建置兼具國家安全與個人隱私保護的資通訊情蒐與分析系統

胡毓忠　　吳啟文

國立政治大學資訊科學系 行政院資通安全辦公室

hu at cs.nccu.edu.tw　　larry at bost.ey.gov.tw

摘要

本論文首先探討與評論現有國家資通訊情蒐與分析系統的現況。接著我們探究最新的資訊安全的研究議題，即如何以巨量資料分析的新技術應用到網路安全以找出新型的網路與系統入侵與攻擊。從犯罪防禦與偵察的觀點來看，國家關鍵資訊基礎建設防護可以充分運用巨量資料技術來進行電腦網路資料的蒐集與分析，以確保其它關鍵基礎設施的防護，落實國家安全與犯罪防制與追蹤的目的。但是從犯罪者的角度來看，他們也可以運用此技術分析資訊基礎建設防護的漏洞，並且將攻擊的行為隱藏在雲端平台上進行持久性的攻擊。我們必須要掌握如何將巨量資料分析技術應用到資訊安全的發展趨勢。最後執法人員在依法執行國家安全工作，進行網路資料的蒐集、分享、整合與分析，可以利用個人資料匿名化處理保護與資料分階段使用權限控管機制來實現個人隱私保護的目標。

壹、導論

建置國家關鍵資訊基礎設施防護（Critical Information Infrastructure Protection, CIIP）架構主要目的是用來維繫並且支撐著其它重要八大關鍵基礎設施的保護(Critical Infrastructure Protection, CIP)，如水資源、能源、交通、中央政府、高科技園區、醫療、金融、資通訊與其它類別的保護(國土辦，2012；Abouzakhar, 2013）。如果我們把 CIIP 比喻成 CIP 的神經傳導系統，則有優質的 CIIP 才能夠確保 CIP 的有效與正確性。當面臨網路資訊戰(Information War)或網路犯罪所產生的資訊安全（簡稱資安）異常事件時，CIIP 則扮演著舉足輕重的地位。我國目前 CIIP 與 CIP 的發展仍在初期，而他們未來的發展和執行將直接與國家安全與穩定有密切的關係(科顧組，2011)。

為了達成國家資通訊關鍵基礎設施防護目的，本論文首先探討與評論國內現有資通訊情蒐與分析的現況，資通訊情蒐的來源類別涵蓋有公開、半公開、與私有資通訊蒐集與分析。依據（科顧組，2011）的報告指出公務部門進行資通訊情蒐、分析與回應時，可以分別透過三種不同的機制來進行：(1)資安監控中心(Security Operation Center, SOC)可以進行整合式資訊安全監控，並對資安事件做出適當的對應機制; (2)電腦危機處理應變中心（Computer Emergency Response Team, CERT）

則以適當的方式提供網路事件處理與應變社群提升其對電腦安全議題的關注，並針對現有電腦與網路系統安全現況進行研究，進而預防未來可能發生的資安事件並找出適當應變機制; (3)資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)則是資訊安全相關資訊之蒐集、分析、與判斷的處理中心，提供資訊安全處理實務經驗分享與資安異常事件訊息的相互流通。

這三種資安機制的處理面臨了幾項挑戰。首先建置這些功能的單位因為是分布在中央政府機關、教育機構、法人機構、和民間資通訊業者，因此是以分散式且各自管理的模式來進行資安防護。至於該如何有效的整合這些單位的分散機制以分享資安事件訊息，進行全方位資安事件處理，確保國家資訊安全來達成 CIIP 本身與其它 CIP 的目的，目前相關機制尚在規劃中。此外如何確保資通訊情蒐、分享、整合與使用是真正符合相關的法律規範，如國家安全法、個人資料保護法、通訊保障及監察法等，也有需要做更深入的探討，以確認執行程序的合法性與適當性。當有犯罪異常現象發生時，如何透過已經蒐集到的資安事件的訊息來進行犯罪事件的事先預防與事後的追蹤和分析則是另外一個重要的議題。最後，目前資通訊情蒐與分析系統是以及時性，還是運用批次方式，或是雙軌其下的方式來進行，則需要更進一步釐清，否則無法解決關鍵性資通訊系統遭受攻擊後的有效復原與正常運作。

雲端運算(Cloud Computing)平台的建置和使用日漸普及，主要是因為使用雲端平台具有高經濟效益誘因，因此大量資訊在網路上流通、存放、分享、整合、與使用等管理功能都可以透過雲端運算平台來實現。這些資訊有些是開放式或半公開放式的型態，如 Web 2.0 社群網路的活動資訊。有些則是屬於私有性個人通訊資料，如電子郵件或電話通訊等，這些私有性個人通訊資料必須要受到個人資料保護法規範其資料的使用。因此唯有這些被大量產生的巨量資料(Big Data)經過匿名化(Anonymizing)處理過後，才被允許在雲端平台上進行委外存放、流通、分享、整合與分析。

巨量資料的概念是來自於資訊網路上大量、快速、及多樣化資料產生後透過資料分析所產生的價值（Manyika, et al., 2011）。配合雲端運算的平台效益與電腦硬體價格的下降，巨量資料的處理成本效益將愈來愈高。因此巨量資料也將逐漸應用在各個領域。兩項相關研究的發展將和本論文有直接關連：（1）雲端運算平台上巨量資料所產生的保護與分析效益(Cardenas, et al., 2013)。從 CIIP 防禦者的觀點來看，電腦系統與網路入侵偵測與追蹤的安全防護網可以透過巨量資料的技術來加以提升。當國家關鍵資訊基礎設施(CII)面臨正規化或非對稱性的攻擊時，因為雲端運算的平台可以讓 CII 產生自我恢復運作的能力。相對的 CIIP 攻擊與破壞者也可以透過雲端平台與巨量資料蒐集與分析的技術來強化其自身的攻擊與身份隱藏的能力，來進行持久性的攻擊；（2）建構與執行巨量資料保護機制來確保個

人隱私權的維護其挑戰度將更高，主要是因為來自多重資料源大量且多樣化的資料，經過有效整合、分析與交叉比對，原有匿名化處理的個人資料，因為個人識別碼(Personally Identifiable Information, PII)的還原，因而產生個人資料的揭露和使用。這是在個人資料保護法沒有明確規範允許揭露的條件下來進行，因而可能違反個人隱私保護的法律準則。

巨量資料格式可以是結構化（Structured）的資訊模式如 Facebook 或 Twitter 社群網路上其人與人之間社會網路關係拓樸架構，這些結構化資料是存放於關連式資料中，但是絕大比率的資料是非結構化(Unstructured)資料，如社會網路使用者之間互通的文字，或圖片資訊。因此對於巨量資料的保護或分析，甚至於應用其於資安事件的分析與追蹤也要能夠同時處理上述兩項的資訊格式。分散式系統架構如 Hadoop 透過 MapReduce 的分散式資料處理可以有效運算來自多重資料源的巨量資料，並且進行非結構化資料的批次性(Batch)分析。至於 R 開放式統計軟體則可以對於巨量資料的結構化資訊如在社群網路上，人與人之間的結構性關係圖進行重要指標的分析與圖形顯示。例如恐怖犯罪份子透過資訊網路互動所形成的人脈關係圖，可以利用 R 的統計軟體來加以分析與顯示。而他們互相通訊內容的資料檢索與查詢則可以利用 MapReduce 的分散式程式語言來完成。

傳統的 CIIP 是在骨幹網路的重要節點建構防火牆（Firewall）與入侵偵測系統(Intrusion Detection System, IDS)。為了確保資訊網路的正常運作與異常資安事件的預防與偵測，我們可以透過防火牆的事前預防與入侵偵測系統的事後偵察方式來完成。此外，為了能夠更有效與完整的來進行資通訊關鍵基礎設施防護網建置，並偵測出日新月異且有系統的網路攻擊行為，如零時差攻擊(Zero-Day Attacks)與進階持續式威脅(Advanced Persistent Threat , APT)(Curry, et al., 2011)。本研究建議在原有的防火牆與入侵偵測系統安全防護系統之外，建置一個兼具國家安全與個人隱私權保護兩項目標的資通訊情蒐與分析系統。並參考現有歐盟的 WOMBAT (WOMBAT, 2011)和美國 PREDICT(PREDICT, 2011)對於網際網路資通訊安全事件蒐集、分享、與分析中心，進行各種資安事件的模擬與演習，來確認 CIIP 防護網的有效性與正確性。CIIP 系統可以運用雲端平台的分散式架構來進行，透過有效且低成本的雲端系統，在國家關鍵資訊基礎設施上，我們除了能夠存放與蒐集網路基本協定層電腦間的原始通訊資料，也可以存放與蒐集網路應用協定層上人與人互動的生活資訊。並且更進一步對於上述兩大類型的通訊資料透過巨量資料有效的分析與推論，進行預防與偵測資安異常事件與其犯罪者所產生的相關連性，以強化國家關鍵資通訊系統基礎設施的防護網。但是這些被蒐集的巨量資料在被使用與分析之前必須要透過有效的資料匿名化處理與資料保護機制來確保個人隱私權不會受到侵犯。為了達成國家安全的目標，當被匿名化資料需要被還原與使用以追蹤可能犯罪者的身份時，我們也必須要透過合法的執行程序來進行。

貳、研究動機

新資訊科技的發展對於建構資通訊情蒐與分析系統將產生具體的影響與改變。根據最近的研究報告(Krekel, et al., 2009)指出傳統的資訊戰(Information Warfare)因為新型態網路與電腦系統攻擊方式的演進將產生新的防守與偵測的挑戰，如零時差攻擊與進階持續式威脅（APT）就是最具有代表性的範例。原有 APT 被啟動主要是達成政治與軍事上的侵犯目的。但是最近這個目的已經轉向成具有商業利益的智慧財產權文件的盜取。我們認為有必要重新檢視目前台灣現有資通訊情蒐與分析系統，並且探究國家關鍵資訊基礎設施防護網是否足夠來支撐著其它重要八大關鍵基礎設施的保護。當面臨新型態的網路與電腦入侵的資安攻擊與挑戰時，我們更該思考如何運用新發展的資訊科技，如雲端運算平台與巨量資料蒐集與分析技術來有效提升資通訊情蒐與分析系統的能力。我們也要確保現有的國家關鍵資訊基礎設施防護網的強韌度，也就是遭受到這些新型網路與電腦攻擊時，能夠自我復原並繼續正常運作，以支撐其它八大關鍵基礎設施的持續運行。除此之外，當國家安全執法人員為了落實國家安全目的所進行的大量資通訊的蒐集與分析，個人資料保護規範則同時需要被考量進來，以確保國家安全與國民隱私保護兩者之間可以達成相互平衡。

參、研究目的與具體貢獻

本論文研究的目的有三項：（1）檢視現有國家關鍵資訊基礎設施防護的現況並分析其保護網的架構與執行的機制是否足以應付新型態的資訊攻擊；（2）為了落實國家安全與犯罪防制與偵察，探討現有資通訊情蒐與分析系統其運作流程是否有考量到個人資料與隱私保護準則；（3）未來國家的資訊基礎設施防護系統，我們該如何考量新的資訊科技，如雲端運算平台與巨量資料分析，並將這些新技術應用於資訊安全來解決現有資訊基礎設施防護網所無法處理的資安事件，以確保國家關鍵資通訊基礎設施防護(CIIP)。

肆、台灣現有資通訊情蒐與分析系統

1. 資通訊情蒐與分析系統

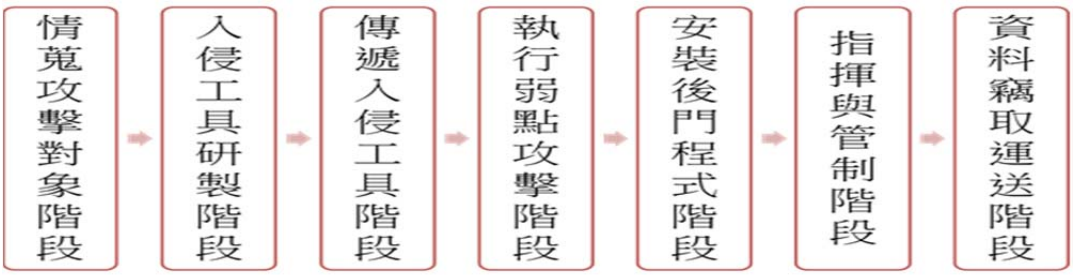
目前中央政府機關對於資通訊情蒐與分析的現況主要是委外給資訊安全專業公司來進行(技服中心，2013)，透過 SOC (Security Operation Center)廠商可以提供網路監控服務的第一線監控；另以行政院資安辦公室角度，目前正規劃第二線監控機制並且由行政院國家資通安全會報技術服務中心（技服中心）執行，請 SOC 廠商回傳資安事件相關資料，並進行資料關聯分析，以掌握資安威脅趨勢，並達早期預警及資安聯防等目標。目前網路監控資料主要包括有防火牆（Firewall）、

入侵偵測系統(IDS)、入侵預防系統(IPS)及電腦伺服器(Server)等類別所產生的活動資訊，並依據資安防護及事件通報與應變作業規範程序來處理。目前網路監控資料主要是透過 SOC 系統，如 ArcSight 等及時分析，進行資安防護及阻擋網路攻擊；另電腦犯罪調查涉及數位證據保全及電腦數位鑑識，目前一般資安事件發現的時間點大都在事件發生後一段時間，因此較難及時發現，如 APT 等攻擊，因此執法人員必須追查事件發生時之相關紀錄資料，以進行事後的追蹤與分析。對於這些資料的蒐集與使用，是否符合國家安全法、個人資料保護法、通訊保障及監察法等法律規範，較少探討。

依據技服中心的報告（技服中心，2013），政府資訊分享與分析中心（G-ISAC）蒐集與分析主要資安事件的情報類別有惡意網頁與釣魚網頁、社交工程郵件攻擊、網路攻擊與惡意程式、殭屍網路攻擊及垃圾郵件等。在 101/06/01 - 102/04/30 的期間 G-ISAC 共分享了 107,736 則情報，其中以入侵攻擊事件的數量 99,679 約 92.52%為最高。這些事實所代表的是網路的資安事件總是層出不窮，我們需要一套有效的防禦與資訊蒐集與分析的機制來處理。因此技服中心建置的 SOC 透過誘捕架構 HoneyBEAR 電子文件自動檢測機制來找出可能的垃圾郵件，並且更進一步分析這些郵件的附檔是否有包含有社交工程攻擊。政府資通安全防護管理中心（G-SOC）則是以雲端化監控架構於共構虛擬機房提供 24x7 的資安監控與防護的服務。101 年加入了巨量資料分析模組 Map/Reduce。根據技服中心報告所提供的 SWOT (Strength, Weaknesses, Opportunities, Threats)的分析（如下圖一所示），我們瞭解到目前政府資通訊情蒐與分析系統面臨最大的挑戰是對於組織型駭客利用新型態的網路攻擊，如零時差與進階持續式威脅反制能力尚未完備。

圖一：政府資安防護優弱機威(SWOT)策略分析圖

洛克希德馬丁公司首先借用狙殺鍊防禦(Kill Chain Defense) 的名詞來定義一種針對進階防禦威脅(APT)與非傳統網際威脅的防禦策略。防護者根據攻擊生命週期蒐集分析資料，並經由關聯分析判斷攻擊目前進行的階段。此方針運用的資訊安全上即稱為網際狙殺鍊(Cyber Kill Chain)（Hutchins, et al., 2011），其架構如圖二所示。



圖二：反擊新型態的網路攻擊如零時差與進階持續式威脅的網際狙殺鍊防禦

目前國內所使用的偵測防護工具並未完全符合網際狙殺鍊架構，因為在功能上尚有許多狙殺鍊架構階段功能未達到，經過檢視自身的弱點後，可由此分析結果提供國內資安防護發展未來改進的參考（請參考圖三）。

階段	A	B	C
情蒐攻擊對象 (Reconnaissance)	O	O	O
入侵工具研製 (Weaponization)	X	X	X
傳遞入侵工具 (Delivery)	X	O	O
執行弱點攻擊 (Exploitation)	O	O	O
安裝後門程式 (Installation)	X	O	X
指揮與管制 (Command and Control)	X	X	X
資料竊取運送 (Actions on Objectives)	X	X	X

A : G-SOC, B : G-ISAC, C : G-ISAC(HoneyBEAR)

圖三：偵測防護工具與網際狙殺鍊架構比對

伍、新世代資通訊情蒐與分析系統

1. 資通訊情蒐與分析系統

資通訊資料的蒐集類別，大致上分成兩大類：具個人識別碼(Personally Identifiable

Information, PII)、不具個人識別碼。通常為了要偵測網路或伺服器資安事件所蒐集到通訊協定層如 TCP、IP 的資訊，如果沒有和其它相關連應用協定層的個人連接，比較不會有侵犯個人隱私的情況出現。但是應用協定層上所產生的資訊則將會有個人識別碼在其中，例如社群網路、電子郵件、電話、電子商務交易、個人疾病資料等被蒐集到的資訊即是。

首先我們針對為了預防與偵測可能產生資安事件且不具個人識別碼的情蒐與分析系統來討論。資通訊情蒐與分析可以透過防火牆與入侵偵測系統（Intrusion Detection System, IDS）。防火牆是為一個內在區域網路所建構規範設定的閘門控管機制，網路連線與資訊流通從外到內或由內到外都需要經過此閘門的檢驗以確保異常的網路與電腦入侵事件可以降低到最小。至於入侵偵測系統則是補足防火牆之不足，針對非法進入內在區域網路漏網之魚的非法網路與系統事件以事後捕抓的方式來進行。

電腦與網路入侵偵測系統可以分成三個世代(Cardenas, et al., 2013)，第一世代的 IDS 指的是最原始的系統架構；第二世代則是從多重資料源所佈建感測器蒐集與篩選回來的示警(Security Information and Event Management, SIEM)系統；第三代則是以巨量資料分析技術為導向的智慧型 SIEM 系統。當我們選擇第三代的 SIEM 系統時，所代表的是資安事件其來源和資訊量非常的多，涵蓋了有結構化與非結構格式所規範的示警資訊，這些情境將不是現有 SIEM 入侵偵測系統所能有效處理的情境。因此我們必須提升到第三代 SIEM 入侵示警系統。當更進一步需要對資安事件分析時，第三代的系統也能夠同時整合結構化 SQL 資料庫與非結構化 NoSQL 的資訊來進行有效的整合性分析。

例如為了能夠判斷有哪些電腦系統被駭客入侵成為 Botnets 的一份子來進行網路與電腦系統的攻擊，我們必須蒐集大量網路監控的流量資訊，並且透過類似 Google 搜尋引擎的 PageRank 演算法與群聚(Clustering)演算法來找出源頭下達攻擊命令的攻擊者與 Botnets 的成員，我們必須要用新世代具有巨量資料蒐集與分析能力的第三代 SIEM 示警與分析系統才能夠完成此任務。同樣的針對最近知名的 APT 攻擊，傳統的第一代與第二代的入侵偵測系統也同樣是無法提供有效的偵測與示警功能。因為大量使用者與電腦主機活動紀錄從不同點產生，它們涵蓋有防火牆的紀錄檔、Web 代理伺服器(Proxies)的紀錄檔、DNS 查詢紀錄檔、一般入侵偵測系統的紀錄檔與 VPN 伺服器所產生的紀錄檔等。這些紀錄檔的整合與分析必須要利用巨量資料的技術才能夠完成有效異常事件的偵測與示警(Giura & Wang, 2012)。

至於蒐集具有個人識別碼的個人上網與使用電腦系統的情蒐與分析，在法律的規範與實際系統的運作上則必須要更為小心，否則執法者將面臨個人隱私被侵犯的

挑戰(National Academy of Sciences, 2008)。因為線上社群網路(Online Social Network, OSN)與電子郵件、電話的情蒐與分析，主要是針對犯罪者或恐怖份子透過電腦網路與電話快速有效溝通平台所留下紀錄。這些溝通紀錄有的只是用來聯繫與發動如何進行實體世界的破壞與攻擊行動，因此犯罪者只是把這些電腦與資訊網路當作工具。但是有的犯罪者則是利用資訊網路的平台進行關鍵資訊基礎設施的入侵與攻擊。假使其它八大基礎設施如果有連線上網，則也會因此受到直接或間接的波及和破壞而產生無法正常運作的情況。上述兩種的攻擊與破壞模式，在背後都有人為的因子在支持。當進行網路上個人資料蒐集與揭露、分析流程時如何有效的找出這些背後的人為因子而不會影響其他人人的隱私保護，來有效進行事先預防與事後調查，將都是執法者所面臨的最大挑戰。

2. 如何兼具國家安全與隱私保護

為了國家安全而進行資通訊的情蒐與分析其最大的挑戰是否能夠同時兼顧個人資料與隱私的保護。因為就資料本身的使用與分析者的觀點而言，總是希望能夠蒐集愈多的資料並且加以使用。但是在資訊氾濫的新科技巨量資料世代，如果沒有一套有效的資料篩選與搜尋的機制，越多資料的情蒐未必能夠找出有用的資訊並且做出正確且及時的判斷。因為有很多被蒐集回來的資料，可能會是無意義的雜訊，而這些不相關資訊的使用如果使用不當，非常容易就侵犯個人隱私，因而違反個人資料保護法。雖然執法人員在執行公務的目的是確保國家安全，但是資料的情蒐還是必須要以合法的程序來進行。

為了確保個人隱私，具體的作法可以分成兩大方向：（1）所有的資訊蒐集與分析必須要在符合個人資料保護法的規範下來進行，如資料擁有者同意並且符合資料使用特定目的和資料使用者身份符合下進行。雖然在執行國家安全目的時資訊的蒐集和使用時，可以是個人資料保護法的例外，也就是要經過當事人事先同意，但是執行人員的身份以及資料蒐集和使用目的還是要符合執行國家安全相關法規的要項;（2）資訊科技在落實個人資料保護法時其系統設計與執行上也必須要同時考量個人隱私保護與國家安全兩大目標。

依據(Popp & Poindexter, 2006)的建議，為了建置一個兼具國家安全與個人隱私保護的資料揭露與使用的資訊系統，每一個被蒐集的資料源必須要安裝一個隱私保護裝置(Privacy Appliance)。當執法人員為了進行國家安全目的的調查而進行型態式資料查詢(Pattern -based Queries)時，這個隱私保護裝置將提供資料使用者的身份認證並決定資料授權的等級，透過匿名化的機制可以依據等級來進行資料欄位選擇性的部分揭露。更重要的是，任何執法者其資料查詢紀錄必須要用無法更改的稽核紀錄檔 (Immutable Auditing Log) 來存檔。當面臨個人隱私受侵害的法律訴訟時，可以利用這些原有的稽核紀錄檔來驗證其適法性。而所有資料源匯集處

的單一資料查詢點則必須提供一個跨資料源的隱私保護裝置，它可以用來整合每一資料源的隱私保護裝置的選擇性揭露性資料，並且分析與推論是否會發生整合多重資料源時，個人匿名化資料被還原而侵犯個人隱私的情境。這種以身份別、等級與目的，並且非一步到位的個人資料分階段揭露方式，是用來確保國安人員在執行國安目的時能夠同時兼顧個人資料與隱私權保護的法律準則。美國自從 2001 年 911 雙子星攻擊事件之後，其國家授與資訊安全與情報單位非常強大的資源與適當的法源依據，如美國愛國者法案(Patriot Act)或 Foreign Intelligence Surveillance Act (FISA)法案，來進行美國境外和境內通訊的原資料(Metadata)通聯紀錄與更進一步通話內容的蒐集與分析。因為電腦建置成本的大幅下降，透過雲端運算平台建置與巨量資料查詢與分析的能力，除了原資料的蒐集與分析之外，美國國家安全局(National Security Agency, NSA)最近被指控因為其透過資訊攔截(Eavesdropping)資訊大廠 Google, Yahoo 其境外資料中心之間的傳輸線以及監聽盟邦如德、法、西班牙、墨西哥、阿根廷等元首電話，這些問題所代表的是資訊科技的發展和（國際）法律規範認知和執行時的落差。同樣的問題也發生在國內執法人員電話監聽程序與法律規範適用性認知差異的問題。這些都表示未來資訊蒐集與分析技術的發展和法律規範如何相呼應需要更深入研究的迫切性。

陸、相關研究

行政院國家資通安全會報與國土安全辦公室所提供的政策報告，可以讓我們瞭解到國家(資訊)關鍵基礎設施安全防護政策與執行的現況(科顧組，2009；科顧組，2011；國土辦，2012；技服中心，2013)。最近幾年資訊安全與通訊知名大廠如 RSA(EMC), Symantec, Verizon 所提出的研究報告則讓我們瞭解到各種網路與電腦系統的攻擊、入侵型態與未來可能的發展趨勢(Baker, et al, 2010; Curry, et al., 2011; Symantec, 2013）。美國自從 2001 年 911 恐怖事件之後，反恐作戰時兼顧資訊科技與隱私保護所提供的研究成果則分別有國家科學院報告(National Academy of Science, 2008)與 Wiley/IEEE 所出版的專書(Popp & Yen, 2006)。資訊安全與資訊戰的年度知名的國際研討會則可以參考(Abouzakhar, 2013; Hutchins, et al., 2011)。雖然網際網路無國界，但是國內資訊安全與關鍵資訊基礎建設保護網的建置還是需要在參考相關文獻的分析之後，因地制宜來進行。

柒、結論與未來研究

本研究的主要目的在於探索與分析現有國家關鍵資訊基礎設施防護網的資料情蒐與分析的現況，主要包含: 資安監控中心(SOC)、電腦危機處理應變中心(CERT)、資訊分享與分析中心(ISAC)這三種類型所進行工作的要項來分析。我們建議這三種型態的資安事件情蒐與分析平台可以更具體與有效的加以整合，以建置全方位資安事件防護網，並利用正在起步的雲端共購機房建置設備來整合資訊安全系統

平台的運作。在這個平台之上蒐集各種的虛擬網路上可能的新型攻擊與入侵案例來模擬與演練入侵偵測系統，以強化國家關鍵資訊基礎設施防護網。

參考技服中心報告，我們瞭解到現有國內網路入侵攻擊事件每一年約有10萬件。但是對於新型態的網路攻擊如零時差與進階持續式威脅的狙殺鍊防禦在現有資訊基礎設施防護網尚有加強的空間。可以參考國外雲端運算平台結合巨量資料分析的新技術來強化新型態網路攻擊與入侵的預防與偵測。對於兼顧國家安全與個人隱私保護的資通訊情蒐與分析系統的建置與執行，可以參考歐美相關資訊系統與法律規範並且因地制宜運用到國內的國家關鍵資訊基礎設施防護網。未來可能的研究重點將是在雲端分散式平台之上建構一個具有巨量資料蒐集、分析能力提供關鍵資訊基礎設施防護網的系統模擬環境。

捌、參考文獻

一、中文文獻

行政院科技顧問組（科顧組），2009，《國家資通訊安全發展方案》，行政院國家資通安全會報

行政院科技顧問組（科顧組），2011，《關鍵資訊基礎建設保護政策指引》，行政院國家資通安全會報

行政院國土安全辦公室（國土辦），2012，《國家關鍵基礎設施安全防護計畫指導綱要》

行政院國家資通安全會報技術服務中心（技服中心），2013，《國內資通訊情蒐分析架構的現況分析與優缺點》

二、外文文獻

Abouzakhar, N. 2013. *Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations.* 12th Annual European Conference of Cyber Warfare and Security (ECCWS). University of Jyväskylä, Finland.

Baker, W. et al.. 2010. *2010 Data Breach Investigation Report.* Verizon Inc.

Cardenas, A. A, et al.. 2013. *Big Data Analytics for Security Intelligence.* Cloud Security Alliance.

Curry, S. et al.. 2011. *RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats*. EMC, RSA.

Giura, P. & W. Wang. 2012. *Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats.* New York, NY. AT&T Security Research Center.

Hutchins, M. E., et al.. 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. 6th Annual International Conference on Information Warfare and Security. Washington, DC.

Krekel, B., et al... 2009. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* Prepared for The US-China Economic and Security Review Commission. Washington, DC, Research Report. Northrop Grumman.

Manyika, J., et al.. 2011. *Big Data: the Next Frontier for Innovation, Competition, and Productivity.* Technical Report, McKinsey Global Institute.

National Academy of Sciences. 2008. *Protecting Individual Privacy in the Struggle Against Terrorists.* Washington, DC, USA. The National Academies Press.

Popp, R. & J. Poindexter. 2006. "Countering Terrorism through Information and Privacy Protection Technologies." *IEEE Computer Security* 4(6):18-27.

Popp, R. & J. Yen, eds.. 2006. *Emerging Information Technologies and Enabling Policies for Counter-Terrorism.* Wiley&Sons/IEEE Press.

PREDICT. 2011. *Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT)*. https://www.predict.org/ .

Symantec. 2013. *Internet Security Threat Report 2013.* CA, USA. Symantec Corp.

WOMBAT. 2011. *Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT).* http://www.wombat-project.eu/ .