資訊科技之快速進步，對傳統社會生活已然造成本質上的改變，亦牽動國家競爭力與國家安全的轉型。

我國關鍵基礎建設安全防護

◎ 方鴻春

一、緒論

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爲指揮通訊工具，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建設安全之防護；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，已成爲各國亟需面對的課題。

二、安全威脅隱憂

2003 年春天美國情報人員在巴基斯坦內陸山區某處，發現一台筆記型電腦，其中包含了許多對於美國關鍵設施的詳細偵察情報，看來蓋達基地組織（A1 Qaeda）顯然花了不少時間在監視美國本土的重要金融中心及企業總部，如紐約證交所、世界銀行與國際貨幣基金組織。其目的很明顯地，是攻擊任何具價值的實體關鍵基礎建設，以削弱美國的經濟實力，令貨幣金融體系失序，並打擊美國甚至國際市場的信心。

此攻擊模式正如 2008 年電影「終極警探 4.0」所描述的情節般令人恐懼；而自從 90 年代以來就不斷有人預言，這種綜合實體與電腦網路的攻擊事件可能會發生。例如：2007 年 5 月就發生「愛沙尼亞」的全國電腦網路遭受來自全球的激烈網路攻擊，幾乎癱瘓「愛沙尼亞」政府及民間活動，史稱這是第一場「網路戰爭」。（詳如本單元下一篇文章）

三、我國關鍵基礎建設防護範圍

所謂國家關鍵基礎建設(Critical Infrastructures, CI)是指「在一個國家中爲維持國家安全、民生、經濟而提供的基本產品或服務，包含維持國家最起碼的經濟、民生、政府運作與國家安全息息相關的實體和以資訊電子爲基礎的運作系統」。常見的關鍵基礎設施包括公民營的電信、能源、銀行、財金、交通、供水及防救災等系統。

我國行政院提出第二期「建立我國通資訊基礎建設安全機制計畫」(2005~2008 年)，報告中指出：安全的通資訊防護機制必須能夠保護國家的利益，並能維持政府與民間生活的正常運作，在政府體系方面，舉凡金融體系、商務運作、政府服務、水、電、油、瓦斯等供給、緊急救援體系、交通及電信等關鍵基礎設施都要能正常運作。在民間方面，則要能確保民眾的日常生活與權益不受影響。因此明確規範至少必須能維持下面六項體系的正常運作：

（一）政府的正常運作。
（二）軍事力量的維持。
（三）救援體系的正常運作。
（四）人民日常生活必需品(電信、水、電、油、瓦斯、食物)的正常供給。
（五）金融體系的正常運作。
（六）商業的繼續進行。

在參酌行政院資通安全會報所提二十個核心資訊系統，重新定義關鍵基礎建設資通安全保護範圍，可概分兩大面向－「工業自動控制系統」與「商業資料處理／傳輸系統」；再依其屬性又細分爲八大類關鍵基礎建設資通安全防護範圍，如前圖 1，所示：

圖 1 我國關鍵基礎建設資通安全防護範圍

（資料來源：國家關鍵基礎建設資通安全防護研究期末報告，研考會）

四、各項安全威脅剖析

在各項安全威脅上，考量國家關鍵基礎建設所有資產、系統與網路所構成的安全防護面向，將它區分爲三種標的物，並分析其可能面臨的威脅與風險來源，詳見圖 2，所示。

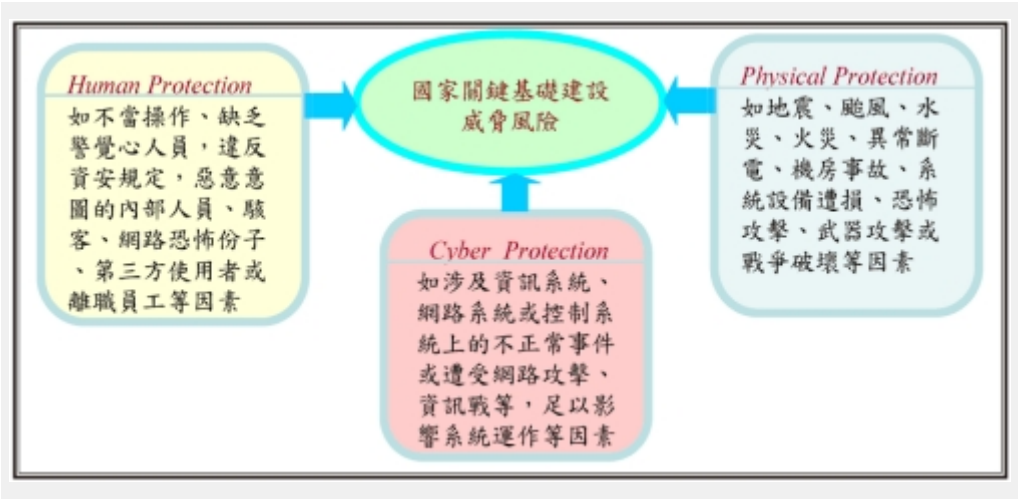

圖 2 國家關鍵基礎建設保護核心威脅來源

（資料來源：國家重要基礎建設資通安全防護研究期末報告，研考會）

五、相依性的關聯關係

除了前述威脅與風險來源，其實關鍵基礎建設項目間彼此依存度的高低，對關鍵基礎建設之間應受保護的優先性，也是重要的參考指標之一。誠如電力與通訊爲其他關鍵基礎建設的依賴度最高，而通訊又對電力依存度甚高，要如何呈現關鍵基礎建設項目之間的依存度，也是國家在擬定「關鍵基礎建設」保護策略上的重要依據。

在研究關鍵基礎建設之間依存度分析時，美國學者 Rinaldi, Peerenboom and Kelly 以「基礎建設相依關聯圖」，說明不同基礎建設間相依需求之關係，詳見圖 3，所示。

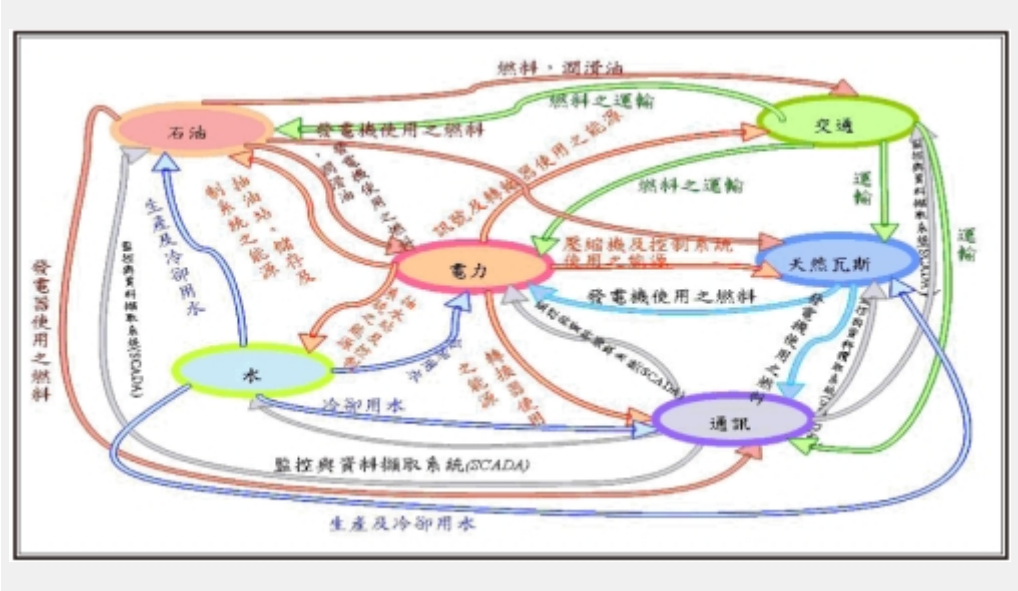

圖 3 基礎建設相依關聯圖

（資料來源：IEEE Control Systems Magazine 2001 –

Identifying, Understanding and Analyzing Critical Infrastructure Interdependecies）

六、防護策略

近來網路犯罪在我國已成爲社會犯罪的最常見形式之一，包括透過垃圾郵件、網路釣魚、社交工程、網路詐騙及網路戰等行爲，導致關鍵基礎建設資訊系統中斷、國防資訊洩密、網頁置換及遭受非法入侵的事例屢見不鮮，也常見各種利用網際網路造謠煽動的網路謠言與聚集活動，造成社會或民眾普遍不安。從現在盛行的網路攻擊手法顯現，我國對於網路犯罪和網路恐怖主義的威脅絕對不可掉以輕心。

美國在 2002 年成立國土安全部，其主要職責爲：將以往散置於各單位缺乏橫向聯繫之各項保護計畫整合於該單位，規劃統整全國基礎建設防護計畫，並於 2006 年 6 月完成國家基礎建設防護計畫(National Infrastructure Protection Plan, NIPP)。NIPP 的基石爲風險管理架構(Risk Management Framework)，詳見圖 4，所示，目的爲管理與降低來自於網際、實體及人員三方面的攻擊威脅風險。包含下列六個防護工作步驟：

研究各國在關鍵基礎建設的保護政策與作法，主要是參考《International CIIP Handbook 2006》的資料進行剖析與檢討，以作爲我國發展關鍵基礎建設相關保護政策與作法的參考。綜合先進國家實務作法，建議我國關鍵基礎建設防護應從以下防護策略著手：

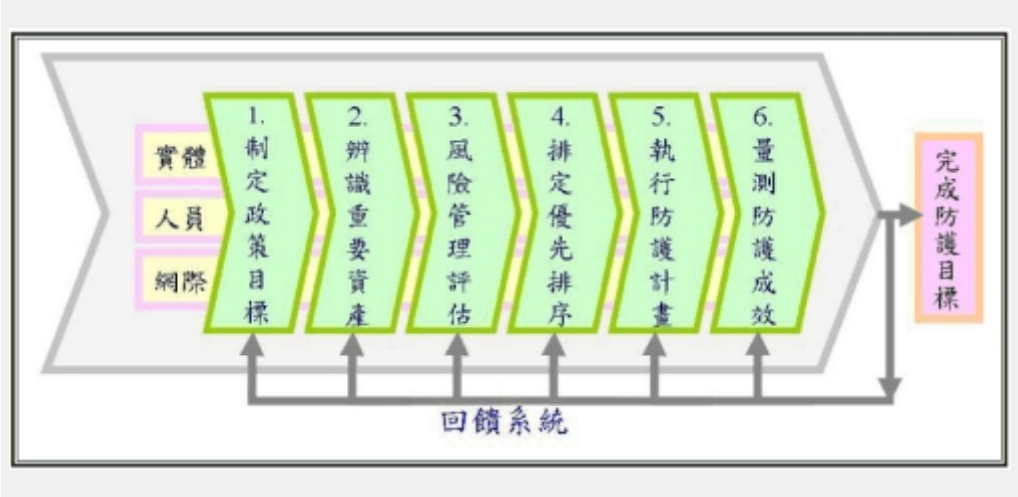

圖 4，NIPP 風險管理架構 (資料來源：National Infrastructure Protection Plan ，2006）

（一）提出國家／國土網際網路安全計畫：以政府爲主導，訂定一個策略性的防範規劃。

（二）培育網路安全管理與技術人才：不單是只有網路技術人才，亦應針對安全管理方面技能進行要求。

（三）提供整合防護策略：由不同的防護軟體，如防毒、防火牆等整合其防護策略。

（四）進行滲透測試：主要針對國家重要資訊基礎建設之商業資料處理／傳輸系統與工業自動控制系統進行測試，以了解弱點並補強。

（五）提供制度化的防範機制：法律與法規的配合，政府相關的政策等。

（六）安全意識的提升：藉由教育訓練與安全意識的宣導活動。

七、結論

全球最大的駭客大會「Defcon」於 2007 年 8 月初在美國賭城拉斯維加斯召開時，與會安全專家就曾警告稱：未來恐怖分子以及駭客會利用新發現的軟體安全漏洞，對包括公民營的電信、能源、銀行、財金、交通、供水、救災，以及製造工廠的「監控與資料擷取系統(Supervisory Control and Data Acquisition, SCADA)」之核心電腦進行大規模攻擊。SCADA 系統儼然已成爲駭客下一個攻擊的目標，所以未來各國所面臨的將會是相當複雜且難以獨自處理的重大資通安全防護問題。

環顧我國資訊科技發展，已歷經多年的基礎；然而，時代在變，潮流在變，近年來資訊科技之進步，十年銳於百載，對傳統社會生活已然造成本質上的改變，亦牽動著國家競爭力與國家安全的轉型。身處資訊快速變遷的環境中，我國自當不斷地調整自己，做好因應挑戰的準備，並爲國家關鍵基礎建設的防護工作預作規劃。

八、參考文獻

（一）國家關鍵基礎建設資通安全防護研究期末報告，研考會，2008/03/31。

（二）「建立我國通資訊基礎建設安全機制計畫」第二期(94~97 年)，行政院資通安全會報，2007/02/15

（三）「資安人雜誌」NO.42,2007.JUN，P28~32

（四）下一次世界大戰(The Next World War)，詹姆士・亞當斯 著，張志誠 譯，新新聞出版，1999/05/25

（五）「強化資安防護作爲，有效防杜中共網軍惡意攻擊」，王崑義 著，青年日報社論，2007/08/15

（六）International CIIP Handbook 2006 Vol.1 & Vol.2

（作者是國家資通安全會報技術服務中心顧問）