關鍵基礎設施防護之實踐與問題

■中央警察大學恐怖主義研究中心主任　汪毓瑋

實踐關鍵基礎施防護，必須以「全災害途徑」去進行設計，換言之，必須經由分而合之的執行「預防」、「保護」、「準備」、「回應」與「復原」工作，且透過與時俱進之「情節想定」去「演練」與「演習」，以檢證「核心能力」而促使變時之「核心功能」仍能夠保持基本運作以持續營運，而最終期盼達成處理全範圍的威脅與危害之「目的」。

關鍵基礎設施之準備與保護的最佳實踐

準備與保護的最佳實踐涉及了五個層面之反復實踐的檢討過程，分別是「關鍵基礎設施資訊」之保護與分享；強調更早階段行動且必須展現出「主動」之「關鍵基礎設施準備」；決定與排列出應該被保護之「關鍵基礎設施功能」;從建構脈絡中思考比較上展現出「被動」之個別的「關鍵基礎設施保護」；並進而期盼達成更高層面之聚焦於「面」之「關鍵基礎設施確保」，此等層面之重要的核心工作內容，簡述如下：

一、*關鍵基礎設施資訊*

1. 敏感但卻非機密性的類別。
2. 資訊擁有者採取合理的與需要的步驟去保護。
3. 在定義與分類上不應該妨礙必要分享原則。

二、*關鍵基礎設施準備*

1. 預防、回應及從重大事件中恢復。
2. 針對自然與人為脈絡下之威脅、風險或是弱點之嚴重與危險層級。
3. 早期階段行動，以減少威脅的可能性與結果或真實的攻擊。

三、*關鍵基礎設施功能*

1. 定義、使用與維持重大關鍵基礎設施的一個過程。
2. 決定可能的需要。

3. 應該使用何種方法。
4. 哪些應該被保護（賴以生存、持續營運及其成功最終依賴的）。

四、關鍵基礎設施保護

1. 非常「地方性」與基礎的層面。
2. 聚焦於「點」。
3. 思考取代性方法。
4. 保護重大關鍵基礎設施之實體與建構脈絡。

五、關鍵基礎設施確保

1. 聚焦於提供獨特服務的環境。
2. 進行額外層級的保護。
3. 系統角度之「殘餘風險」的單點故障，例如不只電廠而是電力網。

風險分析的基礎

準備與保護實踐之方法論，就是風險分析與風險評估。有「資產」就會有風險，從國家層面言，任何被評定為國家「重大關鍵基礎設施」者，就必然存有來自於自然、人為與網路上的風險。且任何的「準備」之首要工作，均是來自於「恰到好處」之分析風險。而風險就是由「威脅」、「弱點」與「可能性」加乘之結果，簡述如下：

一、***威脅：***聚焦於「企圖」與「能力」；必須評估動機的程度、執行能力，以及可以使用的資源。

二、***弱點：***關注的是單一或系統的脆弱性、可進入性、監視機會、固有的弱點（結構性）、可以消解的反制措施。

三、***可能性：***必須從後果與重要性兩個層面去思考，進而可以排比出優先次序：

1. 在後果層面之思考，包括了攸關組織任務之重要資產；恢復營運之難以取代資產；及損失結果，其中衡量之指標計有人、財產、專屬資訊、聲譽及營運生產力等五項。

2. 在重要性層面之思考，包括了六個層面之細緻化評估，分別是對於每日運作是絕對重要的；非常重要，運作可以持續數日；重要，運作可以在減少能量下持續；有些重要，運作將會有嚴重衝擊;不重要,有助於運作;對於任務絕對不重要。

風險評估的步驟

基於前述之風險分析基礎，在具體操作層面上，就必須從資產特徵、威脅鑑定、重要性分析、後果分析、弱點分析、可能性評估等六大層面進行評估，簡述如下：

一、***資產特徵：***營運功能、環境、建築物及周邊類型、人口、進入／撤出等。

二、***威脅鑑定：***能夠瞭解與描述威脅、選擇威脅層級，進而擬出適當的安全計畫。

三、***重要性分析：***與組織任務有關的資產，必須能夠瞭解、描述，及定義出重要性層級。

四、***後果分析：***從精確的角度，決定出與組織任務有關資產損失後之結果層級，包括了傷亡、產品或營運功能、專屬資訊、聲譽等。

五、***弱點分析：***瞭解與展現出組織資產的弱點，掌握可能被那一種方法及武器攻擊，以及攻擊的「可能情節」。

六、***可能性評估：***威脅者如何看待組織的資產、哪些資產最有被利用的可能性。

在實踐上必須正視之問題

一、「混合性威脅」之發展？

二、科技進步之「震驚性」攻擊—針對實體與虛擬空間？

三、法律之依據與多樣化，所引發之權責釐清及不同部門實踐認知的差異？

四、「國土安全」範疇下之關鍵基礎設施防護之真實意涵？

五、有關名詞定義之不明確，以及真實內容認知之差異？

六、「具體化」到什麼程度才是恰到好處？此涉及到「國家關鍵基礎設施確保」之達成。

七、「削足適履」地填寫各項表格，抑或是原則性的統一規範才是「最佳實踐」嗎？

八、如何恰到好處地將資源不同、類別不同的關鍵基礎設施框在同一個架構下？

九、在多樣化公私部門重大關鍵基礎設施之「共性」要求下之「殊性」如何保留？

十、量化之科學化統計數字與圖示，或計較自我評估之威脅等級，真的可以明確地回應「非理性」、「自我調適」的攻擊者，以及不能「完全預測」的自然災害嗎？

結論

一、威脅才是王道，但是真的瞭解與掌握與時俱進的「威脅動變」嗎？

二、要有「全災害」之準備，但真的瞭解自然災害與人為災難的性質不同嗎？雖然最終破壞之結果類似但程度肯定不同，更何況是兩類受災前之「準備」工作重點截然不同。

三、回應行動是基於「分級回應」之原則，強調對於意外事件的回應，必須從最低層級管轄權的地方做起，因為大部分的意外事件均是地方性的管理。但是地方政府及在地之關鍵基礎設施管理部門真的有此體認嗎？

四、如何平衡「案例導向」之思維？

五、國安與行政體系之攸關國家重大關鍵基礎設施之資訊分享真的有到位嗎？

六、如何引導技術人才之「專業」點，擴展到「安全」面之一專多能？

七、基於「威脅鑑定」與「弱點評估」兩大主軸之準備，複雜度與困難為何？

八、「縱向到底，橫向到邊」之因應，必須解決哪些困難？

九、「承受風險」之概念如何貫穿到整個防護作為？

十、若沒有整全的知識範疇，只是看到了某個「點」，是否真的就能夠應對？

十一、若沒有明確的政策，則末端的法律擬定，就找不到依據的源頭，空了一塊，實踐時可能沒有問題嗎？

十二、「客製化」的因應關鍵基礎設施防護之具體需求，是否更能符合成本效益及現實考量？

十三、演練與演習可能涉及公私部門之多樣領域與多個管轄權的異常事件，故若想評估效果及澄清部門與人員之角色與責任，情節規畫應「從嚴」與「從難」，而不僅是已有運作程序之回推情節設計。換言之，如何可以漸進式地進行專業設計，從「似真」發展到「逼真」再演化到「超真」？

十四、「先求有，再求好」真的是一個好的解決問題之哲學思考嗎？

由於國家關鍵基礎設施之防護作為事涉每位民眾的安危，故整編上述論點，盼每位愛臺灣的人能深思！

（本文轉載自法務部清流雙月刊 107 年 9 月號）