關鍵基礎設施面對網路攻擊的新風險：以伊朗為例

作者簡介

沈明室備役上校，陸軍軍官學校正54期、陸軍步兵學校正規班286期、政治大學東亞所碩士84年班、陸軍指揮參謀學院87年班、國防大學政治學博士；曾任排長、連長、人事官、營長、外事連絡官、科長、助理教授，現任國防大學戰略研究所副教授。

提要

一、由於核電廠是重要基礎設施，受到網路攻擊後，若影響民生用電，茲事體大。曾有人懷疑是美國或以色列發動的網路攻擊行動。因為伊朗本來是希望透過高速離心機控制設備來提煉濃縮鈾原料，以製作核武之用。而這次攻擊就是特別針對伊朗核電廠的離心機，目的在先期抑制伊朗發展核武的企圖。

二、伊朗電視媒體引用《華盛頓郵報》報導，指控美國和以色列政府共同開發火焰軟體攻擊伊朗的核能計畫，但是在沒有明確證據情況下，真相難以釐清。

三、震網又稱作超級工廠，是一種Windows平台上的電腦蠕蟲。震網以及它的變種火焰惡意間諜軟體的遊戲規則已經與以往不同，震網會造成重大損失多半是因為駭客主要是針對國家等級的網路，如水庫、油井、電廠等重要

基礎設施發動攻擊，但變形之後的病毒反而會透過消費者幾乎每天使用的隨身碟、外接硬碟等行動儲存裝置散播，一旦被感染，以現在的使用習慣，很可能連手機、平板電腦等都難逃一劫。

關鍵詞：網路攻擊、震網。

前　言

隨著資訊科技發展的日益提升，諸如智慧手機等相關先進產品，使人與人之間的互動更為方便，而且一些關鍵基礎設施透過資訊的整合與運作，效率也大為提升，減少許多人工成本。除了大幅提升效益之外，資訊設備及軟體的大量運用，也增加不少的風險，如資訊攻擊、網路安全與衝突事件層出不窮，其攻擊方式與所使用的病毒軟體，亦隨著網路防衛科技與作為的發展而相應創新。尤其對關鍵基礎設施的威脅日益升高。

歐盟執委會曾經出版《歐洲關鍵基礎設施保護計畫綠皮書》(The Green Paper on a European Program for Critical Infrastructure Protection, Green Paper on EPCIP)，書中將「關鍵資訊基礎設施保護」(Critical Information Infrastructure Protection, CIIP)定義為：「基礎設施擁有者、操作者、生產者、使用者及調整授權單位，針對如何保持關鍵資訊基礎設施在受到失靈、攻擊與意外情況下能持續運作，使之維持最小限量服務，並將危害及復原降到最小的計畫與作為。因此，關鍵資訊基礎設施保護應該被視為跨領域的現象，而非限定在特定的範圍。關鍵資訊基礎設施保護更應該密切的與其他不同類別的關鍵基礎設施保護相互協調」。[1]

在大多數國家的定義中，關鍵是指基礎設施對於經濟、社會福利、公眾安全和政府的關鍵功能提供支持。因此，用「關鍵」是指基礎設施如果被破壞或是失去功能，將導致災難性和深遠的破壞。從這個定義可以看出歐盟對關鍵基礎設施重要性的強調，並著重如何在遭受攻擊後，維持關鍵基礎設施的運作，避免損害的擴大。

在我國關鍵基礎設施分類中，供電也是重要的一環，受到資訊系統的連動。不論是電腦駭客或具特定意圖的攻擊者會透過不同的方式，進入不同的電腦系統中，進行癱瘓、竊取、阻斷的攻擊行動。其所造成的危害，小則造成資料的流失，嚴重則造成供電等重要關鍵基礎設施的停頓與中斷，影響社會正常運作。

舉例而言，2010年，伊朗核電廠受到震網(Stuxnet)蠕蟲攻擊，[2]引起世人的重視。雖然伊朗存有發展核武的念頭，給予他國攻擊的藉口，但是核電廠是重要基

1　Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism, Brussels, COM(2004)702 final, 20 October 2004, p.19.

2　於下頁。

礎設施，受到網路攻擊後，若影響民生用電，茲事體大。當時曾有人懷疑是美國或以色列發動的網路攻擊行動。因為伊朗本來是希望透過高速離心機控制設備來提煉濃縮鈾原料，以製作核武之用。而這次攻擊就是特別針對伊朗核電廠的離心機，目的在先期抑制伊朗發展核武的企圖。

直到2012年，《紐約時報》報導，美國官員承認這個病毒是由美國國家安全局(National Security Agency, NSA)在以色列的協助下研發，並以奧林匹克運動會(Olympic Games)為計畫代號，目的在阻止伊朗發展核武。以電腦病毒攻擊非軍事設施，不僅違反武裝衝突法的必要性原則，更嚴重影響社會民生的需求。本文將以伊朗核電廠遭受網路攻擊為例，探討以供電為主的關鍵基礎設施受到網路攻擊的模式，並以歐盟為例，列舉各國因應法令及政策，以及對臺灣供電關鍵基礎設施維護的啟示及作為。

伊朗核電廠遭受網路攻擊的模式

分析網路攻擊核電廠所產生的風險之前，必須先瞭解網路攻擊伊朗核電廠的模式與細節。德國資訊安全顧問藍格納(Ralph Langner)在一次演講中，透漏了相關的細節。[3]他說，美國所使用的震網攻擊其實是源於Windows釋放程式。[4]首先讓這個程式進入到設備工程師使用的電腦(Windows系統)，再透過USB隨身儲存裝備植入系統。美國曾有匿名官員承認此事，證明強化震網蠕蟲攻擊的運用，可以將國土安全的攻防首次提升到網路攻擊層級。[5]

除了遭受震網的攻擊外，資安攻擊已經提升至國家支助型戰爭的層次。如同樣因為攻擊伊朗石油部而被發現的超級間諜病毒火焰(Flame)，媒體報導也認為是美國與以色列政府聯手開發而成的軟體，目的在延緩伊朗的核武計畫。其中《華盛頓郵報》(Washington Post)於2012年6月19日報導美國官員的說法，認為美國和以色列政府共同發展的火焰病毒程式，目的在蒐集伊朗政府的資料，以做為更進一步網路攻擊的參考依據。伊朗情報部部長莫斯李希(Heydar Moslehi)在同年6月21日公開表示，伊朗受到來自其他國家政府的攻擊，此攻擊是鎖定伊朗的核能設備。「路透社」(Reuters)表示，莫斯李希所說大規模攻擊並未明確指出就是火焰或其他新的攻

2 "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers" BBC News, http://www.bbc.co.uk/news/world-middle-east- 11414483, 26 September 2010, 2015/5/8.

3 Ralph Langner及其團隊協助破解震網的編碼，找出這個數位武器的最終攻擊目標－以及其幕後源頭。經使用電腦數位鑑識方法深入檢視後，他解釋了其運作原理。Ralph Langner, "Cracking Stuxnet, a 21st-century cyber weapon," http://www.myoops.org/main.php?act=course&id=2257, 2014年5月6日。

4 Bright, Arthur "Clues Emerge About Genesis of Stuxnet Worm," Christian Science Monitor, http://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm,1 October 2010, 2014/5/6.

5 吳依恂，〈美國採取網路攻擊戰 阻止伊朗發展核武〉《資安人科技網》(2012年6月4日報導)，http://www. informationsecurity.com.tw/article/article_detail.aspx?aid=6830#ixzz2EqAjTD21，2014年12月9日。

擊。然而伊朗電視媒體引用《華盛頓郵報》報導，指控美國和以色列政府共同開發火焰軟體攻擊伊朗的核能計畫，但是在沒有明確證據的情況下，真相難以釐清。

若將火焰與震網相比較，兩者不論是分布位置或攻擊手法都高度雷同。不過，卡巴斯基實驗室已經發現火焰和震網具有相同原始碼，顯示兩者之間確實有其關聯性。這兩波威脅應該是來自於同一個攻擊單位的兩個開發團隊，差別在於火焰主要任務在進行間諜活動，是用來執行破壞性的活動。[6]

震網運作的模式是先透過USB感染主機，接著尋找主機所在網域內是否有攻擊目標：裝有西門子公司的SCADA(Supervisory Control and Data Acquisition)的Windows平台。假如主機上有符合設定的目標，震網會利用漏洞(其中有4個Zero-day弱點)感染Windows主機，接著透過PLC(Programmable Logic Controller)來達到控制工業設施(發電廠、煉油廠等)的目的。

PLCs是一種使用獨特語言的設備，可用來控制發電廠、化學工廠、煉油廠內的機器，通常PLCs不直接與網路連接，管理者透過像西門子的SCADA系統來控制PLCs，而西門子的SCADA系統必須安裝在Windows平台上，所以當震網想控制PLCs時，會先找上從遠端控制PLCs的電腦，這也是為什麼震網能夠得到入侵Windows平台的漏洞。

當震網被發現時，資安人員對於它用來入侵Windows的軟體程式之複雜感到震驚。而且，資安人員將震網放在實驗環境裡面試圖去破壞感染其軟體系統，以瞭解那些非Windows部分的作用。不過，實驗室的震網始終沒有發揮作用，資安人員換了許多環境嘗試，但震網都不感興趣。此時，資安人員才發現，震網是一種被設計用來進行針對性攻擊的惡意程式。在破解震網後，與所有伊朗境內重要的煉油設施所使用PLCs組合語言比對，才發現震網的目標就是要控制位於伊朗納坦茲(Natanz)進行鈾濃縮操作的PLCs。

震網分為兩個部分：主要安裝模組和PLC模組。震網想進入的是一個控制基礎設施的即時控制系統(Real Time Control System)，一般通稱為灰盒子，技術人員在Windows上面安裝控制灰盒子的軟體，用軟體提供的API控制灰盒子。所以震網必須先入侵控制灰盒子的Windows主機之後才能更進一步控制灰盒子。[7]

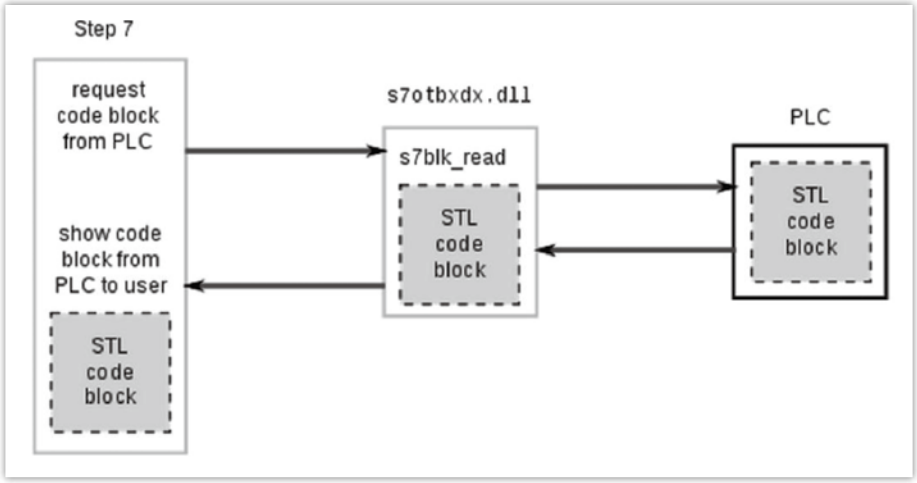
震網主要模組的任務是在散播自己，以及入侵裝有控制灰盒子軟體的Windows主機，透過多種漏洞進行入侵。其中有一個是知名Conficker蠕蟲用的MS08-067漏洞，而其中最令人驚訝的是，微軟公司未曾發布的4個漏洞。控制灰盒子的軟體由西門子的「Step7」這個軟體擔當，震網在感染主機後，會對主機進行偵查，如果主機不能控制住灰盒子，那震網就什麼事都做不成。如果主機是震網瞄準的目標，

6 〈超級間諜病毒Flame 可能是美國與以色列聯手開發〉《資安人科技網》(2012年6月26日報導)，http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6883#ixzz2Eq7n4kIj，2012年12月9日。

7 〈惡意程式-Stuxnet簡介〉，臺灣電腦網路危機處理暨協調中心，http://www.cert.org.tw/docfile/Stuxnet.pdf，2015年5月6日。

那PLC模組便會開始運作，並用PLC模組來控制灰盒子。[8]流程圖如圖一，西門子公司控制PLC的軟體為Step7，Step7透過s7otbxdx.dll來跟PLC進行溝通。

圖一　正常的Step7與PLC溝通過程



資料來源：Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32 Stuxnet Dossier," Symantec Security Response, Version 1.4, http://www.symantec. com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011, p.37.

當震網入侵主機成功之後，會將原本的s7otbxdx.dll更名為s7otbxsx.dll，自己則擔當起原本s7otbxdx.dll的工作。由震網偽裝的s7otbxdx.dll與原本的s7otbxdx.dll函數列表相同，這說明了震網偽裝的s7otbxdx.dll在感染主機之後，會擔當起原本s7otbxdx.dll的工作。對於多數的函數呼叫，假的s7otbxdx.dll都會「正常」處理，只有少數的動作會被震網更動的DLL攔截，以假亂真，使得資訊管理員很難發現震網在背後進行的操作行為[9](如圖二)。

正如藍格納所說的，震網攻擊是一般性的，沒什麼特殊性，可以針對核電廠的離心機及濃縮鈾進行攻擊，也可作用於汽車工廠。因此，是通用的，不需要藉由USB裝置傳遞這個病毒載體，可使用傳統的蠕蟲病毒技術進行傳播，最後變成具大規模破壞性的網路武器。[10]根據臺灣資安專家的看法，以核電廠這麼嚴密的關鍵基礎建設而言，資安防護一定也是相當嚴密，震網之所以可以躲過核電廠資安認證系統的身分認證，就是因為駭客當時竊取了臺灣瑞昱半導體和智微科技這兩家具有良好企業聲譽高科技公司的數位簽章，才躲過核電廠系統的安全認證。[11]

根據賽門鐵克的研究結果，截至2010年8月6日，受到震網影響的國家如表一。其中以中國被影響的次數最多，其次就是被美國及以色列視為威脅的伊朗，僅為中國的百分之一。

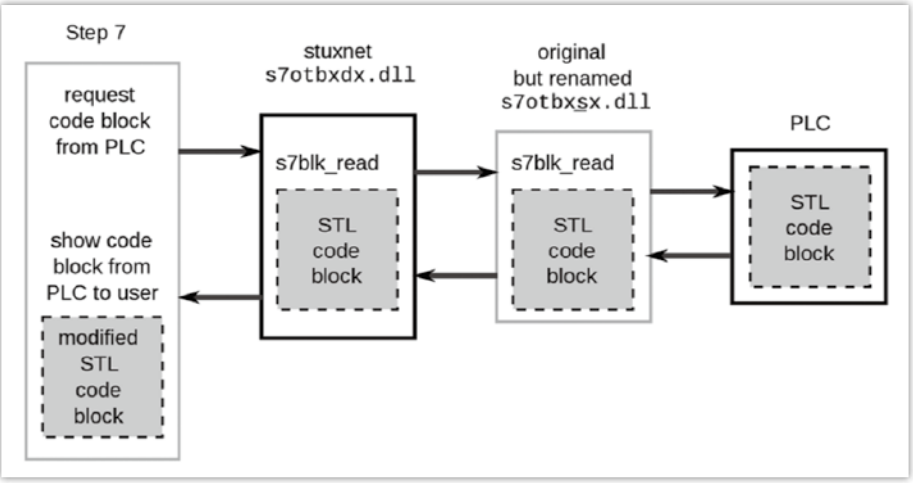
8　"Stuxnet," http://en.wikipedia.org/wiki/Stuxnet, 2015/5/6.

9　同註7。

10　Ralph Langner, "Cracking Stuxnet, a 21st Century Cyber Weapon," http://www.myoops.org/main.php?act=course& id=2257, 2015/5/6.

11　〈網路間諜瞄準企業〉《iThome技術專題》，http://www.ithome.com.tw/itadm/article.php?c=69425&s=4，2015年5月6日。

圖二　震網將原本的s7otbxdx.dll改為s7otbxsx.dll，自己則取代s7otbxdx.dll



資料來源：Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32 Stuxnet Dossier," Symantec Security Response, Version 1.4, http://www.symantec. com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, February 2011, p.37.

供電關鍵基礎設施面對網路戰的風險評估

根據伊朗核電廠被攻擊的模式與經驗，臺灣並無發展核武的野心。因此，遭植入或被網路攻擊的可能性較低，但也不能排除別有用心者，以網路攻擊核電廠運作的資訊系統，使其運轉中斷，或因受到破壞而故障。事實上，核電廠攸關兩種關鍵基礎設施的安全：資通訊與供電的安全，兩者互依性高。一般進行風險評估可以區分為後果、脆弱度與威脅等3項指標。本文從一般性的觀點來探討供電基礎設施可能面臨網路戰的後果、脆弱度與威脅。

一、後果

事件發生造成的結果，包括立即、短期與長期、直接與間接的損失與效應。損失可包括人員傷亡數、財務與經濟損傷與環境衝擊等一般可以量化表示者。後果也可包括較不具體或較難量化的效應，包括政治紛擾、士氣減損、運轉成效或軍事整備的降低或其他衝擊。就後果而言，如果核電廠遭受網路戰的攻擊，一旦因為網路戰攻擊使得離心機內部轉動過快或過慢，就有可能造成爆炸。不但會造成人員的傷亡，更會產生輻射的傷害；其引起的恐慌也會更嚴重，除了會對公眾信心造成影響，使國民對於國家經濟與政治制度的信心與整體士氣為之下挫，並對經濟造成直接與間接的衝擊。在網路上要明哲保身必須要付出很多的心力與金錢，如果沒有分散弱點與威脅的機制，任何的安全防護都不夠用。

尤其遽增的網路應用與連結技術，不但造就了快速改變的複雜環境，而且也帶來了更多的挑戰。網路被大量的商業化應用，也因為全球化而成長。例如網路元件封裝、組合、複雜、多方資源提供者與多階層合約商。未來要進行預測與瞭解網路會被如何使用是非常困難的，畢竟有太多創新與應用的方式。特別在新的弱點與風險不斷湧現後，事件層出不窮導致防禦方式顯得緩慢與不足，複雜的網路環境也使歸類罪犯的屬性變得困難。隱蔽威脅的文化也導致公眾與企業低估網路所帶來的風險。

更要注意的是，網路空間成為水、電、交通等關鍵基礎建設或軍事策略優勢的主要策劃領域，近乎三分之二的關鍵基礎建設公司發現有惡意軟體在攻擊他們的

表一　各國受震網影響次數表

國家	中國	伊朗	印尼	印度	美國	澳大利亞	英國	馬來西亞	巴基斯坦	德國
感染震網電腦數量	6,000,000 (未經證實)	62,867	13,336	6,552	2,913	2,436	1,038	1,013	993	5

資料來源："Factbox:What is Stuxnet?" Fri Sep 24, 2010, Reuter, http://uk.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUKTRE68N3PT20100924, 2015/5/8.

系統。若要強化既存的資訊安全防護能力，必須要保障國家在網路上的利益。雖擁有了良好的網路技術，但是罪犯屬性與行為的改變才是偵測的關鍵。因為網路改變生活，利益帶來威脅，持續變動的環境需要一個新的解決方案。

二、脆弱度

基礎設施資產設計、執行或運轉上的弱點，可因為天災(或為意圖不良的敵方利用)而造成設施的功能失效。此類弱點可能出現在建築特性、設備性質、人員行為、人群位置、設備與建築或運轉人員業務等方面。脆弱度通常是透過內部評估以及消費者、設備供應商、服務提供單位等所提供之資訊來進行辨識，而這些脆弱度的相關資訊，可以提供給主管機關作為風險評估之用。資訊科技方面存在許多相依性的關聯，甚至共用許多關鍵資產，資訊的運作仰賴硬體及軟體，或是其他資通訊部門所提供的服務。如果資通訊部門警覺性不夠，或是缺乏資訊科技的應變及恢復能力，提供便捷迅速服務的資通訊系統，反而會處處都是弱點，顯現出脆弱度所在。

而在核電廠方面，能源的控制系統、維護與修復系統的協調，都仰賴資訊設備與軟體，而系統運作的成功不能僅仰賴資訊設備的更新及人員訓練，而是要預想隨時會有新的威脅形成，即使無法有效制止威脅出現，但必須能夠以最快速行動，立即替換或回覆。

三、威脅

具備造成資產或人員損失或傷害潛勢的徵候、態勢與事件。在數位世界中，隱匿各地的罪犯透過各種方式企圖侵入許多國家的電腦、網路與各種服務。網路也提供了罪犯接近各處孩童與弱點， 跨各國法律管轄區，導致更難打擊犯罪。有些以國家為目標的犯罪是來自於其他國家的間諜策略，以監督某一國的政府、經濟或資產。那些愛國的犯罪者入侵之後，再散布假消息、干擾關鍵服務或在緊張的氛圍下尋求自身優勢。戰爭衝突之下，對手透過入侵降低我們軍事科技之能力，抑或是透過該技術對我方進行攻擊。

尤其在2001年「九一一」事件後，網路已被恐怖分子用來宣傳、激化潛在支持者以便聚集討論計畫、募集資金，並可能在其發現國家關鍵基礎建設之弱點後進行攻擊。以國家為攻擊目標的團體是真的存在的，針對公/私網路服務的攻擊也越來越普遍。網路的匿名性與無國界導致辨別對手之意圖更加困難。

另外，因為網路的成長，威脅也伴隨著機會來臨，而且是必須要加以對抗的。網路成長初期並沒有太注重於網路安全上，當我們放置越多的生活重心於網路就必須要越重視經濟、資產、私人資訊等安全議題。越來越多利用網路竊取、占據、破壞關鍵資料的惡徒，我們的生活就越會

受到影響。

歐洲有關關鍵資訊基礎設施的法令與經驗

有關歐洲關鍵基礎設施的正式與非正式機制中，比較有名的是「歐洲網路與資訊安全局」(European Network and Information Security Agency, ENISA)，這個單位早於2004年3月14日創立，歐盟將其視為法制實體，並透過這個單位的努力，強化歐洲資訊安全的協調與整合。[12]

「歐洲網路與資訊安全局」成立的目的在確保歐洲國家社群網路與資訊安全能夠維持在高度水準。因此，這個單位致力發展利於歐盟內的公民、消費者、企業與公部門組織網路與資訊安全。這樣的工作也讓網路市場能夠順利的運作。網路與資訊安全局的任務，主要在協助歐盟執委會、成員國以及其它的商業社群，以處理有關網路與資訊安全的需求，包括現在與未來歐盟的立法等事務。網路與資訊安全局最後希望成為歐盟成員國及歐盟體制內網路與資訊安全的專家中心，並能對網路及資訊安全等相關事務，提供諮詢。

網路與資訊安全局的工作計畫包括幾項可以做的事情。例如網路與資訊安全局透過與成員國之間的聯繫，掌握了一些網路與資訊安全領域的專家，並製作了一本「網路與資訊安全名人錄」(Who is Who Directory on Network and Information Security)，[13]網路與資訊安全局也出版電腦緊急反應小組(Computer Emergency Response Team, CERT)在歐洲執行相關活動的清單(Inventory)，[14]每一季則發行活動通訊 。除此之外，網路與資訊安全局在成員國之間也組成專題討論會(Workshop)以擴大服務及宣傳。

最後，網路與資訊安全局也界定顧客化的資訊對象群，包括有良好實踐的特定目標群體，如中小型企業(Small and Medium Enterprises, SMEs)或家庭使用者等。另外，網路與資訊安全局也創立派駐成員國聯絡官的網路，以協助網路與資訊安全局與各國之間在日復一日累積的基礎上進行資訊交流與合作。[15]

網路與資訊安全局近期的工作計畫是在2008年進行的「共同性達成影響的建構」(Build on Synergies Achieve Impact)。這項工作計畫主要是讓網路與資訊安全局能夠在與利益相關者合作的基礎上，增加在網路及資訊安全上的影響，這項工作計畫在與所有的利益相關者進一步合作方面，已經在新的途徑上發展出優先性。而且透過界定多重例行主題計畫(Multi-annual Thematic Programs, MTP)的實施，引導出3項主要的元素，如改善歐洲e通訊網路的韌性、發展與保持合作模式、為創造信任與信心來判定緊急風險。

綜合而言，網路與資訊安全局的所有活動概略包括警覺提升與促進最佳實踐，以及強化合作。同時網路與資訊安全局也警覺到本身角色的重要性，並能支持歐

12 http://www.enisa.europa.eu/index.htm., 2014/2/10.

13 http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf., 2014/2/16.

14 http://www.enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf, 2007, 2014/02/15.

15 http://www.enisa.europa.eu/index.htm., 2014/2/10.

洲委員會的策略。透過擴大影響力的活動，網路與資訊安全局致力去影響國家與歐盟層級既有的共同作用與各種方案，並將遵循更多聚焦在以影響因應為主的行動途徑。[16]歐盟於2004年3月成立歐洲網路及資訊安全局(European Network and Information Security Agency, ENISA)，以確保區域內的網路及資訊安全，並發展一個有利於民眾、消費者、企業及公部門組織的資安文化，從而促進歐盟市場順利運作。2004年7月1日，全球第一部針對網路行為加以規範的國際條約 ── 「網路犯罪公約」正式生效。該公約係由歐洲理事會26個會員國與4個非會員國(美國、加拿大、日本及南非)在2001年11月23日於布達佩斯簽署通過。

為了讓歐盟成員國之間能夠熟悉基礎設施弱點與威脅資訊交流、分享，歐盟執委會制定了「關鍵基礎設施保護預警資訊網路」(Critical Infrastructure Warning Information Network, CIWIN)。這個資訊網路的目的是在協助成員國、歐洲的既有機制、基礎設施的擁有者及運作者，能夠對基礎設施的弱點與威脅，以及適當措施及策略進行交流，以支持關鍵基礎設施的保護。[17]

關鍵設施是現代社會的最基本骨幹，而且日益依賴資訊科技與通訊系統。由於資訊系統的日益滲透，使資訊科技可以提供物超所值的服務。另一方面，正如在美國及歐洲所顯示的案例，在動亂的事例中，暴動者的行為難以被控制。此種增加的複雜性，以及多面向的傳統與急迫性威脅危害許多與資訊科技聯結的系統。關鍵基礎設施越來越吸引社會大眾的注意，目前模擬科技已經擴大進入基礎設施程序與運作的分析與規劃，在近期對於關鍵基礎設施，以歐盟的資訊基礎設施系統整體風險降低計畫(Integrated Risk Reduction of Information- Based Infrastructure System, IRRIIS)作為角色模型來分析。[18]

事實上，在歐盟執委會所制定的預警網路中，原就希望透過成員國能建構一個論壇，以做為關鍵基礎設施保護觀點的交流，以及支持關鍵基礎設施擁有者與運作者的最佳實踐。同時這個預警網路可以成為連結歐盟成員國之間的快速警報系統(Rapid Alert System, RAS)。因此，綜合而言，預警網路同時具備雙重功能，既可作為連結成員國之間的快速警報系統，也可以成為論壇以交流關鍵設施保護的觀點與實踐作為。姑且不論最後選擇的作為為何，預警網路可以補充現有網路的不足，而且不會重複。[19]

在公私夥伴關係進行關鍵基礎設施保護的過程中，資訊分享的概念非常重要

16 http://www.enisa.europa.eu/doc/pdf/management_board/decision/enisa_wp_2008.pdf., 2014/2/5.

17 美國從2003年開始也有類似的預警系統，http://www.gao.gov/new.items/d05434.pdf., 2014/2/8.

18 Walter Schmitz, "Simulation Experiments: the Emerging Instruments for CIP," International Journal of Critical Infrastructures, 5.1/2, 2009, p.5.

19 Commision of the European Communities. The Green Paper on a European Program for Critical Infrastructure Protection(Brussels, 17 November 2005),COM(2005)576 FINAL, p.24. http://www.libertysecurity.org/IMG/PDF/ EC_-_Green_Paper_on_CI_-_17.11.2005.pdf, 2014/2/3.

。因為這涉及公私部門、大公司與國家之間資訊的交流，並被政府與研究者視為最重要的公私夥伴議題。根據美國的經驗，在關鍵基礎設施保護中，與利益相關者的資訊分享是最迫切的需求。[20]雖然資訊分享的概念早已形成，但其內容仍很模糊，究竟該由誰交換威脅資訊給誰，目前仍不是非常明確。

資訊分享可以分為4個層級：政府內部的資訊分享、不同國家政府的資訊分享、不同公司之間的資訊分享，以及政府與私領域部門的資訊分享。[21]政府內部及不同政府之間的資訊分享可以嚴格的作為早期預警之用，因為當另一國政府獲得重要資訊時，也必須提供手中掌握的情報資訊給其他政府，如「資訊分享國家戰略」(National Strategy for the Information Sharing, NSIS 2007)的公布也是一種方式。[22]

在私領域中，資訊分享就更顯得重要。民營公司無法執行有效的保護策略，主要因為缺少有關足夠威脅數量及質量的可靠資訊。[23]沒有任何公司能夠預測未來遭受攻擊的損失程度。因此，為了資訊安全，在最樂觀的投資下就無法評估所得的利益。除此之外，有關威脅的數量與質量變化快速，在採取潛在反制作為時，容易產生混淆，故而很難建立可以隨之調整的有效因應策略。在此情況下，最佳的方式就是讓這些不同的公司能夠交換他們經驗，[24]這樣的經驗可以發揮早期預警的效果。

因為資訊分享是資訊安全領域中最主要的早期預警，因此從1988年發生「電腦蠕蟲」(Morris Worm)攻擊事件後，就成立了資訊分享的組織—電腦緊急事件反應小組(Computer Emergency Response Team, CERT)。這個小組企圖建立的專家網路對電腦威脅已構成最佳反應。這樣的事件不只牽涉到事件的管理，也包括預防與早期預警。但必須強調的是，這個小組主要並不是強化早期預警的能力，而是對突發事件的反應。若將反應小組比擬為消防隊，就可以瞭解其主要是在消防及滅火，預防與早期預警則是次要工作。也因為如此，在電腦緊急事件反應小組所做的資訊分享主要是與受影響的企業合作，並聚焦在科技資料的交換。相關法令整理如表二。

美國瞭解需要更廣泛的資訊分享，於是在1990年代為關鍵基礎設施的擁有者及運作者設立了「資訊分享與分析中心」(Information Sharing and Analysis Centers, ISAC)。原本美國想要建立一個大型的分

20 President's Commission on Critical Infrastructure Protection, Critical Foundation: Protecting America's Infrastructure, Washington, D.C. : US Government Printing Office,1997, pp.28～31 .

21 Myriam Dunn Cavelty and Manuel Suter, "Early Warning for Critical Infrastructure Protection and the Road to Public-Private Information Sharing," Inteligencia Y Seguridad, 4, 2008, p.97.

22 http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf, 2015/2/3.

23 Ross Anderson and Tyler Moore, "The Economics of Information Security," Science, Vol.314, pp.610～623.

24 Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," Informaiton System Research, Vol.16, pp.186～208.

享與分析中心，最後則決定依照每一基礎設施的範圍建立獨立的分析中心。[25]在成立之後，對於各自領域的資訊安全已經有了明顯的改善。美國在2002年聯邦政府頒布電子化政府法案的第三章(Title III)－聯邦資訊安全管理法(Federal Information Security Management Act of 2002, FISMA)。2002年11月正式簽署「國土安全法」(Homeland Security Act, 2002)，要求國土安全部發展國家級計畫來保護美國的重要基礎建設，而國土安全部(DHS)也於2003年4月頒布受保護的重要基礎設施資訊計畫(Protected Critical Infrastructure Information Program, PCIIP)。美國明定聯邦調查局(FBI)具有犯罪調查權。

這也顯示相關領域的企業間進行廣泛資訊分享，形成一種非常有效的早期預警，而且可以充分的分享相關可能攻

表二　歐盟資訊安全相關法令一覽表

項　次	類別	條　文　名　稱
第一部分	條例	歐洲議會和歐盟理事會2004年3月10日關於建立歐洲網路與資訊安全局的第460/2004號條例([2004]OJL77/1)。
第二部分	指令	1.歐洲議會和歐盟理事會1998年6月22日關於制定技術標準和規章領域內資訊供應程式的第98/34/EC號指令(技術標準與規章指令)。 2.歐洲議會和歐盟理事會2000年6月8日關於共同體內部市場的資訊社會服務，尤其是電子商務的若干法律方面的第2000/31/EC號指令(電子商務指令)。 3.歐洲議會和歐盟理事會2001年5月22日關於協調資訊社會版權及鄰接權若干方面的第2001/29/EC號指令(資訊社會著作權指令)。 4.歐洲議會和歐盟理事會2002年3月7日關於電子通信網路及相關設施接入和互聯的第2002/19/EC號指令(接入指令)。 5.歐洲議會和歐盟理事會2002年3月7日關於電子通信網路和服務授權的第2002/20/EC號指令(授權指令)。 6.歐洲議會和歐盟理事會2002年3月7日關於電子通信網路和服務的公共監管框架的第2002/21/EC號指令(框架指令)。 7.歐洲議會和歐盟理事會2002年3月7日關於電子通信網路和服務的普遍服務和用戶權利的第2002/22/EC號指令(普遍服務指令)。 8.歐洲議會和歐盟理事會2002年7月12日關於電子通信行業個人數據處理與個人隱私保護的第2002/58/EC號指令(隱私與電子通信指令)。 9.歐洲議會和歐盟理事會2002年9月23日關於消費者金融服務遠端銷售及修正歐盟理事會第90/619/EEC號指令、第97/7/EC號指令和第98/27/EC號指令的第2002/65/EC號指令(遠端金融服務指令)。 10.歐洲議會和歐盟理事會2004年3月31日關於協調公共建設工程合同、公共供應合同和公共服務合同授予程式的第2004/18/EC號指令(政府採購指令)。 11.歐洲議會和歐盟理事會2004年4月29日關於知識產權執法的第2004/48/EC號指令。 12.歐洲議會和歐盟理事會2006年3月15日關於存留因提供公用電子通信服務或者公共通信網路而產生或處理的數據及修訂第2002/58/EC號指令的第2006/24/EC號指令(數據存留指令)。 13.關於歐盟理事會制定確認、標明歐洲關鍵基礎設施，並評估改善保護的必要性的指令的建議。

25　John D. Moteff, Critical Infrastructure: Background, Policy and Inplemention: Congressional Rsearch Report for Congress, RL30153,13 March 2007, Washington, D.C.:Congressional Research Service, 2015, pp.23～35.

第三部分	決定	1.歐盟理事會1992年3月31日關於資訊系統安全領域的第92/242/EEC號決定/341歐洲議會和歐盟理事會1999年1月25日關於採取通過打擊全球網路非法內容和有害內容，以推廣更安全地使用網際網路的多年度共同體行動計畫的第276/1999/EC號決定。 2.2001年12月27日在第95/46/EC號指令下，關於向在第三國的處理者傳輸個人數據的標準合同條款的委員會決定(2002/16/EC)。 3.歐洲議會和歐盟理事會2003年6月16日修訂關於採納通過打擊全球網路上的非法內容和有害內容，以推廣更安全地使用網際網路的多年度共同體行動計畫的第276/1999/EC號決定的第1151/2003/EC號決定。 4.歐洲議會和歐盟理事會2003年11月17日關於為監管電子歐洲2005行動計畫，傳播實踐範例和改善網路和資訊安全而採納多年度計畫(2003-2005)的第2256/2003/EC號決定。

資料來源：參考馬民虎編譯，《歐盟資訊安全法律框架：條例、指令、決議和公約》(北京：法律出版社，2009年)，所列法條及內文。

擊行動的情報。但因為這些分析中心無法即時獲知攻擊的內涵與手段，又無法掌握行為者的背景與動機，使其能力受到限制。

對臺灣的啟示

關鍵基礎設施為人民日常生活所必須，一旦遭受資訊戰或駭客戰攻擊而中斷，不僅造成生活不便，亦連帶造成社會大眾心理的不安，進而擴大社會的動亂。近年來國土安全的目標，除了傳統的國家安全項目外，主要重點並置於維繫全民生活、政府組織、國家重要經濟生產的範圍。處於社會發展科技化與人口向都市化集中的今日，國家的目標在於維繫整體設施的安全，使國家的運作不至於因為天災或人為破壞，而產生停頓，影響整體國力的進展。

關鍵基礎設施的保護必須先擬具一套完整的推動策略，以既定的策略目標來引導不同部會運用其功能與資源，並協力民間資源共享，有效推動關鍵基礎設施的安全保護。

一、確保關鍵基礎設施質量供應無虞

確保電在質量上供應無虞是推行保護策略的首要目標，但也是最基本的。在平時無所缺乏時，上述物資的供應會像打開水龍頭般的理所當然，但若受到不可抗力因素影響，無法獲得相關的供應時，其所引發的民怨會累積成為埋怨政府的負面能量。如果肇發原因是天然災害所造成的，在全民共同瞭解環境因素下，會降低衝擊與影響。但如果政府缺乏應變能力，或是對於可能發生之天然及人為災害應變處置能力不足，就顯示政府沒有一套靈活應變的安全保護策略。因此，安全保護策略的首要目標就在於如何確保關鍵基礎設施的運作及質量供應無虞。

二、建立不同層級單位的安全保護法制

安全保護策略必須結合相關單位的能力及運作，不是隨性的突發性作為。為了確保關鍵基礎設施的運作及供應無虞，有賴一套靈活應變策略，但這些策略必須建立在不同層級單位的法制，才能免於人治色彩所造成的區別性與差異性。受全球化、資訊化發展之影響，以及各國間互賴程度的增加，使得影響關鍵資訊基礎設施之安全問題，不再侷限於單一區域，因此更需要各方多元的合作。然而，國內有關關鍵基礎設施之法規(關鍵基礎設施安全防護條例草案)目前尚在起步階段，未來應可借鏡美國、日本等先進國家之經驗，

逐步建立法源。為了貫徹上下級單位的安全保護作為，必須從上而下的建立戰略指導、執行法規、應變計畫、施行細則及配套規定等，構成一套能夠貫徹戰略目標的嚴密安全保護法制系統。

三、具備有效整合的狀況處置與應變能力

安全保護策略不是紙上作業，更不是聊備一格的文書案牘，而是要透過安全保護策略的制定，讓政府及民間相關安全保護機構具備有效整合的狀況處置與應變能力。關鍵基礎設施的安全保護需要政府、民間的資源共享及協力，才能有效整合處置關鍵基礎設施的應變。在共同的策略目標下，如何針對達成目標的方法及手段有效運用，也是主要的目標。關鍵資訊基礎建設保護不僅僅是領域內各機構的協同保護計畫，亦牽涉到跨領域的協同合作。例如金融與醫療系統仰賴以維持資訊機房、資訊設備的運作，亦仰賴網路系統的傳遞資訊。一旦因通訊或電力系統失效導致這些底層運作機制失靈，將嚴重影響金融與醫療體系的運作。可見關鍵資訊基礎建設的任一缺口對於民眾生命、生態環境、經濟與政治均會產生重大的影響。[26]

四、完善現有關鍵基礎設施的應變體制

根據災害防救應變相關法令，關鍵基礎設施保護也與災害防救應變體制息息相關。如臺灣電力公司依《災害防救法》第十九條規定，訂定臺灣電力公司「輸電線路災害防救業務計畫」，呈報經濟部等中央災害防救主管機關核准後實施。[27]經濟部並訂有「經濟部所屬事業各類災害及緊急事件速報程序」，要求事業單位於發生工安衛生災害(爆炸、火災、危害物質洩漏或運輸事故、重大職災)、生產事故(電廠跳機、限電、重大損失)、環境影響事項時，必須半小時內先以電話回報，並於1小時內填妥後速報經濟部。

我國資訊安全事件通報之規範，主要以「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」、「國家資通安全通報應變作業綱要」等作為執行依據。其中，「行政院及所屬各機關資訊安全管理要點」第10點，要求各機關(構)應評估各項人為及天然災害對機關(構)正常運作之影響，同時訂定緊急應變及回復作業程序，與規範相關人員之權責。

另外，各機關(構)應建立緊急處理機制，在資訊安全事件發生時，應依規定之處理程序，立即向權責主管單位通報，採取反應措施，並聯繫警調單位協助調查等。國內各機構之資安事件判定等級，均依據行政院國家資通安全會報為主，範圍僅侷限於資安事件之處理，尚未全面涵蓋關鍵資訊基礎設施防護事件，故有重新檢視分級之必要。[28]

無論是國營所屬資訊分享交換機制、臺灣電腦危機處理協調中心、臺灣網路資訊中心等，雖在自身體系內有完整的資安通報應變機制，但仍應進一步建立跨領

26 行政院科技顧問組，《關鍵資訊基礎建設保護政策指引》，2011年12月31日，頁27。

27 參考經濟部民國93年8月6日經授營字第09320292030號函「公用氣體與油料管線、輸電線路災害防救業務計畫」、臺灣電力公司《災害防救要點》相關內容訂定。

28 同註26，頁29。

域、跨體系之情資整合、通報應變能力與可互通之資訊交換標準。另外，以整體處理流程來看，國內各關鍵資訊基礎設施，亦須整合早期預警、偵測、監控、分析、處理、復原與數位鑑識等機制，實有建立跨領域整合服務機制，統合整體資訊之需要。

五、保護策略演訓驗證

任何一個完善的安全保護策略都必須經過演練，才能驗證其可行性。而且在演練過程中，必須儘可能的召集所有扮演安全保護功能與角色的單位，務實嚴謹的針對各種可能狀況，逐一進行演練工作。類似的演練必須先完成演練指導計畫，依據外國曾經發生案例，考量國內民情及設施，制定狀況想定及處理計畫。而從兵棋推演開始，逐步擴大到實兵驗證，透過一系列的驗證措施，檢討計畫可行性，以及中央、地方政府、事業單位、民間廠商所應扮演的功能。

六、國家支助網路攻擊的回應

電影中經常發現網路駭客挑戰國安等級，直搗核武機密的情節。真實世界裡，各國情報單位都不敢輕忽病毒可能造成的國家機密外洩問題。網路戰方式早已不同，過去流行竊取網銀帳戶或個資已經不夠看，各國政府甚至已經開始利用網路惡意程式來互相攻擊及牽制。根據《紐約時報》報導，美國政府為了避免擴大戰爭的傷害層級，在小布希時代便選擇對伊朗等疑似發展核武的國家發動網路攻擊，甚至以「震網」等侵襲該國核設施，成功阻止伊朗核武發展。

不過雖然成功避免核武戰爭，但震網病毒卻曾因程式錯誤，而造成了全球網路病毒肆虐，使得網民也不免受到蠕蟲病毒的影響。芬安全(F-Secure)公司公布的研究報告除了詳細揭示了震網病毒以及今年最流行的火焰綜合式木馬病毒惡意程式的改變及威脅外，根據病毒實驗室的估計，開發改良震網的駭客人數一年已超過10人，使得病毒變化的速度比以往更快、傷害性更高。

震網以及它的變種火焰惡意間諜軟體的遊戲規則已經與以往不同，雖然所造成的重大損失多半是因為駭客主要是針對國家等級的網路，如水庫、油井、電廠等重要基礎設施發動攻擊，但變形之後的病毒反而會透過消費者幾乎每天使用的隨身碟、外接硬碟等行動儲存裝置散播，一旦被感染，以現在的使用習慣，很可能連手機、平板電腦等都難逃一劫。此類病毒變形快速，只要使用者連上網路，就會自動啟動更新系統，使用者根本防不勝防。

七、強化防護陣線

時間是網路攻防戰的重點戰略，為了確保操作系統的安全，最好的防範之道還是隨時更新安全軟體的病毒碼，讓專業的網路戰士協助全面性建立防護陣線。[29]另外，虛擬化主要用來整併伺服器與IT資源，以節省成本與空間。虛擬化風行以來，也發現許多意料之外的用途，例如企業逐漸利用虛擬化技術來建置額外的安全防護層。以檢查點(Check Point)為例，現在客戶可透過Amazon Web Services採用檢

29 〈駭客過招挑戰國安等級 情報單位嚴陣以待對抗網路蠕蟲〉《資安人科技網》，http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7053 ixzz2EpoKHvFg，2014年12月3日。

查點的安全閘道器，或可用防火牆、入侵防禦系統、應用程式控管、網址過濾等檢查點軟體及其他防護措施，保護公司資料在雲端的安全。[30]

結　論

基本上，網路攻擊行動依照其動機、手段，可以區分為針對企業、機構及國家安全單位不同層次，其所造成影響大致也可以歸納為對企業、對國家或是對國際政治等。由於資訊科技的發達，各種網路攻擊的科技與手段不斷變化，如果僅屬於個別駭客，或是個人隱私資料遭到破壞或竊取，姑且可以歸納為網路的犯罪行為，並依照一般的相關犯罪法制處理即可。

但是從過去一年的網路衝突來看，部分區域安全衝突因為直接性軍事行動的衝擊過大，或是因為民族主義所引起的激烈行為延伸到網路世界，由國家支助的駭客行為，或是針對國家或政治組織的攻擊行為會越來越多。也因為犯罪證據的難以掌握，或是容易加以否認與撇清責任，未來國家支助的駭客行為，將隨著國際衝突的發生而更趨頻繁。

政府部門各有其職責，對於可預見事故的危害，或對自然災害的發生，均有一定的認知，並依機關內部的要求，預先擬定相關的保護計畫。惟對於危害的認知，或處置作為大都僅及於機關內部的因應措施，鮮少有與其他機關相配合。對於目前的災難、危害狀況，常常是一個機關無法完全排除的，或災害所引起的效應及其他的政府設施功能，卻因缺乏協調，導致事倍功半。

在關鍵基礎設施安全保護策略上也是如此，如供電會影響社會大眾生活甚鉅，在未事先擬定完善的安全保護策略下，倘若遇到關鍵基礎設施的天然或人為災害，將會漫無頭緒，捉襟見肘。因此，必須在明確的策略目標下，以符合國家安全需求的法制為基礎，透過宣傳、教育訓練、驗證及考評等各種積極作為，以成功的推動關鍵基礎設施的安全保護工作。

個別國家或機構為了自保，必須針對各種網路犯罪或攻擊行為及早採取防範措施，但是面對國家支助的駭客行為，被動防護或是攻擊性軟體問市後，才相應採取防護作為都略顯消極。雖然資安服務產業相對日趨蓬勃，但對國家而言，一味被動防護似乎不如採取攻擊性作為，致力發展防護科技之際，也同時研發網路攻擊武器，藉以竊取或懲罰發動網路攻擊者。如果是針對核電廠的網路攻擊，因為核電廠的任何事故，都會引發政治與經濟後遺症，茲事體大，絕對不能輕忽。而且也必須警覺到資訊科技日新月異，各種病毒軟體也在推陳出新，更必須具備有效應變能力，掌握資訊科技發展趨勢，隨時準備因應各種類型的網路攻擊行動。

(本篇選錄自陸軍通資半年刊第125期)

30　賴姿侑，〈2012年資訊安全發展趨勢行動社交網路攻擊變形再進化以人為本才是防護重點〉《科技商情》(2012年2月13日報導)，http://www.digitimes.com.tw/tw/dt/n/shwnws.asp?cnlid=13&cat=1&id=0000271008_FUPL 8XYV1JZ4E17EF44J0&cat1=25&cat2=10#ixzz2EoiZrGjA，2014年12月3日。