漫談國家關鍵基礎設施

CI（Critical Infrastructure）＝國家關鍵基礎設施

是一個國家公有或私有、實體或虛擬的資產，
一旦遭受破壞，恐影響社會運作。

可分為能源、水資源、通訊傳播、交通、銀行與金融、
緊急救援與醫院、重要政府機關、高科技園區等八類。

美國關鍵基礎設施威脅資訊分享框架簡介

■ 行政院國土安全辦公室主任　黃俊泰

值得取經的美國 CI 資訊共享制度

冷戰結束後，隨著安全威脅情勢的轉變，以及資訊科技的快速發展，美國於 1995 年開始以資訊安全的角度，關注關鍵基礎設施保護（Critical Infrastructure Protection, CIP）的重要性，由於美國關鍵基礎設施高達 85% 屬私部門擁有，美國政府早已體認其成功要素在於公、私部門能否充分協力、分享資訊，歷經將近二十年的調整與演進，公、私部門合作建立夥伴關係、資訊共享機制立法、政府組織功能優化、資訊共享環境的建構、各種網路平台的開發與工具運用，以及資訊共享標準的建立，已使得美國在關鍵基礎設施資訊共享制度上累積不少寶貴經驗，值得各國取經。

資訊共享增加 CI 之防災韌性

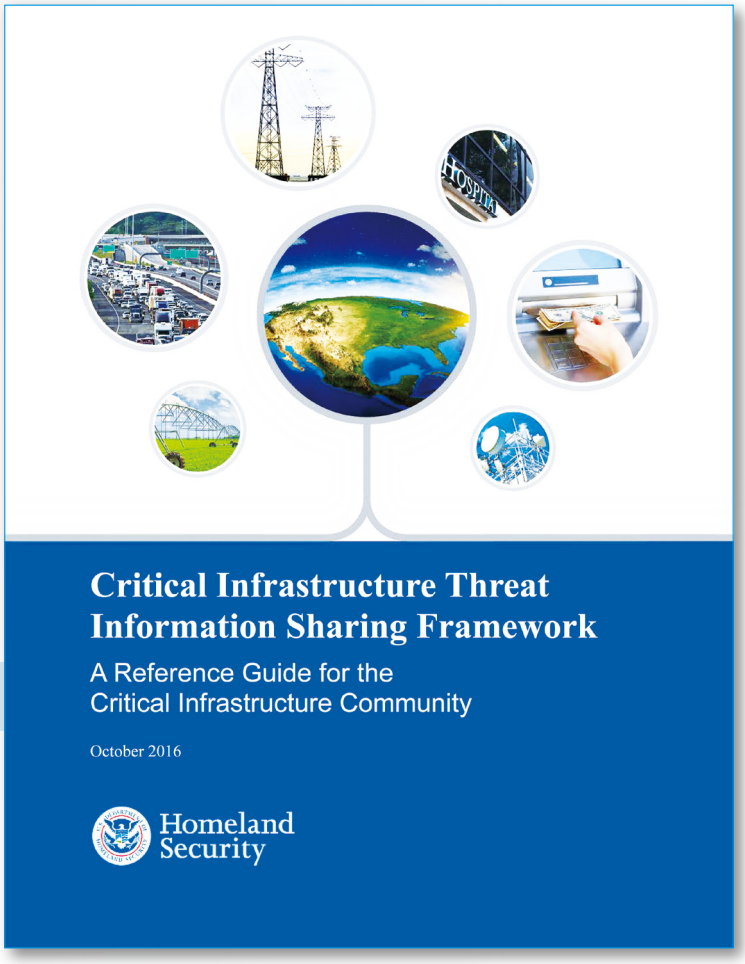
美國民眾對於隱私及自由被侵犯的疑慮，經常因洩密事件而擺盪不安，美國政府因而不斷努力健全資訊分享環境，以建立互信而穩固的夥伴關係，所以非常依賴權責分明的組織、一致的流程標準、多元而友善的分享管道，來促進資訊共享。其中由國家保護計畫局基礎設施保護辦

公室（OIP）營運的國家基礎設施協調中心（National Infrastructure Coordinating Center, NICC），是聯邦政府專用的全天候協調與資訊共享運營中心，當發生影響關鍵基礎設施的事故或事件，而需要國土安全部和國家基礎設施的擁有者及經營者之間進行協調時，NICC 即擔任資訊共享的樞紐來支援這些重要資產的安全性和韌性。

前總統歐巴馬在 2014 年的 21 號總統政策指令中更要求 NICC 須與國家網路安全和通信整合中心（NCCIC）[1] 連結，使各單位間的資訊共享更加順暢，並讓私部門明瞭諮詢服務的窗口，以確保關鍵基礎設施，並使其更具防災韌性。藉由將資訊分類分級的保護，分享管道漸趨多元便利，有助於及時獲得警訊，降低威脅，及早因應，因此能有效消除資訊分享的障礙，私部門共享資訊的意願不斷提升。

美國 CI 資訊分享框架簡介

但是從關鍵基礎設施擁有者和運營商的角度而言，實際上的分享流程如何？2016 年 10 月美國國土安全部發表《關鍵基礎設施威脅資訊分享框架參考指引（Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community）》，清楚交代了美國網路威脅資訊的分享框架與運作機制，並以網路、實體、國際、大型活動等四種類別的實例說明資訊的分享過程，目的在幫助關鍵基礎設施擁有者和運營商以及其他私部門、聯邦和州、地方、部落和領土（SLTT）政府等合作夥伴，了解在各種情況下如何收到和報告威脅資訊。



美國國土安全部發表的《關鍵基礎設施威脅資訊分享框架參考指引》。（圖片來源：美國國土安全部，https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf）

[1] NCCIC（National Cybersecurity and Communications Integration Center）係由網路安全與通訊辦公室（CS & C）營運，下設美國電腦緊急應變小組（US-CERT，服務執法及情報機構，政府單位為主）、工業控制系統網路緊急應變小組（ICS-CERT，與國際及民營 CERT 組織合作）、營運及整合中心（NO&T）、國家通訊協調中心（NCC），整合聯邦政府、情報單位及執法單位資通訊安全情資，並向公、私部門提供 24/7 服務，分享網路通訊威脅資訊並協調公私網域採取緊急應變行動，降低網路攻擊之衝擊。

分享資訊的程序

一旦獲得資訊，政府機關和私部門通常依組織的內部規則、要求和程序的執行步驟，利用正式和非正式管道，傳送到資訊分享平台。該參考指引建議如下七個步驟（請參閱圖一）：

步驟一：發起者獲得資訊

發起者以多種方法（調查、評估和情報收集），從多樣的來源（開放資料、機密、執法、情報、公共和私人）獲取資訊。例如：私人公司的保全人員在其設施或其 IT 網絡上觀察到安全漏洞趨勢；聯邦各級執法部門收集到非法或可疑活動資訊；情報機關經過分析，確定資訊具威脅性等。

步驟二：發起者準備文件並標註保護等級

通常，可透過通用標準整理文件，例如「報告可疑行動（SAR）」規範必備的資料格式與流程，以方便評估作業，另外也必須標記文件機密等級，例如資訊來源為情報單位，通常標記為機密；來自執法單位，則標記 LES（Law Enforcement Sensitive）；含有個資，必須標記 PII（personally identifiable information）。

步驟三：發起者驗證和分析資訊

發起者在能力的範圍內，須結合相關知識，驗證資訊的準確性，並考慮資訊是否符合合作夥伴的正式資訊要求，或者可能對較大的關鍵基礎設施社區有價值。

步驟四：發起人依存取與使用限制提供資訊

根據步驟二的保護標記，發起人須決定誰會看到這些資訊，並依法處理。例如來自情報機關的資訊，而有必要與私部門分享時，由國土安全部或 FBI 將資訊部分內容加以切割或遮蔽，反之亦然；且資訊遞送過程須使用安全的通訊管道，例如「國土安全資訊網—關鍵基礎設施（HSIN-CI）」限定 IP 及雙重身分認證；機密資訊則必須使用批准的機密資訊共享管道和機制來共享。

步驟五：資訊分享中心驗證、評估和分析資訊並傳播

資訊分享中心了解其各種合作夥伴的資訊需求，有能力評估資訊是否需要額外的分析，以及是否應該與其他合作夥伴共享。一旦收到資訊，中心將另進行驗證和分析，並將新資訊與其他知識相結合，並確定是否應將其傳遞給其他合作夥伴，如果是，則須判斷如何限制其使用。

步驟六：降低威脅

關鍵的基礎設施社群接收資訊後，立即進行應變、戰術、和戰略決策，以協助緩解威脅。所採取的行動取決於實體的角色和責任。例如，設施擁有者和經營者可以制定戰術決策來加強保護措施，而協會或負責制定計畫和政策的實體可以開展新的部署及培訓。

步驟七：回饋

資訊共享週期的一個重要部分是向資訊提供者反饋資訊，以提高資訊分析的相關性、實用性和格式。

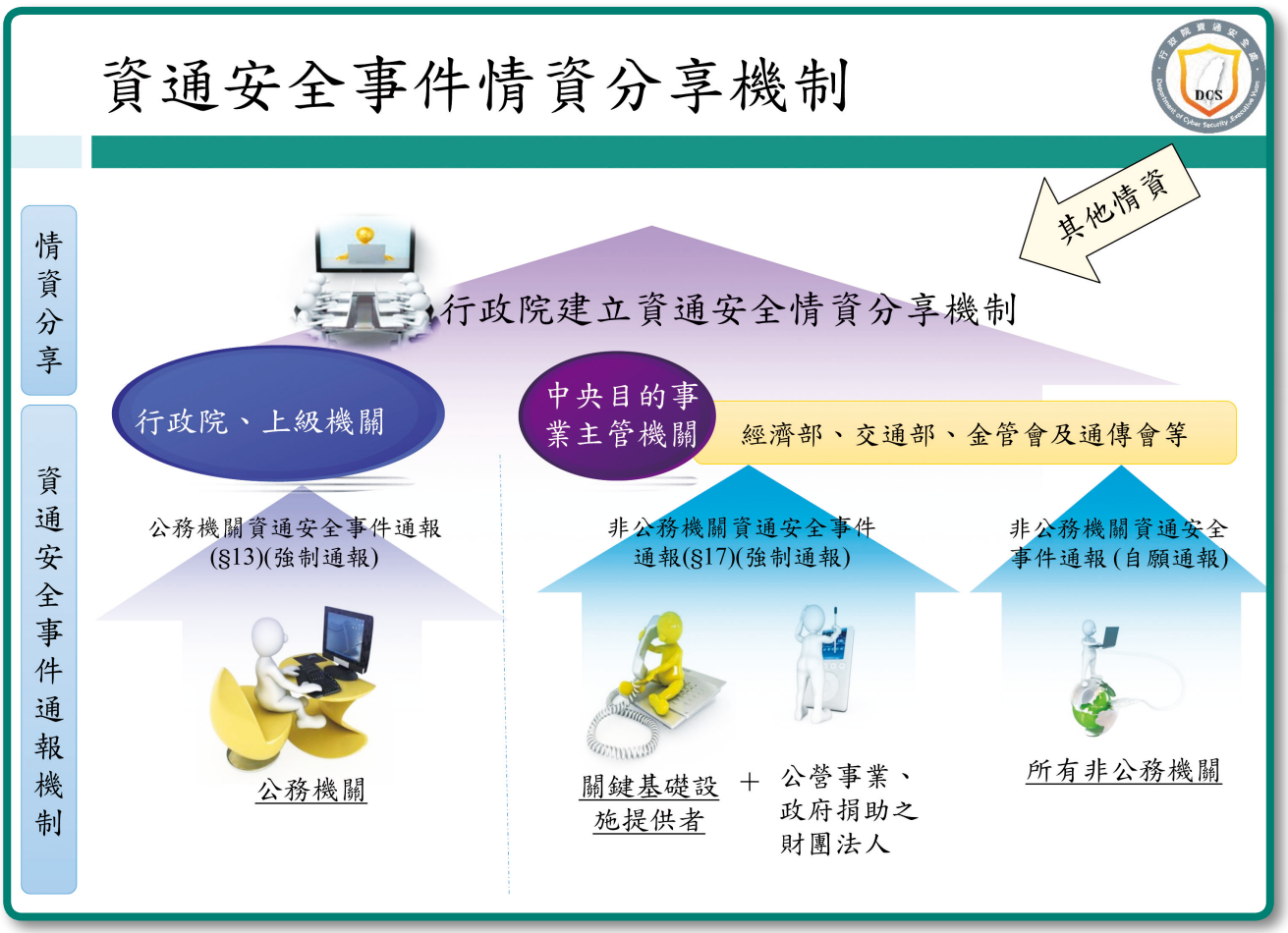
圖一　威脅資訊分享流程[2]

[2] 原圖為《關鍵基礎設施威脅資訊分享框架參考指引（Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community）》P.12 圖二。

結語

從美國關鍵基礎設施威脅資訊的分享框架看來，我國國家關鍵基礎設施的私部門比重雖然較低，但是仍有建置資訊分享平台的需要，以加速威脅資訊的流通，2016 年 8 月 1 日行政院成立資安專責機構資通安全處，於 2017 年推動八大資安旗艦計畫，透過強化關鍵基礎設施的資安防護措施，進一步達到提升整體國家資安防護能力。

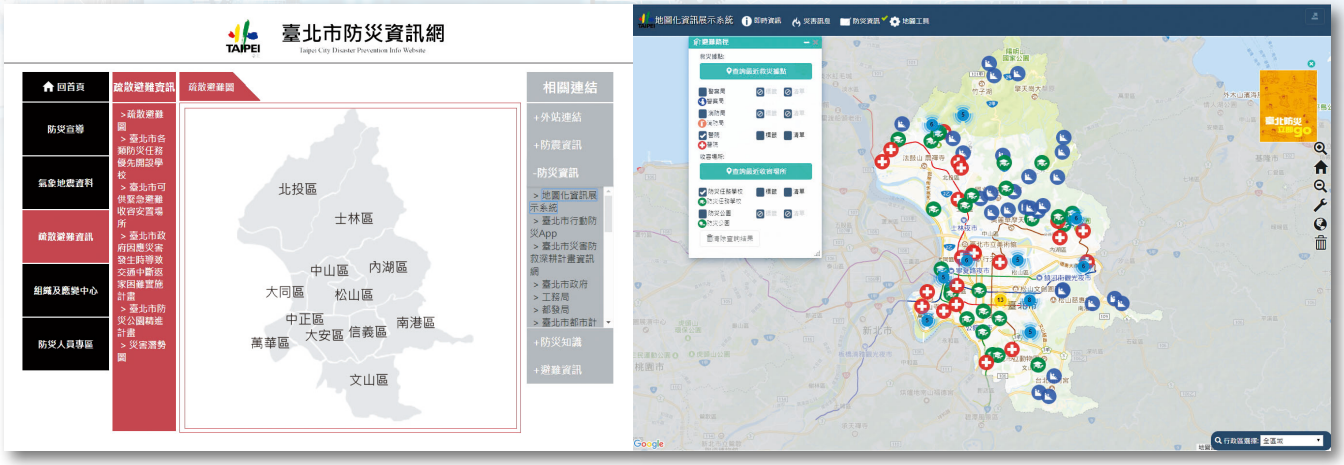
另外，行政院院會也於 2017 年 4 月通過臺灣第 1 個資安專法《資通安全管理法》（下稱〈資安管理法〉），送交立法院審查中。這個法案最大的特色就是，將行政



行政院送交立法院審查的〈資安管理法〉中，明訂關鍵基礎設施提供者應訂定、修正、實施資通安全維護計畫。（圖片來源：行政院資通安全管理法懶人包，https://www.ey.gov.tw/News_Content.aspx?n=F8BAEBE9491FC830&s=26B446DFB5C87E70）

院國土安全辦公室（下稱國土辦）規畫的八大關鍵基礎設施納入〈資安管理法〉的管理範疇中，草案第 15 條規定中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，關鍵基礎設施提供者應訂定、修正、實施資通安全維護計畫。草案第 17 條規定：非公務機關應訂定資通安全事件之通報及應變機制。也就是說，未來包括政府機關、能源、水資源、通訊傳播、交通、金融與銀行、醫院、高科技園區等關鍵基礎設施產業，一旦爆發任何資安事件，皆有責任和義務跟該產業的主管機關通報。

〈資安管理法〉若通過，未來包括政府機關、能源、水資源等八大領域的關鍵基礎設施產業，一旦爆發資安事件，皆必須向該產業主管機關通報。



國家關鍵基礎設施的資訊分享可串聯災防資訊體系，藉由地理圖資判斷彼此相依性，並加速威脅資訊的整合及流通。
（圖片來源：截自臺北市防災資訊網－地圖化資訊展示系統，http://www.eoc.gov.taipei/EOC/EvacuationInfo）

以上這些計畫與法案的推動，與美國發展的軌跡大致相同，先從資安的資訊分享做起，而且已經有具體的成效。至於如何擴大到實體關鍵設施方面的資訊分享，我國於 2013 年由國土辦推動國家關鍵基礎設施安全防護專案，已初步建立國家關鍵基礎建設風險評估、管理與防護的機制，並透過演習與訓練不斷精進，未來在這基礎上，建立資訊分享平台，並據以開發風險評估與管理工具，提供政府與關鍵基礎設施的主管單位，作為設施安全防護方案、緊急應變與復原措施之規劃依據，及資源分配之決策平台，實刻不容緩。但基於機敏性及資安考量，要達到美國國土安全資訊平台提供雙向、多元的資訊分享服務，尚待法規及制度上之長遠規劃。目前可先由基本資料、風險管理、事件案例分析之整理做起，方便檢索及分析，再結合災防資訊體系，提供地理圖資，了解各設施相對位置，以判斷彼此相依性。初期亦可建置網路論壇，嚴格管制使用者身分及網路傳遞的安全，分門別類分享知識、經驗，但仍應限於非機敏性資料，或將個資及機敏部分加以遮蔽，視分享效益再考慮提升系統功能，逐步擴充應用。

「國家關鍵基礎設施防護」的思維與工作面向

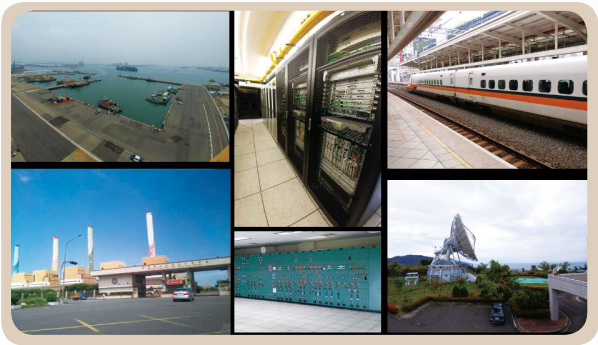
■ 國立聯合大學土木與防災工程學系助理教授　李中生博士

開車返鄉或出遊前，有一件很重要的事必須提醒：須先保養車輛，檢查並確定各項狀況良好，包括引擎、煞車、水箱、電力等系統；也需要確定車裡各項資訊傳輸儀表顯示以及監控系統正常，能夠正確告訴我們檔位、引擎轉速、溫度、油量、電力等控制資訊。然而，就算車輛狀況正常，預備充足的油料與電力也是確保能順利抵達目的地的必要條件。此外，還有一項必要的項目，那就是駕駛。在無人車技術發展成熟之前，缺了駕駛員還是無法成行的。故若我們分析開車出遊這項任務時，執行它所需要具備的條件可以歸納為：車內各項機械系統（實體）、儀表顯示與監控（資通訊），以及駕駛（人員），而燃料與電力則是必要的資源，缺乏前述任何一項條件都將使得這項任務中斷。

而「國家關鍵基礎設施」（Critical Infrastructure，簡稱：CI）所指的即是支持著國家與社會運作所需要的重要功能設施與系統，包括能源、通訊、交通、機場、港口等，而要使這些設施系統能夠正常地運作，同樣必須要仰賴「實體」、「資通訊」控制系統以及「人員」等三類必要條件，而這三類必要條件有各自不同的風險

與安全威脅。若是其中一類遭受災害影響，將進而導致 CI 功能失效，不僅會嚴重影響民眾生活，中斷都市社會運作機能，造成國家經濟重大損失，降低政府聲譽與信用，甚至有可能影響國家安全。

國內外最近幾年發生過多起 CI 防護失當案例，顯示出 CI 一旦失效將造成重大的影響層面與災害損失。因此有必要對這些「CI」進行特別的防護與管理。在我們探討那些設施是 CI 之前，我們必須先了解 CI 防護的思維。



關鍵基礎設施類型。（圖片來源：作者提供）

CI 防護思維

一、安全與韌性

美國推動 CI 防護工作已逾二十餘年，不論是在觀念上以及在作法上都值得借鏡。在 2013 年美國國土安全部提出以「安全（Security）與韌性（Resilience）」為推動目標的國家基礎設施防護計畫（NIPP）[1]。根據美國定義，「安全」是指**「利用實體防護與網路防禦來降低因為入侵、攻擊或天然以及人為災害對關鍵基礎設施所造成的風險」**。而「韌性」的定義則是指**「對於蓄意攻擊、意外，或是天然災害等威脅與突發情況能夠有所準備、調適與因應，以及在中斷後能快速恢復的能力」**。綜整上述描述，CI 的防護工作目標可以整理出以下幾點工作面向來進行說明：

（一）於平時分析威脅來源並進行防護

在 2005 年卡翠納颶風造成重大災害以及後續所發生之重大資安事件後，美國政府即要求以全災害（All-Hazards）的思維來進行分析 CI 威脅並進行防護。

全災害可區分為天然災害與人為災害兩大類，而生活在臺灣對於天然災害的類型並不陌生，包括地質災害以及氣象災害

2005 年卡翠納颶風在美國造成重大災害，不僅數千人在這次災難中喪生，各地基礎設施毀損，經濟損失慘重。

兩類。人為災害，根據美國消防工程師學會 NFPA1600 的分類[2]，則可區分為生物危害、人為意外事件、人為蓄意事件、技術事件以及其他危害等，如表一所示。在這個工作面向中，不僅需要依據 CI 的功能特性與位置，分析來自外部與內部災害威脅的可能性，更需要瞭解威脅一旦發生所可能造成的災害與衝擊影響，進而針對可能遭受破壞的項目進行防護工作。

（二）對於突發事故的處理能夠事前規劃

在此工作面向上，必須掌握設施間的相依性，以及必要的外部資源（如水、電、通訊等），做為分析連鎖性影響的根據。另應該針對不同威脅類別與程度評估可能造成設施失效的狀況、影響範圍與層面，以及災害損失等，並依照災害情境規劃處置對策以及處理程序。

（三）在災害事故發生時能夠有效因應

在此工作面向上，須仰賴有效的災害事故應變組織、機制以及處置對策，更應熟稔應變程序，包括指揮調度在內對各項應變技能進行技術與教育訓練。此外，利用演練與演習驗證、檢討並改善各項處置對策與處理程序，於平時即提升對於各類災害事故的應變能力與技術，以確保在事故發生時能夠有效因應，並降低且限縮災害影響的範圍與層面。

災害發生時，規劃設置災害事故應變組織、機制以及處置對策，可提升救災效率。圖為 2015 年復航空難，臺北市成立災害應變中心，市長坐鎮指揮。（圖片來源：臺北市政府，https://www.gov.taipei/News_Content.aspx?n=F0DDAF49B89E9413&sms=72544237BBE4C5F6&s=AF86AA6116D01948）

平時利用演練與演習可驗證、檢討與改善各項災害處置對策。圖為 2017 年臺北市舉行萬安 40 號演習，演練發生「信義區聯合行政大樓遭敵縱火及挾持民眾狀況」之應變措施。（圖片來源：臺北市政府，https://www.gov.taipei/News_Content.aspx?n=2044902FC839D045&sms=72544237BBE4C5F6&s=E82AD343E540485F）

（四）在功能中斷之後能夠快速恢復

CI 擔負重要功能，因此如何確保在災害事故下能夠持續運作，或是在中斷之後能夠快速的恢復功能，是推動防護工作最重要的目的之一。因此，國際間在推動「CI 防護」的工作上，均已導入「持續營運管理」的觀念，藉由設施功能的允許中斷時間以及目標復原時間，做為持續營運管理以及設計功能恢復手段（如備援）的目標與依據。

二、設施盤點與分級

為了推動 CI 防護工作並有效地進行管理，必須藉由設施盤點與分級建立資料庫。在設施盤點方面，依照系統功能屬性，行政院國土安全辦公室已經將我國 CI 分為八項主領域：能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學與工業園區；而在各主領域下亦再區分次領域，例如在能源領域之下再區分為電力、石油、天然氣、核能、化學材料等次領域。其目的乃希望以領域功能為目標，進行有系統的盤點工作，藉以掌握支持領域功能運作所必要的實體設施與網絡（如供水、供電網絡）、資通訊控制系統，以及關鍵的技術（人員）等。

在設施分級上，不僅需要評估設施的重要性，更需要考慮設施的相互影響關係。在設施重要性上可藉由「功能重要性」、「失效影響」以及「民心士氣影響」三大項目進行評量。功能重要性則建議由政府機關運作、重要資通訊系統、維生與運輸機能、金融秩序、疫病系統、治安與防救、國家重要象徵與資產、重要產業與園區、防衛動員等面向進行評量；在失效影響方面，可由設施價值、影響人數、經濟損失

表一　災害類別與項目

類別	項目
地質危害 Geologic hazards	地震、海嘯、火山、土石流、坡地崩塌等
氣象危害 Meteorological hazards	強風、洪水、暴洪、乾旱、下雪、冰雹、暴風、極端氣候、閃電電擊等
生物危害 Biological hazards	食物中毒、疫病等
人為意外事件 Accidental human-caused events	有害物質洩漏、核能事故、爆炸／火災、交通事故、燃料／資源短缺、機械故障、操作意外等
人為蓄意事件 Intentional human-caused events	罷工、惡意破壞、暴力行為、抗議示威、炸彈威脅、恐怖主義、縱火等
技術事件 Technology-caused incidents	設備故障、設施老舊、網路中斷、網路攻擊、資料遭竊、電力中斷、供水中斷等
其他危害／風險 Other hazards/risk	供應鏈中斷等

CI 防護必須由管理體系與專責單位分層負責推動與落實相關工作，我國目前由行政院國土安全辦公室負責督考各領域的 CI 防護管理工作，推動國家層級威脅情境辨識，擬定國家 CI 管理與執行策略與目標。（圖片來源：中華民國行政院，https://www.ey.gov.tw/cp.aspx?n=9DD1F33EB9A1A6CB、三立新聞）

等進行評量；而在民心士氣影響方面，則由影響國際形象、影響政府聲譽、影響民眾信心等方面評估。藉由上述這三大面向的綜合評估，將使各自領域內設施系統依重要性排序。

三、組織與合作

CI 防護是一項需要持續推動的管理工作，必須藉由管理體系與專責單位，分層負責推動與落實相關工作。我國目前由行政院國土安全辦公室負責督考各領域的 CI 防護管理工作，推動國家層級威脅情境辨識，擬定國家 CI 管理與執行策略與目標。各領域主管機關應建立推動小組，進行領域內的設施與系統的盤點與分級、災害威脅辨識，擬定領域層級的 CI 安全防護計畫，督考所轄的 CI 防護工作，並建立資訊通報與分享機制。而 CI 與系統的營運單位同樣需要導入持續運作的管理方法，擬定 CI 防護管理計畫，執行相關防護工作。唯有如此，才能夠使關鍵基礎設安全防護工作能夠在橫向與縱向上，在跨部門之間整合起來。

結語

若是以人的身體來比喻，CI 就如人體內的骨骼、血管與經脈，支持一個人所要執行的動作。正因為如此，必須要有系統地建立設施資料庫，以系統性的方式進行風險分析後並加以防護。CI 安全防護所推動的是一套風險管理程序，從設定目標、設施盤點與分級、風險評估（威脅、暴露量、脆弱度、後果）、規劃防護優先次序，進而實施防護計畫並且評量實施成效。而在推動過程當中，以「持續營運管理」的方法，在實體、資通訊、人員三個項目上進行風險管理與防護。CI 支持著國家各項重要功能的運作，因此必須要在各層面上提升其耐災韌性，並且對於變動的風險威脅能夠及時調適與因應。

參考資料

1. NIPP 2013, Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (accessed on 2018/1/30)

2. National Fire Protection Association, NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs, 2013 Edition.

強化
關鍵基礎設施的網路安全

■ 華梵大學資管系特聘教授　朱惠中
健行科技大學資管系助理教授　陳惠娟

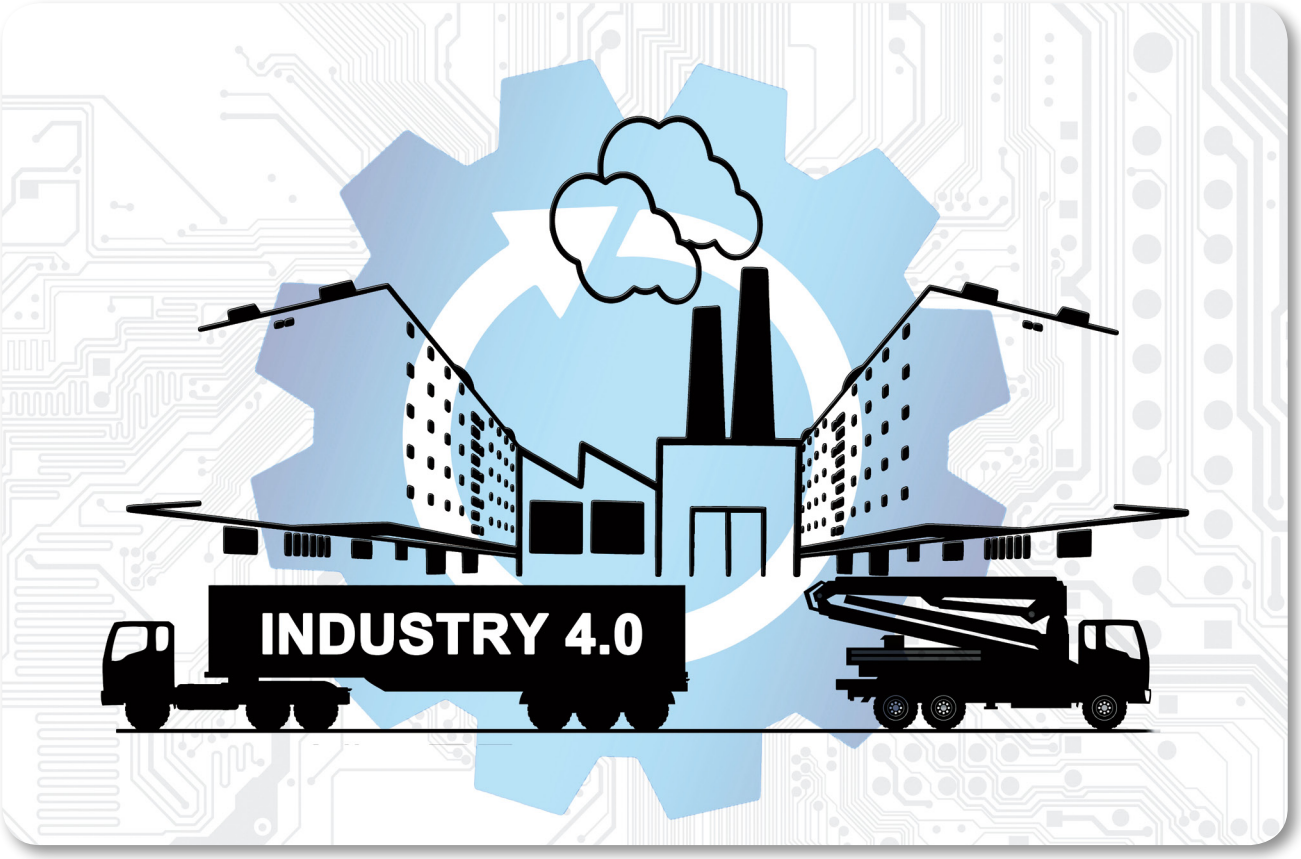
趨勢科技於 2015 年提出「美洲關鍵基礎建設網路安全」(Cybersecurity and Critical Infrastructure in the Americas) 報告，於全球 20 個國家的政府與民間企業進行調查，提出「53% 的受訪者認為去年專門針對 CI 的網路攻擊比以往更多」、「44% 的受訪者認為他們曾遭到惡意的刪除與破壞式攻擊」。[1]

[1] http://www.trendmicro.com/us/security-intelligence/research-and-analysis/critical-infrastructures-security/index.html; http:/www.trendmicro.com/us/security-intelligence/research-and-analysis/critical-infrastructures-security/index.html

背景

在傳統上，營運技術（Operation Technology, OT）與資訊技術（Information Technology, IT）分屬兩個不同的專業領域，彼此間鮮少交集，但隨著網際網路與 IT 的精進與普及，OT 與 IT 環境之間的專屬領域（Segmentation）已逐漸消失，原本與外界網路實體隔離的工業控制系統（ICS）逐漸必須與企業網路整合，利用 IT 在數據存儲、處理和通信方面的能力，來降低成本與風險，及提升效能與靈活度。

惟水可載舟，亦可覆舟，當不安全且含有漏洞的企業網路一旦與工控系統之專屬網路相連後，將使得工控系統暴露在網路攻擊的危險當中，越來越多原本以 IT 環境為目標的複雜網路威脅或攻擊行為，開始滲透到包括工控系統在內的 OT 環境。當此趨勢來臨後，使得仰賴工業控制系統的國家關鍵基礎設施，以及各產業的自動化生產、製造設備，受到網路攻擊的可能性大增，特別是進入工業 4.0 時代，原本可透過物聯網、大數據與雲端智慧，使 IT 與 OT 兩者終能展開對話，由 OT 領域的感測器獲取資料，上傳 IT 領域的雲端中心執行大數據分析，繁衍各種創新應用的目標將無法達成。



工業 4.0 的時代來臨，原可透過物聯網、大數據與雲端智慧繁衍各種創新應用，卻恐因為資安漏洞造成危機。

如何將 IT 與 OT 整合

整合 IT ／ OT 所需解決的問題，大致上可分成組織面及技術面二類：

一、組織面的問題

（一）獨立的企業過程（Business Silos）

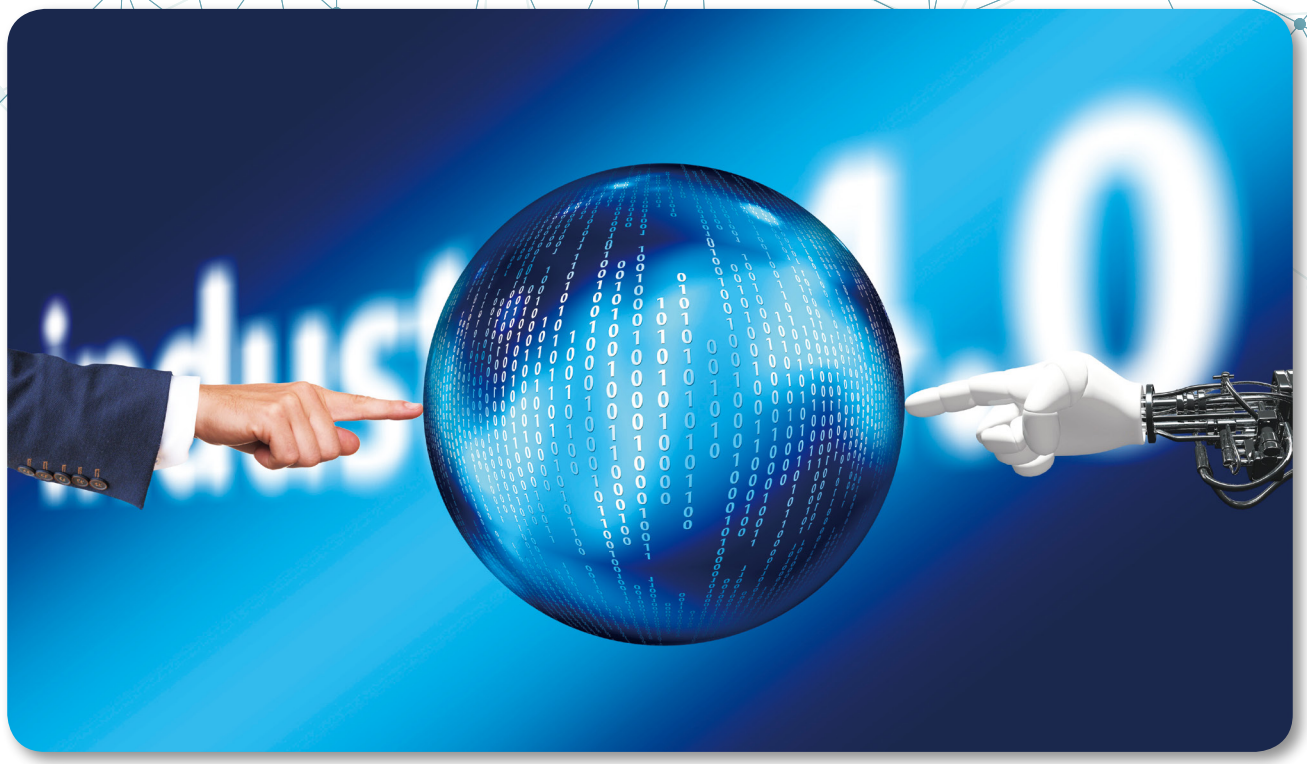
組織方面的問題源起於 IT ／ OT 的系統、人力之間皆有各自的體系，IT 系統由 CIO（Chief Information Officer）指揮，負責公司資產、工作流程管理等等，含括電子商務（e-Commerce）、企業資源規劃系統（ERP）、供應鏈管理系統（SCM）、顧客關係管理系統（CRM）、產品生命週期管理系統（PLM）等工作；而 OT 系統則由 COO（Chief Operational Officer）主導，負責 CI 的實體操作與監控，一般而言，泛指與工廠營運相關的技術，主要涵蓋三個類別：一是自動化；二是自動化整合搭配操作流程整合；三是工廠自動化與資訊技術的整合，諸如製造現場控制（Shop Floor Control, SFC）、製造執行系統（Manufacturing Execution System, MES）、監視與整合控制（Supervisory control and data acquisition, SCADA）等工廠資訊系統，此類系統需與上列 IT 系統進行整合，若雙方各自為政，將難以結合；另在串聯資訊技術與工業現場實體世界的過程中，感測器（Sensors）扮演不可或缺的要角。為了完善整合 IT 與 OT，在策略上 CIO 與 COO 須達成一致。[2]

（二）文化上的衝突（Culture Clash）

IT 部門往往是成本中心，需配合與支持企業客戶，故其政策和規則因須配合客戶需求，必須要做客屬化，亦即可能會建立自己的標準作業程序，以符合客戶需求。依此，他們只需依照與客戶簽訂的服務協議進行，如發生非計畫停電時，按業務維

IT 系統含括電子商務、企業資源規劃系統、顧客關係管理系統等工作；OT 系統負責 CI 的實體操作與監控，涵蓋工廠自動化與操作整合系統等。

[2] 魏于寧，「整合 IT、工控與通訊 加速落實工業 4.0 轉型」，DigiTimes 物聯網，2016-03-28



OT 與 IT 系統需進行妥善整合，避免雙方各自為政，策略上也將仰賴 CIO 與 COO 協調與共識。

運中斷程度處理即可。至於 OT 部門，在大多數情況下是核心業務，人員配置需反映 24x7（全年無休）的關鍵性質基礎設施，系統往往預計會不間斷持續運行數十年，故計畫外的中斷需按預先設定相關的程序啟動，以維持正常運作。

總而言之，OT 人員存有零故障的期望，而 IT 人員則強調靈活性和速度，一個成功的整合必須考慮到雙方的要求。

（三）風險容忍度（Risk Tolerances）

IT 系統下線或當機，往往僅會影響公司的正常運作，而 OT 系統（如電力）下線或當機，則很有可能影響所有用戶的安全；因此，許多 IT 系統視為常態保養的行為，如防火牆更新、系統維護等等，在 OT 系統上則認為是會有相當大的風險，故在整合雙方時，勢必需要列入考慮。[3]

二、技術面的問題

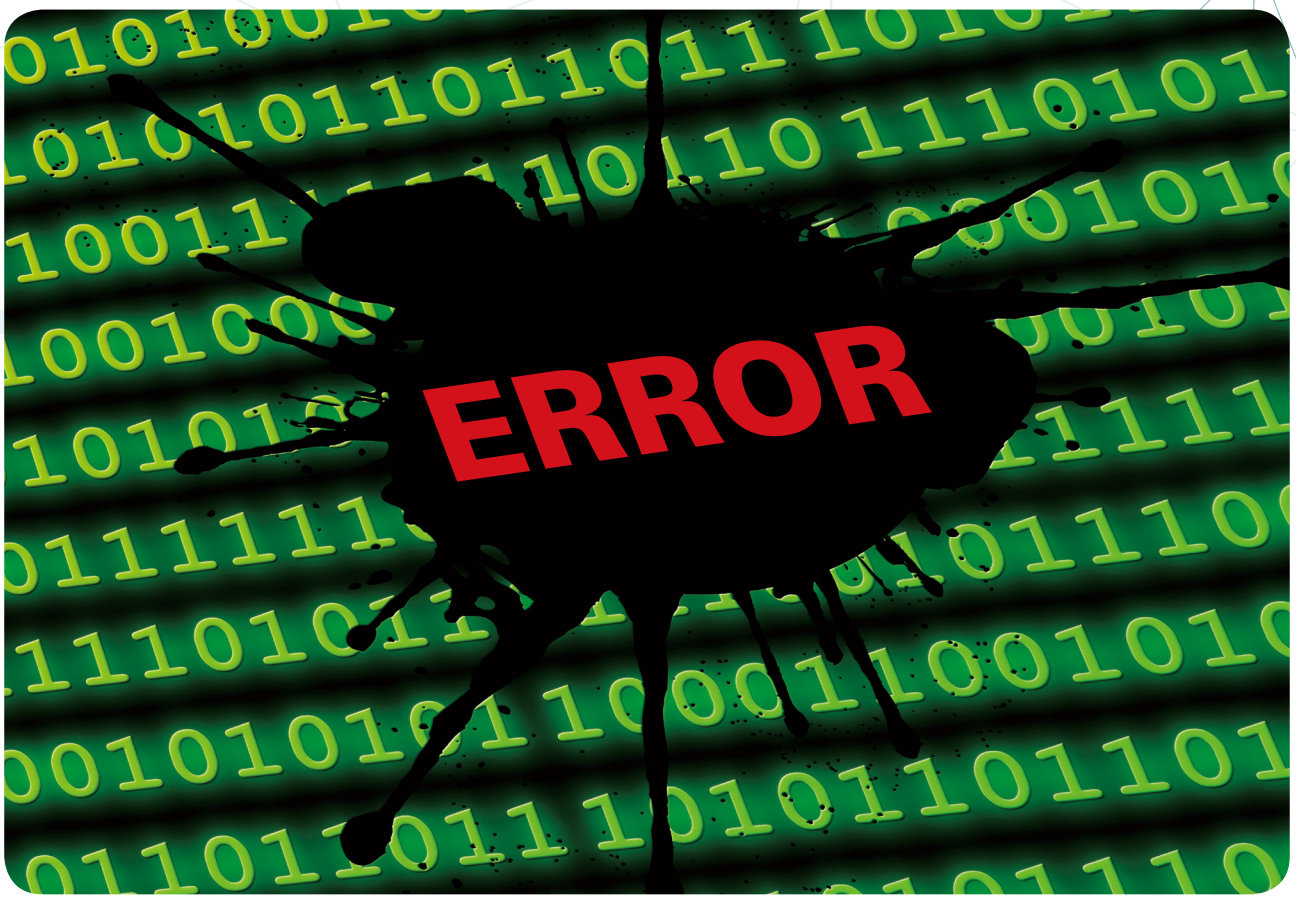
（一）環境性（Environmental）

IT 設備的日新月異，代表其生命週期通常相對較短，一台主機可能使用 5 年就被淘汰；但 OT 設備正好相反，相較於 IT 設備，其可靠性和完整性是 OT 的主要考慮因素。

（二）相容性（Compatibility）

隨著 IT 技術的成熟，鑒於各式軟硬體相容性的問題，導致驗錯功能需求的產生。

[3] Atos, White Paper: The convergence of IT and Operational Technology, 2012



IT 設備的錯誤，往往會影響 OT 設備的正常運作。

OT 系統因為輸入、輸出均為特定格式及設備本身為專屬產品，因此，相容性之要求不高，故 IT 設備的錯誤（Bug），往往會影響 OT 設備的正常運作。

（三）跨領域人才短缺（Skills Shortage）

IT 與 OT 雙方的技術背景具有相當的差距，故具有橫跨領域的技術與經驗，且有能力接手整合後的系統人才極端缺乏。

（四）資安需求（Security）

OT 系統以前均侷限於工廠內部或是鄰近地區，故無防範外部威脅的需求，一旦與 IT 系統整合，便必須防範因使用 IT 由外界造成相對應的威脅。

結論

一、為何要將 IT 與 OT 合併

IT 之技術在其重點領域，即數據存儲、處理和通信等方面已經取得巨大的進步，相較之下，OT 大部分的進展都是在專屬的系統與程式中，造成非專業人士難以理解這些專業工作環境，故難以整合多種相關的技術和提供商。隨著公司的全球化與競爭的日益激烈，IT ／ OT 的整合將具有以下的優點：

（一）降低成本（Cost Reduction）

利用類似技術、標準來治理 IT 和 OT 的原則，公司不再需要維持兩套不同的規範。

（二）降低風險（Risk Reduction）

IT ／ OT 整合意味著資安問題可以利用整合 IT ／ OT 的方法處理，這對防禦外來入侵提供進一步的保護。

（三）提升效能（Performance Enhancing）

IT ／ OT 整合能節省時間和成本，縮短新產品開發完成到上市的時間，減少經濟廢品。

（四）提升靈活度（Flexibility Gaining）

IT ／ OT 整合將會提供更好的透明度，優化成本和調整成本結構；公司也會變得更加靈活，加速製造所在地的轉移。[4]

二、整合 IT 與 OT 需克服的困難

（一）發展 IT ／ OT 聯合組織和治理結構。

（二）共同管理 IT 和執行 OT 跨技術項目。

（三）協調、匯總重複的過程，精簡程序。

（四）發展跨 IT ／ OT 領域的技能，培養了解雙方需求和要求的人才。

（五）IT 與 OT 之間責任的分擔（特別在安全方面）。

（六）聯合管理現在不同的基礎設施，以方便未來的整合。

[4] Atos, White Paper: The convergence of IT and Operational Technology, 2012
Derek R. Harp and Bengt Gregory-Brown, IT/OT Convergence --IBridging the Divide, NextdefenseT

關鍵基礎設施防護失靈是國安危機

■ 國防大學戰爭學院上校主任教官　陳永全

CI 防護機制應提升至國家安全層次

全球之氣候變遷日益惡化，國際局勢變化快速，外在軍事威脅、恐怖攻擊，針對我國環境、政治局勢、及參考過往天然、人為、資通訊與網路攻擊災害經驗，我們所面對之威脅已呈現多樣化、多重化、急遽性及高影響性之發展趨勢。為能適應如此艱鉅之挑戰，我國應具備「全災害對策」作為國家安全政策規劃之基礎，亦即對複合式災害威脅要具備全面性的防護觀念，並將關鍵基礎設施（CI）安全防護機制與執行方式，提升至國家安全層次考量。

CI 防護失靈案例紀實—以能源設施為例

能源關鍵基礎設施安全包括三大範疇，第一是油、電、天然氣廠的實體安全（地震、颱風、水災、火災、土石流、異常中斷、廠房事故、系統設備遭損、恐怖攻擊、武器攻擊或戰爭行動破壞等）；第二是維繫油、電、天然氣廠正常運作的資訊安全（如涉及資訊系統、網路系統或控制系統上的不正常事件或遭受網路攻擊、駭客攻擊、資訊戰等足以影響系統正常運作等因素）；第三是人員安全（如不當操

作、缺乏警覺心、違反資訊安全規定、意圖惡意破壞之內部或外部人員、駭客、網路恐怖分子、第三方使用者或離職員工等），一旦能源供應單位的實體安全、人員安全與資訊安全得以確保，能源設施的安全才得以受到保障。

針對能源設施可能面對之威脅，茲提出以下實例供參考：

一、天然災害威脅

1999 年 7 月 29 日，於臺南左鎮，因連日豪雨致地基土壤流失，台電公司編號第 326 的輸電鐵塔傾斜。由於電力是由南向北傳送，中北部的各發電廠因保護機制而跳脫，進而引發全臺計五分之四以上電廠因輸電系統低壓震盪而跳機，最終導致臺南以北地區從當晚 23 點 38 分開始大規模停電。無預警停電造成新竹科學園區半導體廠生產中斷損失二十餘億元，臺北股市當天開盤重挫及下跌；交通方面，臺鐵有 5 列行駛中電聯車因斷電被迫停止通行。

二、油廠威脅

2015 年 4 月 25 日發生於臺東，嫌犯以租農地種老葉樹，圍黑網掩人耳目，挖掘埋藏於地下的油管，於油管架設連接閥與壓力表藉以控制油壓、油量流速盜油；嫌犯後來雖難逃法律制裁，然花東地區輸油管管線長達 192 公里，若有恐怖分子刻意引爆油管，後果恐不堪設想。

三、天然氣廠威脅

2015 年 12 月 24 日非洲奈及利亞東南部一家天然氣廠發生爆炸，造成逾百人死亡，事發原因是一輛氣罐車在卸下瓦斯之後，未依照等待冷卻的標準作業程序，就逕自駛離，因而引發爆炸，是以，天然氣廠的標準卸收作業流程與程序，是確保安全的重大考量因素之一，絕不可輕易玩忽。

2015 年臺東發生軍用油盜取事件。
（圖片來源：截自中天新聞）

奈及利亞東南部一家天然氣廠發生爆炸，造成逾百人死亡。（Photo credit: https://www.thecable.ng/nnewi-gas-explosion-police-recover-two-more-bodies）

去年的 815 全臺大停電導致許多民眾受困電梯。（圖片來源：高雄市消防局，https://www.nownews.com/news/20170815/2599441?null）

今年 1 月 29 日桃園煉油廠熱爐管起火燃燒，強烈爆炸聲造成附近居民恐慌。（圖片來源：內政部消防署，http://www.nfa.gov.tw/cht/index.php?code=list&flag=detail&ids=22&article_id=3443）

四、電廠威脅

2016 年 1 月 4 日「伊斯蘭國」（IS）攻擊利比亞最大的港口席德拉港、石油重鎮拉奴夫角，以及班加西一座石油發電廠，烈火燃燒整整 4 天。報導指出，由於受損的發電廠主要為利比亞東部供電，因 4 天失能，大大重創東利比亞當地的經濟、民生。

2017 年 8 月 15 日全臺大停電，只因中油對臺電天然氣供電意外停止運轉 2 分鐘，導致全臺 592 萬用戶停電，剛好又正值通勤尖峰時間，臺鐵有 40 個車站停電，光是新北市與高雄市就有超過一千多處交通大打結，上千人受困電梯，科學園區受到跳電影響，產業損失數億元。

五、油廠威脅

2018 年 1 月 29 日，中油公司桃園煉油廠於歲修後重新啟爐，加熱爐管破裂起火燃燒。由於該工廠日產柴油占中油總產量 20%，火勢雖於 1 小時內即撲滅，然已造成附近居民恐慌及環境空氣品質影響。

國軍「守土有責」不遺餘力

國軍在「守土有責」的防衛任務規劃下，如何針對作戰區所轄地境內之關鍵基礎設施，建立彼此平時聯繫機制，戰（災）時相互支援的有效防護能量，是現今國軍除確保自身軍事營區安全外，必須依據國防部聯合參謀計畫與作戰次長室所業管之「國軍重要目標防護」清單，詳加檢視自身防護能量，並規劃足以有效支援關鍵基礎設施防護的人力與物力，方可因應未來的威脅與挑戰。

國軍弟兄對臺灣發生的重大災難救援向來不遺餘力，諸如：2014 年高雄氣爆事件，陸軍司令部派出上千名國軍以及化學兵透過偵測器材，冒險沿著路面偵測可燃氣體是否仍殘餘；2015 年蘇迪勒颱風重創臺灣，多處嚴重積水及發生土石流，當時

2014 年高雄氣爆後，由國軍及化學兵負責偵測路面是否安全。（圖片來源：中華民國總統府）

2016 年 0206 地震維冠大樓倒塌，國軍成立應變中心分派人力至現場協助救援。（圖片來源：葉昇典，https://www.flickr.com/photos/shengdianye/sets/72157664280720832）

至少出動上萬名國軍待命救援。2016 年小年夜發生的臺南維冠大樓倒塌事件，國軍在地震後二十分鐘內立即成立應變中心，第 1 批支援人力於 1 小時後就抵達現場，「便當、麵包」就成為了救災人員的年夜飯；國軍永遠以民眾安危為優先考量。茲彙整重大災變發生時，如何向親友報平安之各電信公司的語音信箱撥打方式供各位參考（如表一）。

表一　運用電話或傳媒之報平安方式

災變發生時，如何報平安	
中華電信語音信箱	手機撥打 777，可儲存留言 20 通及傳真 10 通，每通留言最長 2 分鐘，每通傳真最多 20 頁，新舊留言及新舊傳真皆保留 7 天。
台灣大哥大語音信箱	手機直撥 123
遠傳電信語音信箱	手機直撥 222
亞太電信語音信箱	手機撥打 777
威寶電信語音信箱	手機撥打 777
1991 報平安	手機撥打 1991
Facebook 平安通報站	每當地震、颶風、掃射攻擊或房屋倒塌等危及生命安全的事件發生時，全球性的災難回報機構就會向 Facebook 發出警報。如果在受影響地區有大量用戶發布事件相關貼文，系統就會啟用平安通報站，位於該地區的用戶可能會收到 Facebook 通知，要求標示自己的安全狀態用戶也可前往安全通報站點擊詢問是否平安無事，關心 Facebook 朋友的安危。
Google 尋人系統	Google 尋人系統，日本強震災後尋人工具。

國軍之 CI 防護計畫演練

面對關鍵基礎設施防護，首要的工作是風險辨識，風險辨識的步驟是找出需要管理的風險。必須使用有系統的步驟發展風險情境方案或計畫，如表二所示來進行廣泛的相關資訊蒐集，因為在這個階段沒有被發現的風險將被排除在分析的步驟之外。蒐集應包括所有的風險，不論該風險是否已在單位機關的控制之下。擬定風險情境時，應採用系統化程序，並由事件背景說明開始，以求其完整性，使用結構化的方式進行辨識程序，以確保風險辨識採用的方法有效、可行，且亦有助於完成辨識程序，避免遺漏任何重大問題。

完成了風險辨識工作，接續依據風險的評量可進行情境假定演練，任何國防軍事單位在遂行此類演習活動過程中，在考量相依性與依存度的情況下，關鍵基礎設施防護工作將與軍事活動與安全維護產生緊密結合的鏈結，基此，可於演習中接續前述的風險辨識規劃演習情境的假定與演練，並依據以下相關因素實施演習規劃：

- 一、威脅類別
- 二、情境假設
- 三、可能性及機率
- 四、評量權重
- 五、脆弱度分析（脆弱度、強度）
- 六、衝擊評估（承受度、耐受強度、恢復力）

表二　發展風險情境方案或計畫參考

發展風險情境方案或計畫			
風險項目／情境	風險類別／編碼	風險發生原因	可能後果
天然災害發生			
人為攻擊或恐攻			
資訊安全攻擊			
發生軍事戰爭			

表三　全民防衛動員（民安演習）綜合實作演練課目

風災、水災、地震							
1	2	3	4	5	6	7	8
三會報聯合應變機制編組與運作	跨區支援救災能量整合與運用	各類民防團隊運用治安及交通維護	鄉民疏散撤離具體作為	鄉民收容安置具體作為	非營利事業機構及志工團隊運用	工業管線地下石化埋管氣爆災害搶救	全民國防教育活動具體作為
9	10	11	12	13	14	15	16
緊急通信應援及搶救（修）	重大災害搶救及災情查通報	大量傷病患醫療救護	傳染病防治	毒性化學物質災害搶救	核子或輻射災害	國軍支援兵力運用	教召後備軍人運用
17	18	19	20	21	22	23	24
情資分析研判	水庫潰損災害搶救	土石流災害警戒疏散	居家使用維生器材之身障者斷電處理	水災	儲油槽、石化廠、給水廠、變電所災害搶救	水利、下水道設施災害搶救	橋梁、道路、隧道災害搶救

另檢附全民防衛動員（民安演習）綜合實作演練課目供參（如表三）。「國土安全」，尤其是關鍵基礎設施防護，更是全體國人與國軍不可輕忽的重要議題與重責大任。

結語

關鍵基礎設施防護是國家因應重大危機發生的應變前瞻規劃與具體作為，上至國家安全會議，下至各關鍵基礎設施擁有者，各層級均應有相對應之防護計畫與目標，當遭受重大災害或發生戰爭準備與軍事威脅等情境時，如何透過平日嚴格精實的訓練，整合資源與支援，讓關鍵基礎設施防護能量與國防軍事安全，建立機制與防護能量的相互鏈結，這是國家關鍵基礎設施防護的重要課題，刻不容緩。