增進關鍵基礎建設防護機制，強化國土安全

莫大華　國防大學政戰學院政治系副教授

關鍵基礎建設(critical infrastructures)，是指那些與維持國家最起碼的經濟、民生與政府運作息息相關的實體的和以資訊電子爲基礎的系統。它們包括了公民營的電信、能源、銀行、財金、交通、供水、以及急難救助等系統，由於資訊與電子科技之賜，關鍵基礎建設的自動化與資訊化程度越來越高，系統與系統之間的相互連接愈來愈緊密、資訊交換與作業互動也愈趨頻繁，但也可能因爲裝備故障、人爲錯誤、天候及其他自然因素，或遭受實體與資訊電子攻擊等，使系統失效或被破壞，而嚴重影響國家安全、經貿活動以及人民福祉。但基於美國的發展經驗，關鍵基礎建設一詞已經不足以涵蓋國家所可能面臨的生存威脅，遂以「關鍵基礎建設與重要資源」(Critical Infrastructure and Key Resources, CI/KR)稱呼。

1996 年，美國柯林頓政府頒佈了第 13010 號行政命令(Executive Order13010)－「關鍵基礎建設防護」(Critical Infrastructure Protection)，強調電力、天然氣及石油的生產、儲存與輸送、電信、銀行與金融、水供應系統、交通運輸、急難救助體系、政府運作功能等爲關鍵性的國家基礎建設。並於該年 7 月，集合政府與民間產業界，成立了直屬總統的「國家關鍵基礎建設防護委員會」(President's Commission on Critical Infrastructure Protection)以推動及研擬與關鍵基礎建設有關的國家政策。其範疇包括天然災害、人爲疏誤、駭客入侵、產業間諜、組織犯罪、恐怖活動、網路作戰等。「國家關鍵基礎建設防護委員會」於 10 月完成研究報告與建議，1998 年 2 月 26 日，司法部與聯邦調查局於華府的調查局總部成立了「國家基礎建設防護中心」(National Infrastructure Protection Center)，該中心由聯邦、州、及地方政府相關機構代表與業界代表聯合組成，下設：(一)電腦調查及工作小組(Computer Investigations and Operation Section)，負責電腦入侵之調查、協調與技術支援工作，並藉網路緊急支援小組(Cyber Emergency Support Team)提供遭攻擊之關鍵基礎建設必要支援。(二)分析與預警小組(Analysis and Warning Section)，負責分析關鍵基礎建設之脆弱性以及可能遭受之實體與網路攻擊的風險，蒐集來自公部門、執法機構、情報機構、或民間部門所提供之產業資料，分析並向政府或業界提供適切建議。此外，另有監控作業中心(Watch Operations Center)，與業界、情報、執法、國防等單位合作，適時偵測網路威脅，發佈評估，警告及建議給有關單位運用。(三)訓練、推廣及策略小組(Training, Outreach and Strategy Section)，負責策定該中心的執行策略與預算，並持續對地方、州、聯邦及國內外執法及安全單位、人員，提供與網路及基礎建設防護相關之教育、訓練與演習計劃，藉以喚起全民警覺意識認知，獲取全民的信任。

1998 年 5 月 22 日，柯林頓政府頒布了兩項新的政策指令，用以強化美國對抗恐怖主義及非傳統威脅之能力。總統第 62 號決策指令(Presidential Decision Directive 62)明示了國家面臨的非傳統威脅，包括「網路恐怖主義」，化學、輻射、與生物武器，以及對

抗此等武器的新式系統化手段。總統第 63 號決策指令則強調如何防護可能來自外國政府、國內外恐怖組織，以及國內外犯罪組織對國家關鍵基礎建設的實體與網路攻擊。因此，「國家基礎建設防護中心」遂成爲政府整體防護架構的一部份，擔任針對關鍵基礎建設威脅評估、警告、調查，以及對攻擊反應的主導角色。911 攻擊事件之後，美國政府更加強了，也加速了確保國家關鍵基礎建設的決心與作爲，期能建立一套模式並透過民間企業的參與，共同達成防護關鍵基礎建設的目標。

布希總統遂在 2001 年 10 月 16 日簽署行政命令 13231 號「資訊時代的關鍵基礎建設防護」(Critical Infrastructure Protection in the Information Age)成立「關鍵基礎建設防護理事會」(President's Critical Infrastructure Protection Board)，負責建議與協調有關防護關鍵基礎建設資訊系統的計畫，將通信資訊安全與關鍵基礎建設結合，理事會由部會首長組成，主席由總統的網路空間安全顧問(the Special Advisor to the President for Cyberspace Security)擔任，並納編部會的相關司處首長組成轄下的協調委員會，以及由理事會決議成立的常設委員會或小組(subcommittee)，負責協調政府與民間的相關安全防護的規劃、執行、評鑑。同時也將原先的 1982 年成立「國家安全通信顧問委員會」(National Security Telecommunication Committee)改組，並成立「國家基礎建設顧問理事會」(National Infrastructure Advisory Council)，兩者都是總統的政策顧問管道。「國家基礎建設顧問理事會」期限兩年，除非總統延長期限。

2003 年 2 月，布希總統公佈「國家關鍵基礎建設與重要資產實體防護策略」(The National Strategy for Physical Protection of Critical Infrastructure and Key Assets)作爲美國關鍵基礎建設防護的基本策略，其中將國家紀念建築物與肖像、核能電廠、水壩、政府設施與商業重要資產(如商業中心、辦公大樓、運動場、主題樂園等)列爲重要資產應予以防護。

2003 年 3 月 1 日，「國家基礎建設防護中心」改隸新成立的國土安全部，隸屬於「資訊分析與基礎建設防護室」(Information Analysis and Infrastructure Protection Directorate)，並依據總統國土安全第 7 號命令－「關鍵基礎建設認定、優先性與防護」(Critical Infrastructure Identification, Prioritization, and Protection)發布「國家基礎建設防護計畫」(National Infrastructure Protection Plan, NIPP)整合關鍵基礎建設與重要資源(key resources) 全國政府與民間的防護作爲，以有效地運用聯邦經費與資源降低脆弱性、嚇阻威脅與減少遭受攻擊或意外事件的後果。「國家基礎建設防護計畫」是以相關部會首長(包括農業部、商務部、國防部、教育部、能源部、環保署、調查局、衛生部、國土安全部、內政部、司法部、核能管制委員會、國務院、運輸部)共同簽署協議(Letter of Aggrement)的方式公佈，以顯示政府的決心。在「國家基礎建設防護計畫」中，國土安全部列出所認定與優先的防護關鍵基礎建設與重要資源部門，並且必須在「國家基礎建設防護計畫」核准後的 180 天內協調公私部門擬定「特定部門的防護計畫」(Sector-Specfic Plans, SSPs)配合「國家基礎建設防護計畫」的風險管理架構，「特定部門的防護計畫」內含該部門的防護活動與資訊分享的機制與協定。「國家基礎建設防護計畫」也包含了

「國家基礎建設防護計畫初步執行提議」(NIPP Initial Implementation Initiatives)以落實執行相關的防護作爲及措施。

從美國關鍵基礎建設與重要資源體制的發展過程，個人提出以下的幾點建議，就教各位先進：

一、建立國家層級的國家關鍵基礎建設與重要資源統一指揮機制：政府目前將關鍵基礎建設的防護過於偏重在通資訊的基礎安全，例如政府的「建立我國通資訊基礎建設安全機制計畫」即可看出此點(但是在其目的說明時，卻又是「針對電力、電信、金融、交通等**國家基礎建設之安全維護**，共同研析相關因應作爲」，個人認爲會轉爲通資訊防護機制是因爲研擬計畫者假定了「**在資訊戰進行時**，我國至少必須能維持下面體系的正常運作」)，就國家關鍵基礎建設與重要資源防護而言，應擴展其安全機制(行政院國家資通安全會報可以擴大成國家關鍵基礎建設防護理事會；行政院國家資訊通信發展推動小組可以擴大成國家關鍵基礎建設防護執行委員會)而有效協調政府內部及政府民間部門就關鍵基礎建設與重要資源(仍待有關單位明確界定)的安全防護(針對實體攻擊以及網路攻擊)，規劃建立通報、資訊分享、協調合作及應變機制。

二、加速研擬防制國家關鍵基礎建設與重要資源防護政策與法規：邀集學者、專家及相關主管機關，定期召開研討會或專案研究計畫，共同研究增修相關政策與法規，以健全防護體制的規劃與執行。

三、積極發展關鍵基礎建設與重要資源防護相關的核心軟硬體技術：政府應與民間部門合作發展評鑑風險、風險管理等分析技術與監測預警技術，若能發展成資訊軟體系統尤佳，通資安全的防護資訊系統的開發更是重要，以及防護實體安全的硬體技術，藉以認定、設定防護優先性與措施。

(一)強化防護作爲

1.降低災損引發的效應

關鍵基礎建設的設置多集中於城市內，若攻擊後環境過度損害，造成結果惡化的可能性遠比攻擊偏僻地區來得大，應盡量降低受災損所引發之效應。在防護強化上應先評估災損引發之影響。假設敵人以關鍵基礎建設或重要資源作爲攻擊目標時，若事先已透過評估預測引發的效應程度大小，則可藉由分散、建立備份、成立第二中心、或先期可增加其防護方式或擬定應變對策，使第一時間內能達到有效控制，以降低災損引發效應。而降低受到災害損失後所影響的範圍。

2.建構防護與救援機制

關鍵基礎建設中攸關國家安全指揮的機制應積極建構重要指揮處所及電力設施及通訊系統地下化設施，使其具有標準之防護功能。甚至，遭受破壞與攻擊時，也能具備救援修護的機制，儘早恢復運作。至於國家歷史紀念建築物或肖像也應建構基本的防護或應變措施與作為，例如故宮博物院文物的防護。

(二)妥擬應變作為

政府應針對不同關鍵基礎建設與重要資源屬性，與民間部門建立與保持協調溝通管道暢通，構建共同防護機制網絡。在敵人各種方式攻擊中，得以有效防護與降低所受到之影響。

1.加強狀況判斷研討與演習

將定位於關鍵基礎建設與重要資源之建設、設施與機構處所，依據重要性及防護重點工作項目，針對環境、現地威脅與風險及預判可能發生之危安因素，做好不同臨危的狀況判斷，以透過政府與民間共同研討的方式，訂定適切可行的各產業與設施的應變計畫，詳列各種工作要項、預防措施、緊急應變作為，在計畫中律訂各單位之職責，使能明確分工及建立各單位之責任制度，把單位中人力及可使用之資源做任務賦予與編組。平時要加強狀況下達與任務演練，將關鍵基礎建設與重要資源內的人、物力做好防護編組，藉由定期或不定期的演習針對不同狀況的下達做驗證，當有問題發生時則能透過研討做改進與修正。經過不斷強化的狀況判斷研討、演練與演習，未來在面對受敵攻擊及人為蓄意破壞等各種突發緊急狀況時，則能臨危不亂，在有限的時間內或資源下做好各項應變。

2.建立檢查與回報系統落實預防整備工作

就國家關鍵基礎建設與重要資源防護的缺失或可能發生的危安事件，應積極檢討與擬定改進方案，藉由探討各種可能發生的成因，在落實預防整備工作上，可以針對各不同的關鍵基礎建設擬定每日安全防護檢查表，以對檢查表中各項目之檢查，來做到最初步的防護，若對發現安全防護上之缺失，應立即更正或短時間內改進，並列為複查重點，嚴格檢查，並就關鍵基礎建設與重要資源的優先性選擇必要的建設與資源，建立回報系統由上述提議的國家層級的統一指揮機制(類似於美國的監控作業中心)，以避免形成安全防護的漏洞，由逐步的檢查、改進與減少安全防護的疏失。

3.關鍵基礎建設防護管制措施

在關鍵基礎建設內建立各項管制措施，以構成多重綿密的安全檢查管制防線，落實人員安全等級分級制度，禁止非相關人員進入關鍵基礎建設與重要資源的核心地帶，藉由此種主動的安全防護管制與識別管制系統，防止遭受攻擊或破

壞。當然恢復原有的重要建設或設施的保安警察或橋隧警備部隊也是可以考慮的範圍，否則也就必須將某些優先性較高的關鍵基礎建設列入軍警防護的範圍，避免敵人進行實體破壞。

四、成立「國家關鍵基礎建設防護訓練中心」：除了協調各相關政府單位與民間部門辦理內部的關鍵基礎建設防護訓練外，應該由行政院在上述的統一指揮機制下成立「國家關鍵基礎建設防護訓練中心」負責統合性的訓練計畫，以及年度演練與演習(可併入萬安演習進行)。