2017伊斯蘭國威脅仍在且強

■ 法務部調查局專門委員　陳能鏡

伊斯蘭國領土日漸喪失，不再可能發動大規模恐攻，但受到暴力意識鼓舞的個人，以及返鄉的外國聖戰士，仍將伺機發動攻擊，對各國國家安全仍具重大威脅，亦衝擊我政府新南向政策。

壹、軍事反擊，哈里發國瀕臨瓦解

伊斯蘭國（IS）前身「獨一真主與聖戰組織」屬蓋達組織分支，利用伊拉克宗派衝突及政府貪瀆腐敗而坐大，2011 年更趁敘利亞內戰，蠶食鯨吞領土，2014 年 6 月宣布「建國」，定都於敘利亞拉卡市（Al-Raqqa），該市成為中央指揮中心，伊拉克的第二大城摩蘇爾市為「陪都」，利比亞的蘇爾特（Sirte）為「備胎首都」，一旦伊、敘失守，則轉進蘇爾特，圖謀再起。

2015 年 11 月的巴黎恐攻案強化西方國家殲滅伊斯蘭國的決心，西方國家採取強力空中轟炸以支援及掩護當地國地面部隊之戰略，同時對敘、伊及利三國境內 IS 據點展開攻擊，步步向前述三都包圍進逼。首先於 2016 年 8 月 2 日攻進備胎首都蘇爾特，隨後摧毀 IS 的總部，但遭到 IS 聖戰士頑強反抗。

2016 年 10 月 17 日，以伊拉克政府軍為首聯軍展開對摩蘇爾市的攻擊，同年 11 月 6 日阿拉伯—庫德族聯軍亦大規模攻擊拉卡市，雙城戰役都採取先包圍孤立再進城解放的戰術，在美國空中轟炸支援下，均能迅速攻占城市周邊村莊及小鎮。

貳、領土喪失，仍具威脅

一年前，IS 是地表武力最強大、經費最富足的恐怖組織，但在美、蘇等國強力轟炸下，領土、油田、銀行金庫已喪失泰半，赴敘、伊的外國聖戰士亦急速陡降，依美國國防部說法，已由 2015 年早期每月 2000 人降為日前每月 200 人；至於宣傳影片，依美國西點軍校反恐中心報告，由前年 700 部降為去年 200 部，今日的 IS 雖為維持正常運作而掙扎，但其威脅性仍在且強，其原因分述如下：

一、激進意識延續數代：英國負責國內安全及反情報的軍情五局局長帕克接受英國「衛報」專訪時表示，伊斯蘭激進分子的威脅是持久的，在英國境內約有 3000 人接受伊斯蘭激進意識的本土暴力分子，且於過去 3 年中曾發動 12 件恐攻未遂案。另在伊、敘戰區企圖對英國煽動恐攻的 IS 戰士中，外國聖戰士有 4 萬人來自 85 國，返回母國者部分仍有興趣繼續執行恐攻任務。

二、不安及內戰仍滋養恐怖主義：伊拉克政府軍貪腐嚴重，吃空缺、扣軍餉，士兵叛逃，人力不足，無法獨力作戰，只得借重庫德族戰士、什葉派民兵及遜尼派部族戰士，但各方的敵意及不和存在已久，歷經此次戰亂，益加難解。至於敘利亞內戰，涉及代理人戰爭及教派領導權，更是複雜難解，中東仍將動亂不安，持續滋養伊斯蘭激進主義。

三、川普政策弱化全球反恐聯盟：川普意外贏得美國第 45 任總統大選，任內將採行保護孤立主義，以美國本土為優先，不再充當世界警察，緊縮海外反恐戰線龐大軍費，勢將弱化全球反恐聯盟，帶給 IS 等恐怖組織喘息及再起機會。另一方面，IS 為彰顯存在感及繼續吸引年輕人加入，勢將加強指揮全球孤狼恐怖分子發動本土恐攻。

參、在東南亞之發展衝擊我新南向政策

新政府執政後，為反制我國在經貿上過度依賴中國大陸，力推「新南向政策」，鼓勵國人、廠商前往東南亞、南亞國家投資、工作及人才交流。此際，相關各造應將恐攻、海盜、反華暴動、排華運動等列為投資風險、旅遊平安的評估指數，以確保生命及財產安全。

據「國際海事局」（International Maritime Bureau）統計，全球超過 1/3 海上攻擊或攻擊未遂事件發生於東南亞，該區已取代東非，成為全球海盜最猖獗地區，菲律賓恐怖組織「阿布薩亞夫」（ASG）是最大主謀。國人記憶猶新的臺商張安薇綁架案，幕後主謀亦是阿布薩亞夫組織。

除了海上及陸上綁架人質外，ASG 另一項生財工具是向商家或個人強徵「革命捐」（Revolutionary Taxes），每月向商家收取 100 美元至 200 美元不等之保護費，個人則徵收 80 美元。

菲國境內至少有 4 個恐怖組織向 IS 宣誓效忠，經過年餘的討論與協調，IS 於去年 1 月正式宣告，成立「菲律賓伊斯蘭國」，統合各組織，並以 ASG 在巴西蘭島的頭子 Isnilon Hapilon 為總首領。

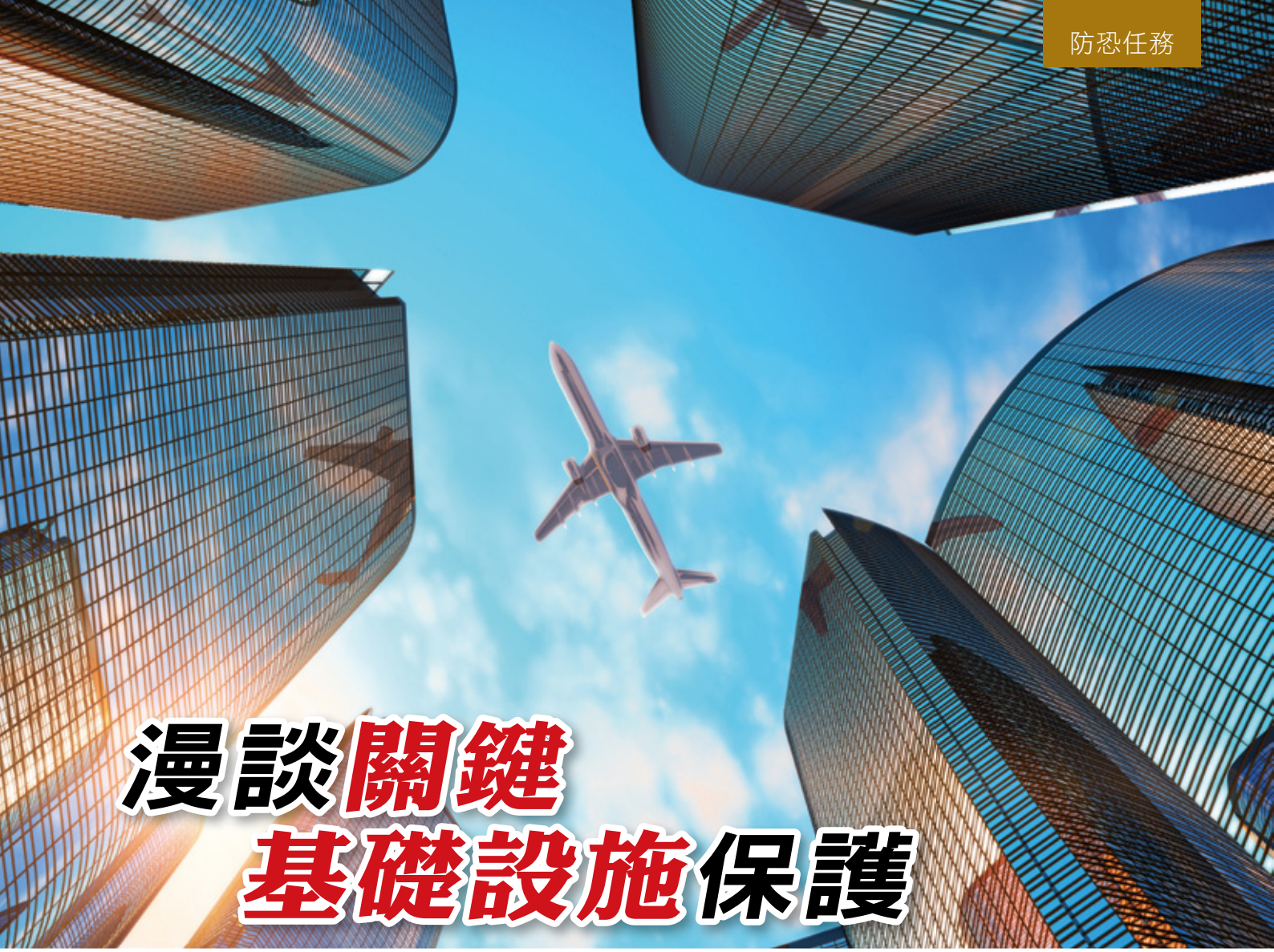
在馬來西亞，已有 7 個恐怖組織與 IS 有關連。去年 1 月，馬華公會總主席廖中萊甚至警告，IS 企圖滲透當地華人社會，傳布恐怖主義，也企圖召募當地華人穆斯林，達到擴大影響力的目的。至於印尼，澳洲司法部長去年 12 月曾警告，IS 夢想在印尼建立一個遠方哈里發國，夢想成真的可能性不高，但經過去年 1 月的雅加達恐攻案，至少證明 IS 已在印尼建立永久性的根據地，另去年 11 月 4 日雅加達數十萬穆斯林反省長鍾萬學的示威遊行，證明了激進伊斯蘭基本教義派的當道。另新加坡總理李顯龍前年 5 月即坦言，東南亞已成為 IS 的主要召募中心，威脅不但在遠方，也在近處，東南亞地區正面臨 IS 嚴重的威脅。

據統計有 600 名至 1200 名東南亞青年前往中東加入聖戰行列，並於 2014 年 9 月編組為「馬來群島大隊」（Katibah Nusantara），成為 IS 武裝部隊之一，也是 IS 在東南亞擴張勢力的前鋒部隊。他們一旦返國後，將宣傳激進意識、教授作戰技能、招募人員及策劃、發動或呼應恐攻。

IS 在去年 6 月間已發行馬來語版定期宣傳刊物，企圖激化印尼、馬來西亞、新加坡等國年輕人，先默化為支持者（Supporter）或同情者（Sympathizer），進而型塑為潛在的恐怖分子（Potential Terrorist）。在東南亞地區，IS 的支持者恐達數萬人。

肆、結語

傳統恐怖主義以民族主義為論述基礎，獨立建國是其終極目標，恐攻只是其手段之一。但今日恐怖主義植基於意識形態，以無差別殺人為目標，「受害人不確定性」（Victimization Indiscrimination）是其最顯著特徵，已歸類於新興跨國犯罪，我國應加強國際合作交換恐攻預警情資外，亦在推動新南向政策時須考慮海盜、恐攻等威脅，將這些安全因素列入評估變數之一。



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
健行科技大學資訊管理學系助理教授　陳惠娟

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

105 年度金華演習模擬世大運可能發生之危機應變作為
（圖片來源：http://2017.taipei/files/14-1000-2201,r13-1.php）

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，分為以下五類，並略述於次：

一、國家情治機關或專業組織（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

美國 911 恐怖攻擊事件

（Photo by Robert J. Fisch, Flickr user TheMachineStops, https://commons.wikimedia.org/w/index.php?curid=11786300）

倫敦地鐵爆炸案

（User: FrancisTyers, https://commons.wikimedia.org/w/index.php?curid=214539）

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，如倫敦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、內涵及應有的作為尚有若干落差，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關的協同保護，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，而且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，這對政府機關是項挑戰，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。