美國政府對關鍵基礎設施防護的戰略思維

◆ 華梵大學特聘教授 ── 朱惠中

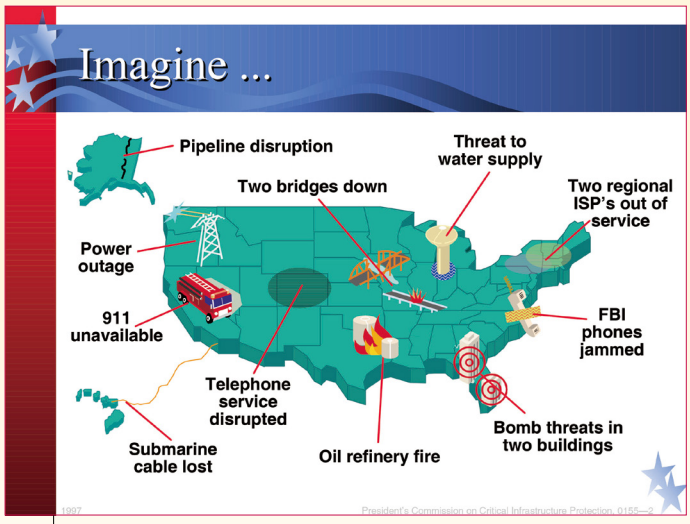
2001 年美國發生舉世震驚的 911 恐怖攻擊事件，恐怖組織利用「網際網路」作為指揮通訊工具，以民航機分別衝撞位於紐約的世貿大樓和華府的五角大廈，造成慘重傷亡，並癱瘓美國國土防衛及金融體系。隨著網際網路科技的日新月異，除已提高了攻擊行動的不可預測性，亦暴露出關鍵基礎設施的弱點。

回顧

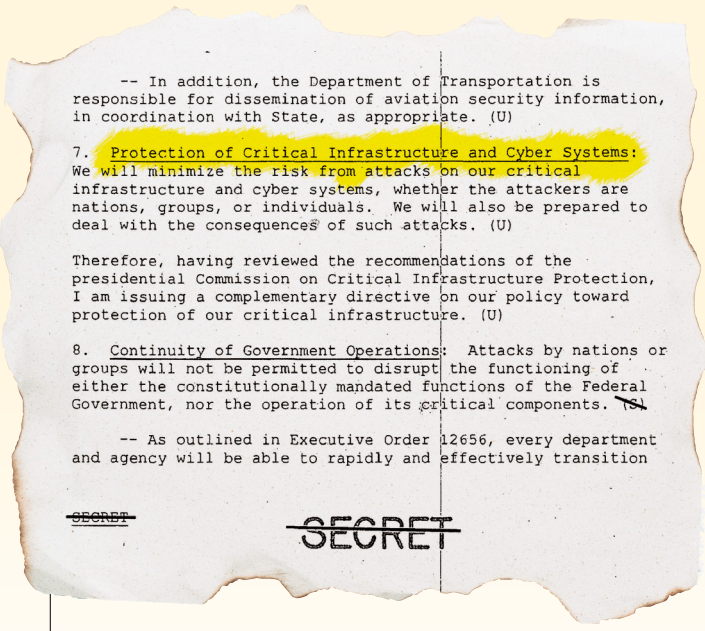
自 1996 年 6 月 15 日愛爾蘭共和軍（IRA）在英國曼徹斯特市中心發起的一場恐怖襲擊後，強化「國土安全」已成為美國新世紀的核心戰略思維，亦即思考如何更完善的規劃國家關鍵基礎設施安全之防護。近 25 年來，美國歷任總統（柯林頓、小布希、歐巴馬、川普、拜登共 5 任）均將「關鍵基礎建設防護」列為其施政的核心與重點，茲簡要回顧此 5 任總統對關鍵基礎設施防護的作為及各項指令如次：

一、柯林頓時期

1996 年 7 月，美國柯林頓政府頒布了第 13010 號行政命令（Executive Order 13010）─「關鍵基礎建設防護」（Critical



柯林頓政府頒布的第 13010 號行政命令強調電力、石油、電信、水供應系統、交通運輸、急難救助體系等各種運作功能為關鍵性的國家基礎建設。（Source: Homeland Security Digital Library, https://www.hsdl.org/?abstract&did=2361）



-- In addition, the Department of Transportation is responsible for dissemination of aviation security information, in coordination with State, as appropriate. (U)

7. Protection of Critical Infrastructure and Cyber Systems: We will minimize the risk from attacks on our critical infrastructure and cyber systems, whether the attackers are nations, groups, or individuals. We will also be prepared to deal with the consequences of such attacks. (U)

Therefore, having reviewed the recommendations of the presidential Commission on Critical Infrastructure Protection, I am issuing a complementary directive on our policy toward protection of our critical infrastructure. (U)

8. Continuity of Government Operations: Attacks by nations or groups will not be permitted to disrupt the functioning of either the constitutionally mandated functions of the Federal Government, nor the operation of its critical components. (S)

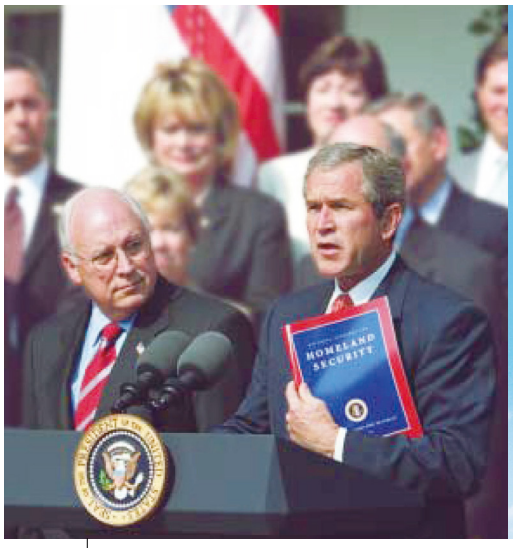
-- As outlined in Executive Order 12656, every department and agency will be able to rapidly and effectively transition

~~SECRET~~ SECRET

柯林頓總統第 62 號決策指令明示國家面臨包括「網路恐怖主義」的非傳統安全威脅。（Source: Homeland Security Digital Library, https://www.hsdl.org/?abstract&did=758094）

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、政府運作功能等為關鍵性的國家基礎建設。並集合政府與民間產業界，共同成立了直屬總統的「國家關鍵基礎建設防護委員會」（President's Commission on Critical Infrastructure Protection），來推動與關鍵基礎建設有關的國家政策。

1998 年 5 月，柯林頓總統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安全威脅之能力；第一項政策指令為「總統第 62 號決策指令」（Presidential Decision Directive 62）：明示了國家面臨的非傳統安全威脅，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；第二項政策指令為「總統第 63 號決策指令」（Presidential Decision Directive 63）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。準此，「國家基礎建設防護中心」（National Infrastructure Protection Center）遂成為政府整體防護架構的一部分，擔任針對關鍵基礎建設威脅的評估、警告、調查，以及對攻擊反應的主導角色。




小布希總統公布的「國家關鍵基礎建設與重要資產實體防護策略」將國家紀念建築物與肖像、核能電廠、水壩、政府設施及商業重要地點等列為應予以防護的重要資產。（Source: Homeland Security Digital Library, https://www.hsdl.org/?abstract&did=1041）

二、小布希時期

2001 年 10 月小布希總統簽署第 13231 號「資訊時代的關鍵基礎建設防護」（Critical Infrastructure Protection in the Information Age）行政命令，聯邦政府據以成立「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，並將通信資訊安全與關鍵基礎建設相結合。

2003 年 2 月，小布希總統又公布「國家關鍵基礎建設與重要資產實體防護策略」（The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets），作為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、政府設施及商業重要地點（如商業中心、辦公大樓、運動場、主題樂園等）列為重要資產應予以防護；另依據國土安全第 7 號總統令（Hspd-7）—「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為，以有效地運用聯邦經費與資源消弭弱點、嚇阻威脅與減低遭受攻擊或意外事件的後果。該命令為聯邦部門和機構制定了一項國家政策，以確定和釐清美國的關鍵基礎設施和關鍵資源，並保護它們免受恐怖襲擊。

2013 年，美國的國土安全部修訂及更新「國家關鍵基礎設施防護計畫」（National Infrastructural Protection Plan, NIPP），

提出以「安全（Security）與韌性（Resilience）」作為推動國家關鍵基礎設施防護計畫（NIPP）的目標。其中「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，以及具備在中斷後能快速恢復的能力」。

三、歐巴馬時期

歐巴馬總統於 2013 年簽署的 PPD-21 號總統政策令與第 13636 號總統執行令（Executive Order, EO），其與美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）的標準，均有一共同的宗旨與職責，即為協同執行美國關鍵基礎建設、資訊等項目之保護工作；另外，美國政府亦於 NIPP 2013 中訂定有關關鍵基礎設施之安全組織架構、項目規劃分析及 NIPP 2013 國內公、私部門之合作架構圖。

四、川普時期

2017 年 1 月，美國川普總統上任之後，公布「強化聯邦網路與重大關鍵基礎設施網路安全」之總統執行命令（Presidential Executive Order: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure），要求各聯邦機關首長應

NIPP 2013 強調跨部門合作的優勢。（Source: Federal Emergency Management Agency, https://training.fema.gov/hiedu/14conf/presentations/thur_kolasky_nipp2013.pptx）

執行改善關鍵基礎設施網路安全之框架，管理該聯邦機構所遇到的網路安全風險。

美國近期重大駭客攻擊事件

自拜登總統上臺後，美國政府各重要部門即連續發生網路安全事件及遭受新型態的駭客攻擊，對國計民生造成莫大的衝擊，例如總部設於德州的 SolarWinds 公司（為專門研發系統／網路／基礎設施管理軟體的業者），根據美國白宮前國安顧問佛林（Michael Flynn）的說法，該公司之客戶涵蓋美國國務院、國家安全局、司法部及總統辦公室外，亦為美國整個關鍵基礎設施的入口，2020 年 3 月美國財政部與商務部遭駭客利用 SolarWinds Orion 的安全漏洞滲透到組織的內部網路，並藏匿於受害者的系統長達數月之久。2020 年 5 月駭客組織利用 DopplePaymer 勒索軟體成功入侵 NASA 之資訊外包商，及美國能源部和國防部的合作廠商 DMI 公司的系統，取得 NASA 的人事檔案，且公開數個壓縮檔並貼出於暗網。2021 年 2 月佛羅里達州淨水處理廠遭駭險被水中下毒事件，發現廠方外包業者的網站去年底即被植入惡意程式，被駭客用來竊取佛州當地政府單位以及民間水利公司資料。2021 年 3 月初爆發的 Exchange Server 攻擊行動導致大量受害者，包括州政府及公家機關均發現駭客入侵證據，其目的在竊取私密郵件，3 月底美聯社（AP）報導：駭客已取得屬於川普政府國土安全部負責人 Chad Wolf 的電子郵件帳戶，以及該部門網路安全人員的電子郵件帳戶。此外，近期勒索病毒攻擊造成負責美國東岸近半數油管運輸的 Colonial Pipeline 公司主動關閉營運；2021 年 5 月，駭客攻擊全球最大肉品供應商（JBS），此為第一件大宗商品成為駭客下手的目標，致使其北美和澳洲的電腦網路關閉，並導致客戶及供應商的部分交易延遲。

拜登政府的規劃：強化國家網路安全防禦及保護聯邦政府網路

為解決此類的問題，拜登總統於今年 5 月簽署發布，其主軸為要求改善國家的網路安全並保護聯邦政府網路，同時，提醒人們美國公共和私營部門最近所發生的網路安全事件，越來越多來自於極端民族主義者和網路犯罪分子。這些事件具有之共通性，為網路安全防禦不足，使公私部門更容易受到事件影響。

Colonial Pipeline 事件亦讓美國政府了解，僅靠聯邦行動是不夠的，尤其美國國內的大部分關鍵基礎設施係由私營部門擁有和營運，這些私營部門對網路安全的投資均由各公司自行決定。因此美國政府認為需要鼓勵私營部門跟隨聯邦政府的腳步，採取較積極的措施來增加和調整網路安全投資。

Colonial Pipeline 為美國最大的油管供應商，該公司在遭到勒索病毒後主動關閉營運，導致美國東岸民眾大排長龍加油。（Photo Credit: Mark Mathosian, https://flickr.com/photos/markgregory/51175339315；美聯社／達志影像）

綜而言之，拜登總統此次簽署的行政命令包括下揭主要事項：

一、政策

美國面臨持續且日益複雜的惡意網路活動，除威脅到公私部門，最終更威脅到國民的安全和隱私。政府必須加強努力，以識別、威懾、防範、發現和因應這些行動和行為者。政府更須仔細檢查任何重大網路事件中發生的情況並吸取經驗教訓。

漸進式改進不會帶來安全性；相反，政府需要做出大膽的改變和重大投資，以保護支撐美國人民生活的重要機構。這些機構的資訊系統，無論它們是基於雲端、本地端或是混合環境的系統，政府均須充分利用其公權力和資源來保護。而保護的範圍必須包括處理數據的資訊系統（資訊技術— IT）和執行確保安全的重要機器系統（營運技術— OT）。

2021 年 5 月，駭客攻擊全球最大肉品供應商（JBS），此為第一件大宗商品成為駭客下手的目標，導致供應商部分交易延遲。

總之，政府的主要政策是指對網路事件（Incident）的預防、檢測、評估和復原。政府必須以身作則，所有政府資訊系統都應滿足或超過本指令規定和發布的網路安全標準和要求。

二、 消除公私部門之間共享威脅情資的障礙

確保 IT 服務供應商能夠與政府共享威脅情資，並要求供應商分享某些不願公開或系統安全漏洞的情資。由於合約的規定，IT 供應商常常猶豫或非自願共享此等訊息；也有一種情況是供應商可能只是不願分享有關自身安全漏洞的情資。因此，政府必須消除任何合約障礙並要求供應商分享可能造成政府網路資訊外洩的情資。

三、 聯邦政府精確落實更現代化的網路安全標準

過時的安全模型和未加密的數據將導致公私部門的系統受到損害。政府必須帶頭並增加對安全最佳實務的採用，諸如採用零信任安全模型、加速移動到安全雲服務以及持續建置多因子身分驗證和加密等基礎安全工具。

四、 強化軟體供應鏈安全性

政府須建立一套軟體開發之安全標準，以提高軟體的安全性，包括要求開發人員保持對其軟體更高的可見度和公開安全數據。它建立了一個並行（Concurrent）的公私部門合作營運計畫（流程），研發新的創新方法來保護軟體開發，並利用聯邦採購的力量來推動。例如創建「能源之星」[1] 類型的標籤，以便政府以及廣大群眾可以快速確定軟體開發是否安全。

五、 建立網路安全審查委員會

因應本項要求，將成立由政府和私營部門共同主持的網路安全審查委員會，可能會在發生重大網路事件後召開會議，分析發生的事件並提出具體建議以改善網路安全。一直以來，組織經常重複過去的錯誤，並無從重大網路事件中吸取教訓。因此，當發生問題時，政府和私營部門需要面對問題並進行必要的改進。

六、 建立網路弱點事件之緊急應變的標準手冊

組織不能等到他們受到威脅才思考如何因應攻擊。由最近的事件顯示，政府內部緊急應變計畫的成熟度差異很大。該手冊將確保所有聯邦機構達到一定的門檻，並準備採取統一措施來識別和減輕威脅，此外亦可為私營部門提供標準作業程序（SOP）。

[1] 提高能源效率的計畫。該計畫使用不同的標準化方法提供有關產品和設備能耗的訊息。

七、強化聯邦政府網路安全弱點及事件的檢測

本項要求藉由啟用政府網路上的端點檢測和應變系統以及改進聯邦政府內部的資訊共享，將可提高檢測聯邦網路上惡意活動的能力。組織對於基礎網路安全工具及作業實務的建置，若採取懈怠與不一致的態度，將給予敵人可趁之機。政府應在網路安全檢測方面作為領導者，進行完整的政府網路端點檢測和響應（EDR）部署，而精準且完整的政府內部情資共享將扮演重要的角色。

八、強化聯邦政府的調查和復原能力

本項要求為聯邦部門和機構制定了網路安全事件日誌要求。日誌記錄的精準與否將影響組織對於檢測入侵以及事後確定事件程度的能力。穩健且一致的日誌記錄將可解決大部分問題。

結論

經過 25 年的研析及 8 屆政府的努力，美國政府對關鍵基礎設施防護的戰略思維已與資訊科技的發展同步精進與成熟，「他山之石，可以攻錯」，美國所走過的路，應可供我們借鏡。

參考資料 1. 黃俊泰。美國關鍵基礎設施威脅資訊分享框架簡介。
2. 李中生。「國家關鍵基礎設施防護」的思維工作面向。
3. 陳佩修。九一一事件後美國國土安全任務與反恐聯盟建構：兼論對東南亞安全情勢的影響。
4. 莫大華。增進關鍵基礎建設防護機制，強化國土安全。