關鍵基礎建設防護之模擬

Simulation of Critical Infrastructure Protection

黃士育[1]　范金鳳[1]　易俗[2]
[1]元智大學資訊工程系
[2]清雲大學資訊工程系
[1]csfanc@saturn.yzu.edu.tw; [2]swuyih@cyu.edu.tw

中文摘要

為了評估關鍵基礎建設保護(Critical Infrastructure Protection, CIP) 的效能，各國均發展相關的模擬工具。本文首先提出影響關鍵基礎建設保護效能的因素和因素間的關係 ，並根據這些因素及關係，模擬基礎建設受攻擊後所引起的後續影響。此模擬可了解基礎建設的相互相依關係(interdependencies)、可產生各種攻擊劇情以回答萬一如何(what-if)的問題、也可辨認關鍵基礎建設保護的弱點。

關鍵字：關鍵基礎建設保護、相互相依關係、貝式信心網路、模擬。

Abstract

In order to evaluate the effectiveness of Critical Infrastructure Protection (CIP) measures, many countries are engaged in developing related simulators. This paper first discusses the factors affecting CIP effectiveness and the relationships among these factors. Based on these factors and relationships, a simulation tool has been constructed to investigate the effects of interdependencies, to answer what-if questions, and to identify potential vulnerabilities of CIP.

Keywords: Critical Infrastructure Protection (CIP), interdependencies, Bayesian Belief Network (BBN), Simulation.

一、緒論

在 911 之後，人們注意到關鍵基礎建設保護措施 (Critical Infrastructure Protection, CIP)隱藏的脆弱性及相關保護措施的重要性。關鍵基礎建設指的是民生需求所仰賴度的電力、交通、用水、通訊等領域。各項關鍵基礎建設現今皆應用到電腦或連接上網路，故 CIP 的重點為 CIIP 關鍵資訊基礎建設保護(Critical Information Infrastructure Protection, CIIP)。近幾年內各國無不開始檢驗其基礎建設之間的防護措施，發展更完整的保護計畫以因應未來的挑戰。

在基礎建設中最重要的議題是基礎建設之間的相互相依關係或關聯關係(Interdependencies)。因為基礎建設現今皆應用到電腦、網路，關鍵基礎建設之間的相互相依關係密切，牽一髮動全身。國外針對基礎建設的相互相依關係，已經有相當多的研究[5-8]，反觀國內目前尚無針對此議題作深入探討的報告。

本研究方法主要探討影響關鍵基礎建設保護效能的因素和關係，並發展了一套具有多點攻擊的模擬評估工具，分析關鍵資訊基礎建設的相互相依關係影響。

二、背景

以下將介紹美國國家基礎建設保護計畫(NIPP)、國際關鍵資訊基礎建設保護手冊(CIIP Handbook)、貝式信心網路(BBN)、基礎建設的相互相依性(interdependencies)等相關背景。

2.1 美國國家基礎建設保護計畫 (National Infrastructure Protection Plan, NIPP)

美國國家基礎建設保護計畫(NIPP)[11,12]為美國執行基礎建設保護的依據，目的為降低威脅之風險。其核心部分為風險管理架構(Risk Management Framework)，該架構包含六個工作步驟，分別為制訂安全目標(Set Security Goals)、辨識重要資產(Identify Assets)、評估風險(Assess Risk)、優先排序(Prioritize)、執行保護計畫(Implement Projects Program)和量測成效(Measure Effectiveness)。在其風險管理架構中強調相互相依關係的重要性。美國為資訊領域之強國，該國之保護計畫極具有參考價值。

2.2 國際關鍵資訊基礎建設保護手冊 (CIIP Handbook)

國際關鍵資訊基礎建設保護手冊(CIIP Handbook[9,10])對關鍵基礎建設資訊系統保護的主要議題提供整體性與國際性概觀(overview)。於2002、2004、2006年先後發表了三個版本。2006年版介紹20個國家的資訊基礎建設保護措施計畫。該手冊之資料豐富，為討論關鍵基礎建設保護措施相關議題的重要指引以及參考資料來源。

2.3 貝式信心網路 (Bayesian Belief Network, BBN)

貝式信心網路(Bayesian Belief Network, BBN)[3]為一種有向的非循環圖形(Directed acyclic graph)。主要由兩個部分所組成，包含了節點(nodes)與連結線(arcs)，並結合了一組狀態機率表(Condition Probability Tables) 表達節點間的條件機率。

本研究用 BBN 來表示影響基礎建設相互相依關係的因果關係。我們首先將影響基礎建設關聯性的重要因素辨識出來，然後再利用 BBN 來表示這些重要因素之間的因果關係；而每個重要因素都有其機率，都會影響到成功防禦的機率。

2.4 關鍵基礎建設的相互相依性塑模(Modeling) 及模擬(Simulators)

現今的基礎建設架構下，很少有基礎建設是完全獨立、不受其他建設影響的。不論是直接的影響、間接的影響、或是政策上、地理上的影響，多數的基礎建設已經無法與其它的基礎建設有所分割。

關鍵基礎建設單點攻擊的模擬已有數個常用的模型及工具，例如 SAVI， EASI [1,2,4]等。至於多點攻擊及基礎建設相互相依性的塑模和模擬，許多國家皆在進行中，例如 Pederson 在 Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research 一文中提到的眾多模擬基礎建設相互相依關係的計畫和案例[5]。但是模擬背後的影響因素和應用公式，在我們開始做此研究時卻不多見，可能這些模擬研究皆正進行中，且與具有區域性等因素有關。最新的文獻中已開始見到一些相互相依性模擬相關公式，例如義大利的經濟效益公式[8]。

2.5 相互相依關係(interdependencies)

現行基礎建設多數連結網路，其中任一節點的問題，均會影響網路上其他的部分，所以關鍵基礎建設保護中的相互相依性關係相當重要。

2001 年 Rinaldi 等人提出以六個維度(Dimensions)探討相互相依關係的概念。他們將相互相依關係以六個維度予以辨識、了解及分析。此六維度為環境、相互相依關係的類型、操作的狀態、基礎建設特性、錯誤的類型、耦合度和反應的行為。六維度間彼此涵蓋及影響，為迄今較能完整分析相互相依關係的方法。

三、研究方法

我們的研究方法主要是模擬在多點攻擊下，關鍵(資訊)基礎建設保護(Critical (Information) Infrastructure Protection, CIP/CIIP)活動的效應及相互相依關係的影響。

3.1 建立模擬相關因素的因果關係

首先，我們推論影響成功防禦(successful defence)的主要因素如圖 1 所示。因素包括：

1. 此部門 CIIP 的防禦措施等級(CIIP level)
2. 此基礎建設的防禦等級(defence level)
3. 此基礎建設的恢復力(recoverability)
4. 民眾的容忍度/信心(tolerance)

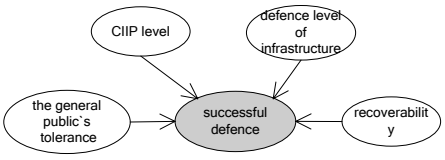

圖1 影響模擬因素的因果關係圖

至於關鍵資訊基礎建設保護措施的等級(CIIP level)，假設等級分為五級(1~5)，我們有另文說明其可能的評估方法[13]。至於其他三個因素，我們則利用 BBN 來建立其細部相關因素的因果關係。BBN 可表達並量化因素之間的相互相依關係(或關聯關係)。

就人民信心程度(tolerance) 而言，若民眾的信心夠強，忍受時間會比較長，則成功防禦攻擊的機率則會加大。眾多因素影響到人民信心的程度，包含實際上的考量(practical concern)以及 CIIP 的保護活動(如圖 2 所示)。而 CIIP 保護活動主要為風險管理(risk management)。而風險管理的效益又受到計劃(plan)、定義資產(identify assets)、評估風險(assess risk)、資訊分享(information-sharing)以及訓練(training)等因素的影響 (見美國國家基礎建設保護計畫 NIPP 的活動項目[11-12])。實際考量(practical concern)部分則受到替代方案(alternative)及復原力(recovery)兩項因素所影響。因此，我們可以利用 BBN 將這樣的影響關係呈現出來，其圖形如圖 2 所示。

就恢復力(recoverability)而言，恢復力會受到基礎建設特性(infrastructure property)、攻擊者特性(attacker property)以及 CIIP 的保護活動等因素的影響(如圖 3 所示)。其中 CIIP 保護活動的影響因素同上。基礎建設特性(infrastructure property)則受到相互相依性(interdependence)、技術相關的硬體備份(duplicates)、或軟體多個版本(N-version)等因素影響。而攻擊者特性(attacker property)則包含眾多因素，如攻擊的類型(attack type)、攻擊的特性(attack property)、及破壞程度(destructiveness)等。而其中的攻擊的類型(attack type)又分為三

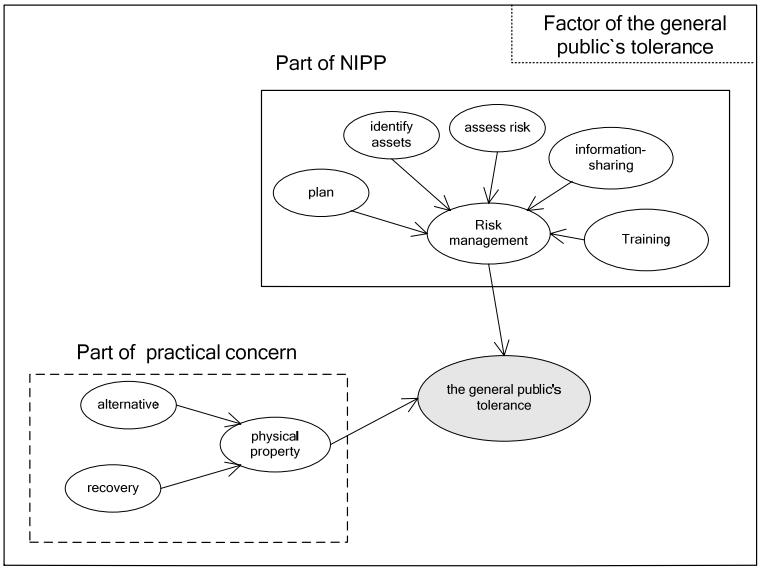

圖 2　人民信心程度的因果關係圖

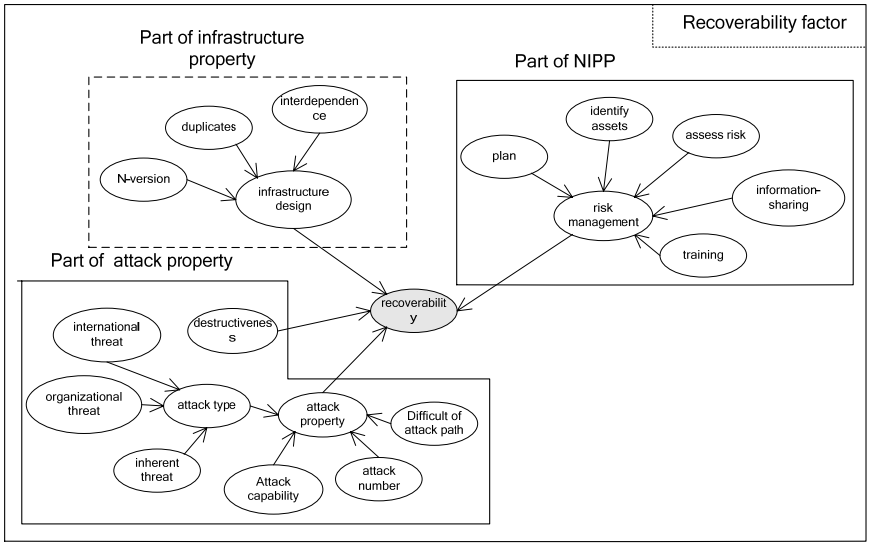

圖 3　恢復力的因果關係圖

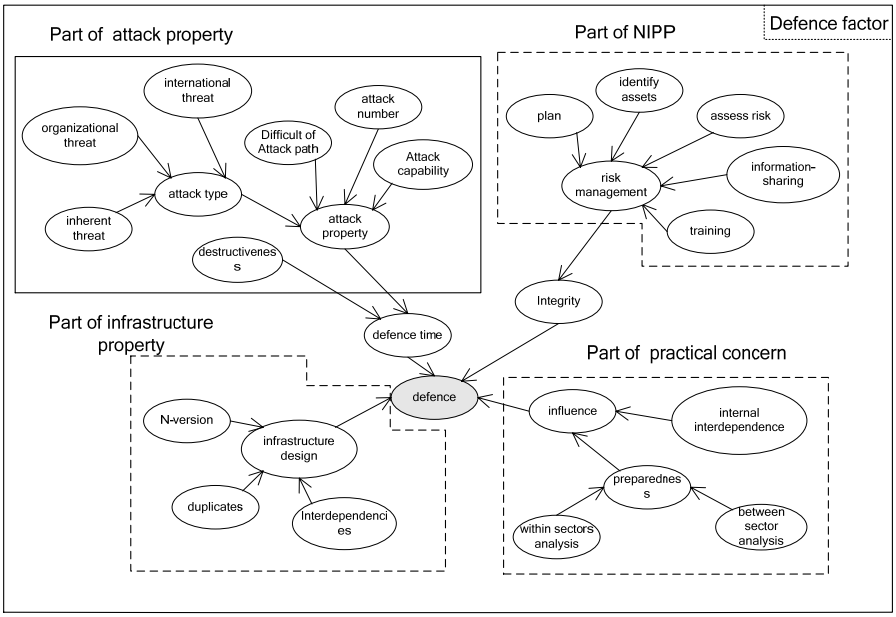

圖 4　防禦力的因果關係圖

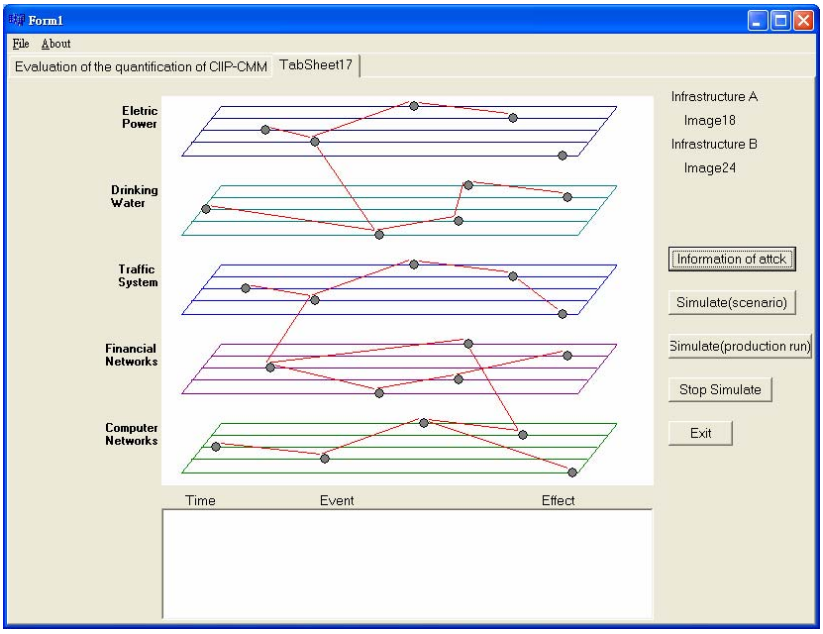

圖5　模擬工具

個因素，有國際間的威脅(international threat)、組織間的威脅(organizational threat)，和內部的威脅(inherent threat)。攻擊的特性(attack property)則是受到攻擊路徑(attack path)、攻擊者數目(attack number)、攻擊時間(attack time)等三個因素所影響。因此，我們可以利用 BBN 的方式將這樣的影響關係呈現出來，其圖形如圖 3 所示。

最後，影響基礎建設最重要因素就是防禦力(defence level) (見圖 4)。防禦力會受到基礎建設特性(infrastructure property)、實際考量 (practical concern)、攻擊者特性(attacker property)以及 CIIP 的保護活動等級等因素的影響。這些因素的細節如上所述。

這些細部因素可在模擬之前以 Hugin 工具(www.hugin.com)先行計算。以下的模擬僅用到其結果，即圖 1 所示的影響成功防禦的主要因素 (即防禦力等級、人民信心、CIIP 等級、以及恢復力等級)。

3.2.2 模擬基礎建設相互相依性的方法及工具

如上所述基礎建設相互相依性模擬公式在文獻中不多見。我們自行發展了相關的關係式。在基礎建設遭攻擊時，需要模擬的效果不外乎下面幾項：

(1) 防禦力的變化(defence(t))：我們將復原力亦納入考慮。

(2) 其他建設波及受影響的傳遞時間(cascading time)。

(3) 其他建設影響的效果(cascading effect)。

我們發展了一套用來模擬關鍵基礎建設關聯性的工具，此工具產生潛在的攻擊劇情來判斷保護措施的弱點。輸入則使用上述 BBN 圖的結果，即防禦力、恢復力、人民信心，及 CIIP 措施等級。我們的個案假設有五層不同的基礎建設，即水力、電力、交通、金融和網路，如圖 5 及表 1 所示。使用者需先輸入基本的攻擊資訊，包含了敵人數目、攻擊裝備、攻擊武器、是否有計畫以及訓練程度。這些資訊在此皆等級化(1~5)，如表 2 所示。

表1　基礎建設特性表

層級	防禦力	恢復力	人民信心程度	CIIP 保護計畫
水	極高、高、中等、低、極低	極高、高、中等、低、極低	極高、高、中等、低、極低	1~5
電力				
交通				
金融				
網路				

表 2　攻擊參數表

攻擊項目	參數(量化等級)				
	1	2	3	4	5
敵人數目	1 人以下	10 人以下	100 人以下	1000 人以下	1 萬人以上
攻擊裝備	徒步	戰車	戰鬥機	潛艦	航空母艦
攻擊武器	刀	手槍	步槍	火箭筒	手榴彈
是否有計畫	毫無規劃	稍微計畫	詳細規劃	基本戰術	高階戰術
訓練程度	烏合之眾	稍微訓練	嚴格訓練	菁英部隊	特種部隊

攻擊力(attack)的計算會需要考慮到以上五個項目，而每個項目皆量化成五個等級，分別乘上一個權重(weight)而得到，其公式如下：

$$attack = (w_1 * number\ of\ \text{attckers}) + (w_2 * level\ of\ strength\ of\ equipment) + (w_3 * level\ of\ strength\ of\ weapon) + (w_4 * level\ of\ strength\ of\ plan) + (w_5 * level\ of\ strength\ of\ discipline)$$

其中w1, w2, w3, w4,w5為使用者自行給予之權重值，預設值為1。

上述的公式中，每一攻擊項目的等級皆為1~5，總共有五項攻擊項目，故以加總的方式計算，攻擊力的範圍會介於 5~25 之間。為了方便與防禦力能夠相互比較，故我們會將攻擊力所得到的數值乘上 4，將攻擊力的範圍界定於 20~100 之間。

在防禦力變化(defence(t))上，我們會根據攻擊方的攻擊力(attack)與防禦力(defence)的差距而有所不同。當防禦力遠大於攻擊力時 (例如防禦力的值大於攻擊力的值 40 以上)，下一刻防禦力不變。當防禦力大於攻擊力(例如若介於 0~40)，而下一刻防禦力剩下使用者設定的部份(D1)；我們並將恢復力列入考量。當防禦力小於攻擊力(例如其若介於 0 ~ -40)，下一刻防禦力剩下使用者設定的部份(D2)；另要考慮到恢復力和人民信心程度。當防禦力遠小於攻擊力時(例如若小於-40)，基礎建設則是遭受到完全的破壞，下一刻防禦力降為 0。以上 4 狀況公式如下：

$$defence(t+1) = \begin{cases} defence(t) & if\ \ defence >> attack \quad (1) \\ defence(t) * D_1 & if\ \ defence > attack \quad (2) \\ defence(t+\Delta t) * D_2 & if\ \ defence < attack \quad (3) \\ 0 & if\ \ defence << attack \quad (4) \end{cases}$$

狀況(2)中，我們亦考慮到恢復力，即攻擊力逐步復原至某一程度，例如會隨著 4 個時間單位而增加 1%，維持四個週期才停止，則公式如下：

$$defence\ (t+4) = defence\ (t) * (1+1\%)$$

恢復力增加以每 4個時間單位為一週期

再者，狀況(3) 中，我們考慮恢復力及人民信心程度，逐步復原的間隔則由人民信心決定，當民眾的信心程度越低，所需要的恢復時間越長，反之越短。其範例公式如下所示：

$$defence(t+\Delta t) = defence(t) * (1+1\%)$$

Δt代表防禦力恢復的時間間格

人民信心程度的等級分為極高、高、中等、低、極低，所以△t 是將人民的信心程度的等級做一個量化後所對應的時間間隔 (例如：依照人民信心程度的等級由極高至極低，其分別對應的時間間隔是 2, 4, 6, 8, 10 個時間單位)。

換言之，上述四狀況為：

(1) 可接受範圍，可立即恢復

(2) 少部分受到影響，需短時間才能恢復

(3) 大部分都遭到破壞，需長時間才能恢復

(4) 遭到永久性破壞，而無法復原

至於基礎建設之間彼此的相依性，我們則參考 Rinaldi [6] 的相互相依類型(type of interdependency)來界定，包含了實體的(physical)、地理上的(geographic)、邏輯上的(logical)以及網路上的(cyber)。此外，我們加上了必要的(essential)這個類別，如下表 3 所示。

表 3 基礎建設相依特性表

	電力	水力	網路	交通	金融
電力	essential	essential	essential	essential	essential
水力		essential	geographic	geographic	geographic
網路			cyber	cyber	cyber
交通				physical	cyber
金融					physical

至於其他基礎建設受到波及影響的時間(cascading time)，則會根據以上所述的基礎建設之間的相依性不同而有所不一樣。例如基礎建設之間的連結是地理上的(geographic)，受到影響的時間則會是隨距離增加(距離可等級化為n)。若基礎建設之間的連結是實體的(physical)、網路上的(cyber)或必要的(essential)的話，受到影響的時間則是下一個的時間單位。公式如下所示：

$$\text{傳遞的時間} = \begin{cases} T+1 & if\ link = physical \\ T+n & if\ link = geographic \\ T+1 & if\ link = cyber \\ T+1 & if\ link = essential \end{cases}$$

至於其他建設受影響的程度(cascading effect)，則可以以防禦力降低的等比率方式計算。例如其中基礎建設 B 受 a 與 b 兩個基礎建設的影響，所以 B 防禦力的降低率為，

B防禦力的降低率 =
(a防禦力的降低率 * $\frac{1}{2}$) + (b防禦力的降低率 * $\frac{1}{2}$)

四、 模擬案例

4.1 特定劇情模擬

本工具提供特定劇情模擬及自動模擬模式。以下為一實驗案例，基礎建設的節點及其相關聯性可在圖上點選、拉線。防禦力、恢復力以及人民信心程度的等級皆以極高、高、中等、低、極低為分類。而 CIIP 保護計畫則是讓

使用者去評估基礎建設的保護計畫是否完善，而其等級分為 1~5 級。此外，使用者由表單點選輸入相關資訊如表 4、5、6 所示。圖 6 為執行結果，隨時間變化的劇情在圖下方顯示。上面為節點最終的狀況。

表 4　個案輸入--民生基礎建設防禦能力的設定

層級	關鍵基礎建設名稱	防禦力	恢復力	人民信心程度	NIPP 保護計畫
水	水庫 A	極高	低	中等	5
	水庫 B	中等	極高	低	3
	水庫 C	高	中等	極高	4
電力	發電廠 A	低	低	中等	5
	發電廠 B	極低	中等	中等	4
	發電廠 C	高	極高	極低	4
	發電廠 D	低	中等	高	5
交通	國道 A	極低	極高	低	3
	高速公路 A	低	高	極高	3
	鐵路 A	高	極高	低	2
	國道 B	極低	極高	中等	4
金融	銀行 A	極高	高	低	3
	證券期貨局 A	低	中等	極低	2
	股市 A	極高	低	極高	1
網路	電信 A	中等	極高	高	4
	電信 B	高	低	極低	3

表 5　個案輸入--攻擊方資訊的設定

攻擊項目	攻擊者 1	攻擊者 2	攻擊者 3	攻擊者 4
敵人數目	100 人以下	1 人以下	10 人以下	1 萬人以上
攻擊裝備	潛艦	戰車	戰鬥機	航空母艦
攻擊武器	步槍	手榴彈	手槍	火箭筒
是否有計畫	基本戰術	高階戰術	稍微計畫	詳細規劃
訓練程度	稍微訓練	嚴格訓練	嚴格訓練	菁英部隊

表 6　個案輸入--攻擊方的攻擊點和時間的設定

攻擊項目	攻擊者 1	攻擊者 2	攻擊者 3	攻擊者 4
攻擊點	國道 A	水庫 B	銀行 A	發電廠 C
攻擊時間	5 個時間單位	30 個時間單位	13 個時間單位	21 個時間單位

圖中實心圓代表正常，空心圓代表輕度受創，半空心圓代表中度受創，細叉空心圓代表重度受創，粗叉空心圓代表徹底毀壞。透過模擬工具的運算分析，我們可以觀察得知以下兩點心得。第一由圖6可以看到總共有三個基礎建設完全遭受到破壞，粗叉空心圓的這三個基礎建設並非直接遭受到攻擊者的攻擊，但是由於這三個基礎建設的防禦力、恢復力、人民信心程度以及CIIP保護活動並不完善，故當遭受到攻擊者的波及時，便很容易就導致徹底被破壞。第二，當基礎建設受到破壞時，如果基礎建設的相依性越高，則影響的層面越深，也越容易形成徹底毀壞的情況。

4.2自動模擬模式

本工具亦提供自動模式，固定各參數僅留一參數不設定，由電腦亂數產生以辨識最好及最差情境。例如，我們輸入固定基礎建設之間的連線、基礎建設資訊、攻擊參數等設定，惟獨攻擊點沒有固定，讓模擬工具去模擬出各種的狀況。最後，計讓此程式自動去執行隨機產生的 100 個案例，然後找出最好及最壞的案例出來，如圖 7 所示。

透過模擬工具的自動模式分析，我們可以得到最好與最壞的案例，好壞案例的分別在於基礎建設受損的程度。每個基礎建設都有其受損程度，我們將基礎建設受影響的程度量化成四個等級：可接受範圍、少部分受到破壞、大部分受到破壞以及嚴重損壞。當受損的基礎建設數目越嚴重，其量化成等級後的分數也越高，即代表這樣的案例是較差的案例。最後我們將每個案例裡的基礎建設受損程度作一個加總，從其案例的分數來判斷每個案例的優劣。最壞的案例中，可以看到有多個對外相依性相當高的基礎建設完全遭受到破壞，影響最嚴重的。所以，當一個基礎建設與其他基礎建設的相依性相當高，那該基礎建設的保護活動更是格外重要。

5. 結論

關鍵基礎建設保護的核心為建設間的相互相依性關係[9]。國外對相互相依性關係正進行的塑模及模擬研究眾多，國內尚無此類研究。故本研究探討在於影響關鍵基礎建設防護的因素及其關係，模擬關鍵基礎建設之間的相互相依關係。藉由模擬的方式找出基礎建設以了解各個關鍵基礎建設之間的相互關聯性及防禦力的缺失。本研究僅提供通用性的模擬雛型，考量相關的因素及關係，並容易進行彈性的細節調整。下一步將納入台灣的地理資訊系統(GIS)，以進行較完整的案例測試。

誌謝

本研究部分接受國科會編號：NSC96-2221-E-155-047 及 NSC96-NU-7-231-001 計畫經費補助。

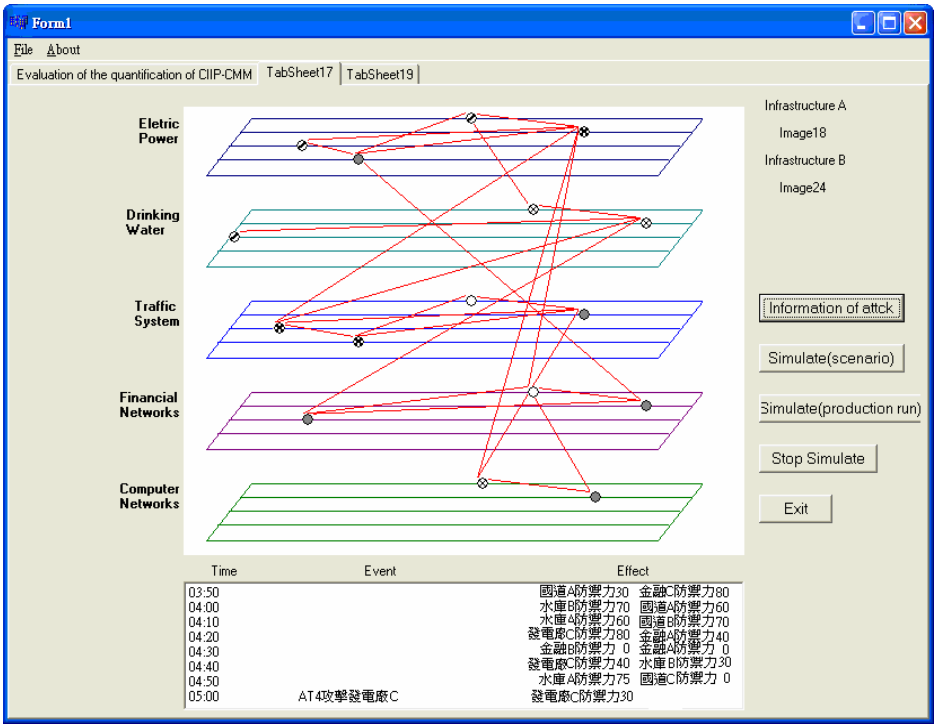

圖6　模擬劇情的量化評估工具

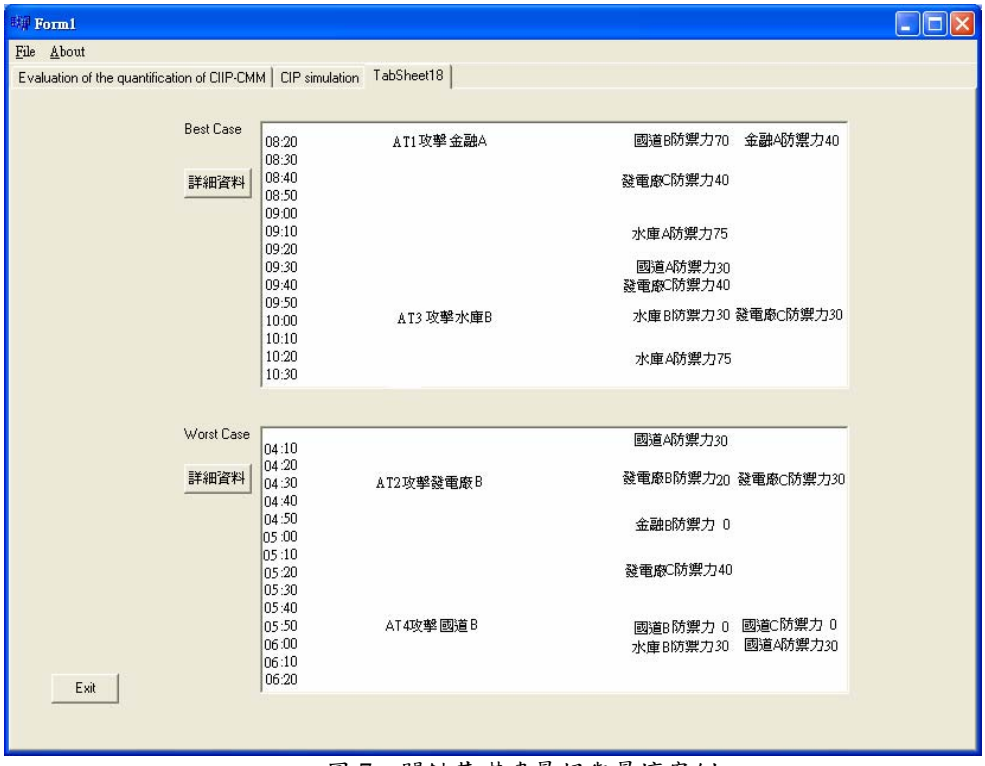

圖 7　關鍵基礎建最好與最壞案例

參考文獻

[1] H.A. Bennett, “The EASI approach to physical security evaluation,” SAND Report 760500 1977; 1-35.

[2] L.D. Chapman, and C.P. Harlan, “EASI estimate of adversary sequence interruption on an IBM PC,” SAND Report 851105 1985; 1-63.

[3] F. V. Jensen, An Introduction to Bayesian Networks, Springer, 1996.

[4] J.C. Matter, “SAVI: A PC-Based Vulnerability Assessment Program,” SAND88-1279, July 1988.

[5] P. Pederson, et al., Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Idaho National Laboratory report INL/EXT-06-11464, August 2006.

[6] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analysis Critical Infrastructure Interdependencies”, 2001 Control Systems Magazine, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

[7] S. M. Rinaldi, “Modeling and Simulating Critical Infrastructures and Their Interdependencies,” Proceedings of the 37th IEEE Hawaii International Conference on System Sciences – 2004.

[8] Roberto Setola, “Analysis of interdependencies among Italian economic sectors via Input-Output Inoperability Model,” Proceedings of the first annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Dartmouth college, New Hampshire, March 2007.

[9]Swiss Federal Institute of Technology Zurich, International CIIP Handbook 2004, http://www.isn.ethz.ch/pubs/ph/details.cfm?id=452.

[10] Swiss Federal Institute of Technology Zurich, International CIIP Handbook 2006, http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_06_Vol.1.pdf#search='CIIP%202006.

[11]U.S. Department of Homeland Security, DHS-NIPP 2005, http://www.fas.org/irp/agency/dhs/nipp110205.pdf.

[12]U.S. Department of Homeland Security, DHS-NIPP 2006, http://www.dhs.gov/interweb/assetlibrary/NIPP_Plan.pdf.

[13] 陳仲緯，”關鍵資訊基礎建設保護措施效能評估模型建立及應用，” 元智大學資訊工程系碩士論文，2006 年 7 月。

.