

(二)　近期犯罪集團透過第一銀行倫敦分行資訊系統內網遭外網入侵之資安漏洞，遠端操控盜領現金數千萬元，即屬此類。

四、 恐怖主義組織

(一) 該組織以破壞關鍵基礎設施為目標，企圖對目標或受害人以外的人物或團體造成具傷害性的心理影響，並利用傳媒曝光之機會以達到最佳的宣傳效果，進而影響目標觀眾及達到短期或中期的目的，並進一步追求長期的最終目的。

(二) 2008 年大陸舉辦北京奧運期間，相關新聞報導及體育網站成為新型態網路攻擊的目標，大量散布惡意程式，藉以竊取個人或企業的機密資料，並破壞公民營電信、電力、能源、交通等服務；此外，如敦倫地鐵爆炸案及孟買恐怖攻擊等案例，犯罪團體成員間利用公民營電信進行通訊及傳播犯罪事件，均屬此類。

五、 激進駭客(Hacktivist)

(一) 激進駭客的出發點是政治動機而非金錢，渠等認為某些組織跟自己的理念不合，故去對該等組織的電腦網路發動攻擊，以癱瘓該等組織的電腦網路。

(二) 駭客團體「匿名者」(Anonymous），曾於

2012 年舊金山灣區捷運系統管理局關閉手機服務，以防止人群遊行抗議警察在捷運上射擊之行為時發動攻擊;104 年我國政府推動高中課綱微調時，癱瘓包含教育部、經濟部、國民黨等多個網站，均屬此類。

我國應有的作為

從關鍵基礎設施的攻擊案例，已凸顯出關鍵基礎設施所潛藏之脆弱性,以及國家訂定相關保護措施之必要性。因此，近年來歐、美等各國政府均高度重視，並紛紛提供相當之預算，以加強「關鍵基礎設施保護」及「關鍵資訊基礎設施保護」之措施。為達成上述目標，對「關鍵基礎設施保護」之認知與教育訓練應為落實的基石；我國行政院國土安全辦公室每年聘請專家學者對約 15 個重要單位進行指定演練及訪評，期能發掘潛藏之脆弱性及提前找出解決或防禦的方法，惟上述單位或因單位任務及性質不同，或因單位資源之差異，或因認知之差異，對關鍵基礎設施保護的定義、內涵及應有的做為尚有若干落差，經綜整相關資料後，對前述之落差提出建議，包含「關鍵基礎設施」的威脅範疇;「關鍵基礎設

施保護」的定義、參與部門、層級；「關鍵基礎設施保護」各層級(國家層級、領域層級及企業層級)業務承辦的專業單位、各層級業務落實的標準作業程序(SOP)、所需的資源及持續營運之韌性與相依性；資訊分享中心(ISAC)、電腦緊急應變團隊(CERT)、資安監控中心(SOC)及資安託管服務供應商(MSSP)的層級、定位與職掌。

結語

關鍵基礎設施保護不僅是領域內各機構的協同保護，亦牽涉到跨領域的合作。例如金融與醫療系統仰賴電力與電信以維持資訊機房、設備的運作，亦仰賴網路系統傳遞資訊。一旦這些底層系統失效，將嚴重影響金融與醫療體系的運作，可見關鍵基礎設施的任一缺口對於民眾生命財產、生態環境、經濟、政治與國家安全均會產生重大的影響。

安全的意義是管理風險，面對變化莫測的大環境，能夠事先模擬各種可能面對的風險，事先防範才能快速應變、降低損害，這對政府機構是項挑戰，更有賴於機關首長與全體工作人員的專業與態度。

再者，對企業而言，面對安全的態度，等同面對危機的

態度，輕忽安全問題也會輕忽危機引發問題的廣度與深度。一銀事件為我們詮釋了，企業經營如果只看經營數字效益，不僅安全不會做好，對社會更無法帶來實質效益。

國際社會已就核生化武器達成有關協議，卻未曾討論影響更全面性的網路武器，網路武器之危險遠高於核生化武器或軍備競爭，期未來能透過公開討論以建立全民共識，避免網路戰可能帶來的嚴重後果。

參考資料

一、行政院國土安全辦公室，國家關鍵基礎設施防護指導綱要。

二、行政院科技顧問組，關鍵資訊基礎建設保護政策指引。

三、柯孝勳，我國關鍵基礎設施防護工作之推動概況。

四、行政院國土安全辦公室，國家關鍵基礎設施防護(CIP)實務訓練概要。

五、趨勢科技，認識駭客等，

http://blog.trendmicro.com.tw/?p=1857。

六、*iThome*, 聯合新聞網(udn)相關報導。