淺析建構國防領域資安資訊分享與分析中心之研究

作者／李建鵬中校、狄學謙少校

提要

一、在資訊科技蓬勃發展的情況下，資訊安全議題日益受到重視，尤其在關鍵基礎設施方面，對於國家安全造成的影響備受關切。

二、資安威脅漸趨複雜且多樣化，加以虛擬化、雲端運算、物聯網和大數據等科技發展，正引領著資訊領域轉型趨勢，除了帶動資訊服務產業的商機和發展外，亦對資訊安全工作帶來了不同程度的挑戰。

三、本文藉由探討美國與我國資安資訊分享與分析中心的起源與發展、相關政策的演進，以及目前正所面臨的資安威脅與挑戰，進一步提出建構國防領域資安資訊分享與分析中心的建議，並提供其重要因素，作為我國未來防護國防產業鏈資訊安全的參考，期可確保國防自主政策順利地推展遂行。

關鍵詞：資安資訊分享與分析中心、關鍵基礎設施防護、資訊安全。

前言

近年來由於資訊發展愈趨貼近生活應用與廣布各行各業，人們開始大量運用資訊系統解決各領域職場及民生所需各項難題。迄今，資訊系統已融入各行各業的作業流程中，資訊系統的安全性逐漸成為組織營運不可忽視的重要項目。2007 年的愛沙尼亞網路戰爭，喚起了各國政府對於資訊安全的重視，人口只有 130 萬人的愛沙尼亞，約有 30 萬俄人聚居，當年 4 月愛沙尼亞政府由於選舉考量，決定將首都塔林(Tallinn)蘇聯時代所製作的軍事紀念像搬遷到軍人墳場，該舉動引起愛國境內俄裔人士及俄國政府強烈抗議及示威活動。4 月 27 日起，該國多個網站開始受到網路攻擊被迫關閉，災情自報紙及電視台等媒體網站開始，蔓延到學校及銀行，其中部分網站的首頁被置換，出現俄國的宣傳口號及偽造的道歉聲明，另該國總統的網站同樣失去運作能力。經查網路攻擊的主要目標網站計有愛沙尼亞總統和議會網站、政府各部門、各政黨、六大新聞機構中的三家、最大兩家銀行及通訊公司。5 月 3 日網路攻擊出現第一次高峰，不但中央政府主要各部會及報社媒體網路受到分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)，電子郵件無法收發、網路中斷或是網頁遭置換，由於銀行也遭受攻擊，網路交易及轉帳都無法進行，該國曾經一度切掉所有對境外網路應變，使得

該國如同網路孤城一般。[1]愛沙尼亞首相指出，雖然本次攻擊來源看似來自世界各地的電腦，但國防官員追查攻擊時，發現攻擊的源頭直接來自俄羅斯，部分網域名稱還以俄羅斯總統普丁的名義登記。[2]

愛沙尼亞網路戰爭之後，資安的威脅持續加劇，2015 年 12 月 23 日烏克蘭電力網路遭駭客攻擊，導致伊萬諾-弗蘭科夫斯克州 22.5 萬戶陷入停電，成為全球駭客攻擊造成電網大規模停電首例，引發全球關注；[3]2018 年 5 月 28 日智利銀行(Banco de Chile)遭受來自國際網路，名為 KillDisk 的惡意程式攻擊，該程式將銀行內部約 500 台伺服器及約 9000 台工作站硬碟格式化，致使分行與電話銀行服務無法運作，另同年 1 月趨勢科技亦公布於其他拉丁美洲銀行偵測到該類型的變種惡意程式活動。[4]此外，根據美國華盛頓郵報報導，中國政府於 2018 年 1 月與 2 月兩度入侵美國海軍承包商，竊取機敏資料多達 614GB，其中涵蓋了美國潛艦所用之超音速反艦飛彈專案內容，[5]顯現網路攻擊已有模組化及針對性的發展趨勢，並已擴及國家關鍵基礎設施及國防產業。而依據世界經濟論壇於 2019 年 1 月的全球風險報告，網路攻擊及資料遭竊已被列為全球前五大可能性的重大風險之一，[6]資訊安全成為國家與企業不容忽視的議題。

我國面臨的資安威脅與挑戰

一、資安威脅環境複雜

行政院國家資通安全會報技術服務中心研析全球網路攻擊事件，歸納出資安威脅趨勢，分別為「進階持續威脅攻擊竊取機密資料」、「分散式阻斷服務攻擊癱瘓網路運作」、「物聯網設備資安弱點威脅升高」、「關鍵資訊基礎設施資安風險倍增」、「網路與經濟罪犯影響電子商務與金融運作」及「資安(訊)供應商持續遭駭破壞供應鏈安全」等6項，[7]所面臨之資安威脅既複雜且多樣化，以下茲針對各項列舉近年駭客侵入事件做探討。

(一)進階持續威脅攻擊竊取機密資料

首先，在進階持續威脅(Advanced Persistent Threat, APT)攻擊竊取機密資料方面，APT攻

---

[1] Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia,” The guardian, http://www.guardian.co.uk/world/2007/may/17/topstories3.russi, (2019/2/15).

[2] Steven Lee Myers, “Cyberattack on Estonia stirs fear of virtual war,” The New York Times, https://www.nytimes.com/2007/05/18/world/europe/18iht-estonia.4.5774234.html, (2019/2/15).

[3] 藍弋丰，〈烏克蘭電力系統遭駭原因是網路釣魚，如何加強資安防護引討論〉《科技新報》，https://technews.tw/2016/04/26/ukraine-power-system-phishing-information-security-protection/，(檢索日期：2018 年 10 月 2 日)。

[4] 林妍溱，〈智利最大銀行遭駭，疑近萬台系統遭癱瘓，再用 SWIFT 網路盜轉〉《iThome》，https://www.ithome.com.tw/news/123770，(檢索日期：2018 年 10 月 2 日)。

[5] Ellen Nakashima and Paul Sonne, “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare,” The Washington Post, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08,(2018/10/2).

[6] World Economic Forum, “The Global Risks Report 2019 14th Edition,” http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf, (2019/3/12).

[7]〈107 年第 4 季資通安全技術報告〉，行政院國家資通安全會報技術服務中心，https://www.nccst.nat.gov.tw/TechnicalReport?lang=zh，(檢索日期：2019 年 3 月 16 日)。

擊為有組織、具針對性的攻擊活動，通常駭客除了會運用一般常見的攻擊技術與工具之外，還會針對目標製作客製化的武器，而該攻擊手法的節奏具有低調和緩慢的特色，藉由長時間的潛伏，慢慢掌握目標的弱點與系統運作特性，逐步地突破各層防禦措施，使受駭者難以察覺。2013年5月初，我國行政院電子公文交換網路系統即遭此手法入侵，負責電子公文交換的用戶端軟體eClient，在提供該軟體直接下載的網站中，被置換成一個惡意程式，不知情的用戶在安裝惡意程式後，會對外連線到不明的中繼網站。經追查駭客攻擊手法，發現為長期埋伏、有組織、有系統的攻擊行為，而影響範圍經行政院資通安全辦公室評估，超過7,000個政府機關單位受到影響，包括中央機關、地方機關、市政公所、醫院、中小學校都可能暴露在公文被複製竊取的風險中。[8]

(二)分散式阻斷服務攻擊癱瘓網路運作

其次，在分散式阻斷服務攻擊癱瘓網路運作方面，DDoS攻擊在愛沙尼亞網路戰即打響名聲，為較為傳統的網路攻擊手法，惟仍不可輕忽，該手法的特色為駭客透過大量電腦對目標進行攻擊，其目的在耗盡目標的網路或系統資源，使其無法正常提供服務。2017年1月至2月間，我國計有13家證卷商遭受此手法攻擊，其中最大的攻擊流量曾達到2至3Gbps，致使部分證卷商下單網站被短暫癱瘓。駭客以分散式阻斷服務攻擊癱瘓網站，其動機在藉此勒索比特幣，以謀取利益。[9]

(三)物聯網設備資安弱點威脅升高

由於資訊科技帶動的產品數位化轉型，物聯網的應用正在漸漸地擴展和普及化，相對應的資安威脅也正在同步增加。如前揭所述，由於物聯網設備多數暴露於未經保護的網路環境下，如系統本身安全防護機制設計不當，就很容易遭駭客入侵，被作為殭屍網路(Botnet)利用。2016年9月一種被稱為Mirai的惡意程式出現，入侵全球約14萬臺CCTV網路監視器，包含其他類型的IP攝影機及路由器，形成了以物聯網為主的殭屍網路，並向法國雲端服務與主機代管供應商OVH和美國網路服務商Dyn的DNS服務發動了DDoS攻勢，攻擊的殭屍網路來自世界各地，而我國亦受駭，成為Mirai殭屍網路的10大來源國家之一。[10,11]此外，2018年5月，我國網路設備製造商居易科技公司(DrayTek)所生產的路由器被揭露資安弱點，導致用戶的路由器設定遭駭客竄改，將網域名稱服務(Domain Name Service, DNS)連線被導向中國大陸的惡意伺服器，使駭客得以運用釣魚網站手法，以偽冒的網址蒐集用戶的資訊，受影響的家用路由器

[8] 黃彥棻，〈政府電子公文系統被駭，主管單位竟企圖遮掩〉《iThome 電腦報週刊》，http://news.pchome.com.tw/magazine/report/li/iThome/9716/137027520065460075005.htm，(檢索日期：2019 年 3 月 11 日)。

[9] 〈臺灣史上第一次券商集體遭 DDoS 攻擊勒索事件〉《iThome》，https://www.ithome.com.tw/news/111875，(檢索日期：2019 年 3 月 11 日)。

[10] 黃泓瑜，〈百萬 IoT 殭屍大軍來勢洶洶，Tb 級 DDoS 攻擊越演越烈〉《iThome》，https://www.ithome.com.tw/news/111220，(檢索日期：2019 年 3 月 11 日)。

[11] 〈Tb 級 DDoS 攻擊現身，每秒 1.5Tb 爆量創記錄〉《iThome》，https://www.ithome.com.tw/news/110135，(檢索日期：2019 年 3 月 11 日)。

超過25款。[12]從物聯網的資安事件可以得知，資訊科技的轉型不僅僅帶來了新的資安威脅，也提高了面臨既有網路攻擊手段的風險。

(四)關鍵資訊基礎設施資安風險倍增

關鍵資訊基礎設施為支持關鍵基礎設施持續運作所的資通訊系統或調度、控制系統，如因網路攻擊受損，將影響政府及社會功能運作、人民傷亡、財產損失、經濟衰退或損害國家安全與利益。[13]前述的2015年烏克蘭電廠，即為典型的關鍵基礎設施遭受攻擊事件，駭客透過釣魚郵件與惡意程式入侵電廠內部資訊網路，並在竊取權限後入侵其工業控制系統，在數小時內導致供電數次中斷，影響22.5萬用戶。[14]美國政府責任署(Government Accountability Office, GAO)於2018年10月發表了一篇針對國防部武器系統的滲透研究報告，指出部分武器系統缺乏嚴密的安全機制，只要運用簡單的工具及技術就能在不被偵測的情況下獲得相關系統的控制權，其中某一測試團隊僅僅一個小時就成功進入其中一個武器系統，接著只用一天的時間即取得該武器系統的完整控制權；許多測試人員發現能輕易地取得複製、竄改及刪除系統內部資料的能力，另一團隊甚至從系統裡直接下載了大約100GB的資料。[15]回到國內，2017年3月臺北市政府衛生局遭駭客入侵，駭客先攻陷資安防護較差之中小企業網站做為跳板，再對衛生局的資訊系統進行攻擊，以木馬程式盜走約298萬筆個資，經查攻擊IP位址來自上海，除衛生局外，連同國內其他十餘個政府機關、公立醫院、大學與上市公司的網站都遭受同類攻擊；同年5月，臺電大林廠770臺行政用電腦遭著名的勒索病毒WannaCry入侵，失去運作能力，所幸未影響供電，[16]以上事件均顯示出關鍵資訊基礎設施防護的重要性。

(五)網路與經濟罪犯影響電子商務與金融運作

網路與經濟罪犯較常見的網路攻擊手法為竊取個人隱私資料、結合詐騙及偽冒交易，金融領域亦為我國的關鍵基礎設施領域之一，2017年我國爆發了遠東國際商業銀行遭入侵案件，駭客入侵了該銀行負責處理匯款交易的SWIFT系統，盜轉了18億元匯款到柬埔寨、斯里蘭卡和美國，對我國家金融和經濟影響之大，不言而喻。[17]

(六)資安(訊)供應商持續遭駭破壞供應鏈安全

最後，在資安(訊)供應商持續遭駭破壞供應鏈安全方面，基於主要攻擊目標的防範措施嚴密，駭客可轉向入侵目標的上游供應鏈，一旦遭成功入侵，駭客可透過供應鏈將惡意程式

---

[12]〈2018 資安年刊〉(臺北市)，臺灣電腦網路危機處理暨協調中心，2018 年 12 月 25 日，頁 20。

[13]《國家關鍵基礎設施安全防護指導綱要》(臺北市：行政院，2018 年 5 月 18 日)，頁 3。

[14] Antiy Lab, "Comprehensive Analysis Report on Ukraine Power System Attacks," http://www.antiy.net/p/comprehensive-analysis-report-on-ukraine-power-system-attacks/, (2019/3/12).

[15] United States Government Accountability Office, "WEAPON SYSTEMS CYBERSECURITY: DOD Just Be-ginning to Grapple with Scale of Vulnerabilities," October 9 2018, p.22.

[16] 中央社，〈台電被勒索病毒攻擊，152 台電腦待修〉《科技新報》，https://technews.tw/2017/05/15/taipower-wannacry/，(檢索日期：2019 年 3 月 11 日)。

[17] 黃彥棻，〈遠銀遭駭追追追：更多入侵細節大公開！18 億元遠銀遭駭盜轉事件追追追〉《iThome》，https://www.ithome.com.tw/news/117397，(檢索日期：2019 年 3 月 12 日)。

以目標受信任的管道傳遞，達到間接入侵主要目標的目的。系統維護軟體CCleaner，是用來清除電腦的垃圾檔案、操作紀錄或程式的軟體工具，2017年9月，駭客利用數位供應鏈(Digital Supply Chain)將惡意程式植入CCleaner公司的安裝與更新系統，利用受信任的管道散播病毒，估計全球有227萬人已使用受影響的軟體。分析指出，駭客並非無的放矢的攻擊全球用戶，中毒的主機會自動將電腦中的重要資訊，包括IP位址、上線時間、主機及網域名稱等訊息傳送到外部的伺服器，由駭客透過回傳資訊分類出該主機是否為其針對目標，藉此決定是否進一步發布第二波惡意程式，而被針對的目標計有Singtel、HTC、Samsung、Sony、Gauselmann、VMware、Intel、Microsoft、Cisco、O2、Vodafone、Linksys、Epson、MSI、Dvrdns、Akamai、D-Link等電信及科技企業，其中HTC、MSI及D-Link均為我國廠商，對於供應鏈內的各種威脅應有所警覺。[18]

我國長期面臨中共文攻武嚇，相同的處境也反映在網路威脅上，政府部門每月平均遭受到的網路攻擊約有2千萬至4千萬次，其中多來自中共，而2018年政府部門被攻擊成功的案例就多達360件，[19]面對如此嚴峻的威脅環境樣貌和安全挑戰，實有賴政府與民間共同合作，共同維護國家的數位疆土與關鍵基礎設施。

二、資訊科技轉型挑戰

隨著電腦的普及和網路的蓬勃發展，有許多的資安漏洞和入侵知識、滲透工具都可以從網際網路上輕易獲得，或是透過交易取得，當今的網路環境除了技術專精的駭客外，還充斥著不具備專業知識卻運用工具程式四處刺探各網站弱點的腳本小子(Script Kiddies)。此外，科技發展帶來的虛擬化、雲端運算、物聯網和大數據等轉型趨勢，這些趨勢之間具有相當程度的相互依存性，帶動了產業的商機和發展，但也對資訊安全工作帶來了不同程度的挑戰。[20]

虛擬化是可讓組織將單一實體電腦或伺服器分割為數個虛擬主機，各部虛擬主機接著可採獨立或互動方式運作，並可執行不同的作業系統和應用程式，同時共用單一實體主機電腦的資源。[21]虛擬化面臨的資安威脅可從4個部分來探討，首先是虛擬主機本身是否遭植入惡意程式，獲得虛擬主機或是安裝在虛擬主機內部的應用軟體是否安全；其次為虛擬防火牆及網路的組態設定和架構是否提供有心人士可運用的漏洞，虛擬主機之間的網路流量，由於是在單一實體主機的背板上直接傳輸，原本傳統的網路安全設備如防火牆、入侵偵測系統等將無法偵測並阻擋網路攻擊，需透過同樣虛擬化的網路安全設備來因應；接著為虛擬主機管理層

---

[18] 林妍湊，〈植入 CCleaner 的後門程式已感染逾 200 萬台電腦，微軟、HTC、友訊、微星疑遭鎖定〉《iThome》，https://www.ithome.com.tw/news/116984，(檢索日期：2019 年 3 月 12 日)。

[19] 林孟汝，〈公部門遭網攻每月逾 2 千萬次，多數來自中國〉《中央社》，https://www.cna.com.tw/news/firstnews/201804050047.aspx，(檢索日期：2019 年 3 月 11 日)。

[20] Thomas A. Johnson 著，黃文啟譯，《網路安全-捍衛網路戰時代中的關鍵基礎設施(Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare)》(臺北：國防部政務辦公室，2017 年)，頁 357。

[21] 〈甚麼是虛擬化?〉Microsoft Azure》，https://azure.microsoft.com/zh-tw/overview/what-is-virtualization/, (檢索日期：2019 年 3 月 6 日).

的安全性，虛擬主機管理層負責監控和管理所有的虛擬主機，一旦被攻陷而被惡意人士取得控制權時，將嚴重影響所有虛擬主機的安全；最後是資料的安全，[22]當虛擬主機做為服務提供不同用戶操作和使用後，如何確保曾經使用過的機敏資料會被完全銷毀，而非殘留在儲存裝置裡，面臨資料外洩的風險，這些資安風險不容小覷。[23]

雲端運算是透過網際網路分享伺服器、儲存體、資料庫、網路、軟體、分析等運算服務，以靈活的資源運用方式提供更高的運作效能[24]。而根據雲端安全聯盟(Cloud Security Alliance, CSA)2018年的報告，雲端運算目前面臨的主要資安威脅計有12項：1.資料外洩；2.身份辨識、憑證和存取管理不當；3.不安全的應用程式與介面；4.系統漏洞；5.帳戶遭盜用；6.惡意的內部人員；7.進階持續威脅攻擊(Advanced Persistent Threat, APT)；8.資料遺失；9.組織未盡責；10.雲端服務的濫用；11.阻斷服務攻擊(Denial of Service, DoS)；12.共享技術的漏洞。[25]如此多元的威脅有賴組織從雲端資料安全、雲端平臺與基礎設施安全、雲端應用程式安全、維運管理等多個面向整體規劃，共同建立起防護措施，才能有效降低及消弭資安風險。

物聯網將物品透過網際網路連結起來，以提供智慧化的管理服務。然而，多數的連網設備並非位於有防護措施的網路環境，如家庭網路，且物品內的內嵌作業系統也存在著存取管控機制(如弱密碼、預設密碼、缺乏密碼輸入錯誤的鎖定機制)及安全更新機制(如對於更新資料的來源缺乏驗證或無法通知有更新軟體釋出)等風險，[26]管理不當的設備暴露在未提供網路防護的環境裡，無疑是提供駭客可利用的網路攻擊跳板及殭屍網路(Botnet)資源。

大數據的定義十分多元，但其本質脫離不了龐大的資料量、多元的資料型態以及高速的資料傳輸速率，以為達到廣泛、多面向和即時的資料分析。大數據的系統結構可能結合雲端運算、虛擬化或是物聯網的應用技術，以支撐起整個分析和運算環境，而其分析的資料來源可能包含網際網路、社群媒體、行動裝置及既有的資料庫，其安全議題可從基礎設施安全、資料隱私、資料管理、資料的檢測與應變安全4個面向來探討。首先在基礎設施安全方面，由於大數據系統多採分散式儲存和運算技術，需防範資料在計算過程中遭到蓄意攔截、破壞和竄改，還有資料庫系統本身遭惡意攻擊；在資料隱私方面，需注意運用的資料是否具機密性，並避免機密性資料遭不當人士揭露；在資料管理方面，需確保資料儲存的安全，如果加密後的資料與密碼金鑰如保管不當，會提供駭客可趁之機。而如果系統與用戶端程式的溝通方

[22] Bashir Aliyu Yauri, Joshua Abah, “Mitigating Security Threats in Virtualized Environments,” IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.1, January 2016, pp.104-105.
[23] 花俊傑，〈虛擬化安全與雲端資安服務〉《網管人》，https://www.netadmin.com.tw/article_content.aspx?sn=1212100015，(檢索日期：2019 年 3 月 5 日)。
[24] 〈何謂雲端運算?〉《Microsoft Azure》，https://azure.microsoft.com/zh-tw/overview/what-is-cloud-computing/，(檢索日期：2019 年 3 月 6 日)。
[25] Insure trust, “The 12 biggest cloud security threats in 2018,” https://www.insuretrust.com/the-12-biggest-cloud-security-threats-in-2018/,(2019 年/3/9).
[26] OWASP, “OWASP Internet of Things Project,” https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project, (2019/3/10).

式有漏洞，用戶亦可能被偽冒的系統服務商欺騙，下載帶有漏洞的更新程式；最後在資料的檢測與應變安全上，系統需能判斷資料的來源是否為可信任的對象並予以反應，有心人士可能偽冒資料來源端，傳送惡意的資料內容，干擾或影響系統運作。[27]由於大數據的基礎設施結構較雲端運算、虛擬化技術更為複雜，資料的蒐集來源也相當廣泛，因此大數據面臨的資安挑戰與風險絕不低於雲端運算和虛擬化。

美國資安資訊分享中心的發展與政策演進

關鍵基礎建設(Critical Infrastructure, CI)是指「為維持國家安全、民生、經濟而提供的基本產品或服務，包含維持國家最起碼的經濟、民生、政府運作與國家安全息息相關的實體和以資訊電子為基礎的運作系統。」[28]而關鍵資訊基礎設施(Critical Information Infrastructure, CII)為支持關鍵基礎設施持續營運所需之重要資通訊系統或調度、控制系統(Supervisory Control and Data Acquisition, SCADA)，亦為國家關鍵基礎設施的重要元件與資通訊資產[29]。資安資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)，其主要功能為蒐集與分析威脅情資並提供予所屬會員，以發揮早期預警功能，達到防護國家關鍵資訊基礎設施的目的，並降低資安風險。美國自1996年起便開始意識到國家關鍵基礎設施存在的弱點即可能成為恐怖分子攻擊的目標，因此由當時的總統柯林頓下達「13010行政命令」，將電信、電力、天然氣及石油儲存與運輸、銀行與金融、交通、供水、急難救助(含醫療、警政和消防)、政府持續運作能力等8項領域列為對美國至為關鍵的基礎設施，並說明「若其功能喪失或遭受摧毀，將削弱美國國防與經濟安全。」此外，該行政命令還要求成立「總統關鍵基礎設施防護委員會」，以策劃後續相關政策及事務推展。[30]

1988年5月22日總統決策令第63號(PDD-63)，要求與關鍵設施領域相關的聯邦政府各部門建立特定領域的組織，以共享資安威脅與弱點訊息，確立了ISAC的最初概念，[31]並鼓勵一般民間單位能自發性成立ISAC，隔年金融服務領域的ISAC機構隨即成立，為第一個在PDD-63決策令下成立的ISAC。2003年11月17日國土安全總統7號指令(HSPD-7)修正PDD-63決策令，明確要求資安資訊分享之任務，包含分析、預警、減少弱點、損害控管及災難復原，且領域需涵蓋各重要產業及基礎設施，如農業、醫療、環境保護、能源及國防工業等，另關鍵基礎設施各領域之主管機構應與私部門合作，以協助設施與產業擁有者/操作者防護其設施、人員及客戶免於資訊安全、實體安全及其他方面的危害，[32]隨後交通、能源及水資源等領域紛紛

[27] Cloud security alliance, “Expanded Top Ten Big Data Security and Privacy Challenges,” April 3 2013, https://cloudsecurityalliance.org/artifacts/expanded-top-ten-big-data-security-and-privacy-challenges/, (2019/3/10).
[28] 方鴻春，〈我國關鍵基礎建設安全防護〉《清流月刊》(新北市)，2 月號，法務部調查局，2009 年，頁 1。
[29] 同註 13，頁 3。
[30] 同註 20，頁 112。
[31] National Council of ISAC, “About ISACs,” https://www.nationalisacs.org/about-isacs, (2018/10/2).
[32] Homeland Security, “Homeland Security Presidential Directive 7:Critical Infrastructure Identification, Prioritization, and

成立ISAC機構。而為整合各領域的情資並促進各ISAC之間的互動與情資交換，跨領域ISAC之管理組織「資安資訊分享與分析中心國家委員會(National Council of ISACs, NCI)」於該年成立，以協調及管理各領域ISAC運用。

此外，2006年愛達荷國家實驗室(Idaho National Laboratory)的研究報告提出，各領域的關鍵基礎設施之間可能由於政策、程序或時空等因素形成跨領域的複雜關係、依存性和相依性，而關鍵基礎設施的防護能力取決於更全面地去理解各種基礎設施系統之間如何相互依存，如電力基礎設施受到損害會對天然氣供應、石油管線和供水產生影響。因此，關鍵基礎設施的防護應從過往各別單一防護的策略，轉換為考量相互依賴性所產生影響的整體防護思維[33]。後於2013年2月12日第21號總統政策指令(PPD-21)指出，美國的關鍵基礎設施具有多元性及複雜性，其涵蓋了美國所有的分散網路、不同組織架構，以及於實體空間與網路空間發揮功能的運作方式，關鍵基礎設施做為離散有形資產的概念已不合時宜，各設施均已和網路空間連結，多重系統之間的運作已具有更高的相互依賴性，此種網路與實體的融合造成了安全風險的改變，需透過有效的情資交換並建立防護陣線，以對抗實體與網路之安全議題。此外，該指令亦明確的定義了美國的關鍵基礎設施計16項及其負責的業管部會，其定義作為領域劃分基準沿用至今。[34]

2016 年 10 月，美國國土安全部進一步提出了關鍵基礎設施的威脅情資分享框架(Critical Infrastructure Threat Information Sharing Framework)，以協助關鍵基礎設施的所有者與營運者、其他私部門、聯邦、州與地方政府等合作夥伴如何分享、接受與報告網路及實體的威脅情資，在美國既有的國家安全戰略和計畫原則上建立了網路威脅資訊的分享框架與運作機制，並運用標準作業程序，以網路、實體、國際間、國家特別安全事件等四種類型的情境範例，詳細說明情資分享與交換的過程，其中該框架將威脅情資分享程序劃分以下七個步驟：

一、 情資來源者獲得情資

情資來源者可透過多元管道和手段獲得情資。如私人企業在其設施或網路上發現安全漏洞的趨勢；聯邦、州政府及地方機關收集到非法或可疑活動的情資；情報機關經過研判具威脅性的情資等。

二、 情資來源者將情資文件化並增加情資的保護措施

為組織發展和通報威脅情資和事件的報告程序，其中包含如何、何時將情資傳送給其他組織，該程序應涵蓋將「威脅情資標準化」及「標示威脅資訊保護措施級別和授權存取限制」等兩個步驟。

Protection," https://www.dhs.gov/homeland-security-presidential-directive-7, (2018/10/2).

[33] Idaho National Laboratory report INL/EXT-06-11464, "Critical Infrastructure Interdependency Modeling : A Survey of U.S. and International Research," 2006, pp.iii-7.

[34] Homeland Security, "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper," https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf, (2018/10/2).

三、 情資來源者針對所獲情資實施驗證與分析

情資來源者應在其能力範圍內，將所獲威脅資訊與其他知識整合，以驗證威脅資訊的準確性。此外，情資來源者應考量情資是否符其他合作夥伴的情資需求，以及該情資對關鍵基礎設施社群的價值。

四、 情資來源者遵守存取與使用限制來提供資訊

為確保第二步驟的情資保護措施規定執行順遂，情資來源者應依法規決定哪個組織或部門必須知道相關情資。聯邦政府的情報部門與執法機構、ISAC 等相關組織均已建立標示與處理威脅情資的標準協定。而情資來源者可以透過口耳相傳、電子郵件、電話或定期會議等，非正式與正式管道將情資傳遞。

五、 情資分享機構收集、整合、驗證、評估與分析資訊，並產生與分享成果

美國的情資分享機構包含聯邦調查局、ISAC 與地方執法部門等，情資分享機構在收到情資後，應對該資訊進行驗證和分析，整合其他情資與知識，並決定是否應提供給其他合作夥伴以及如何符合夥伴的使用需求。如果情資分享機構決定向其他合作夥伴提供情資，需包含該機構分析後的成果。

六、 降低威脅

關鍵基礎設施社群在接收威脅情資後，應依各單位角色及責任，制定應變的策略及執行作法，以降低威脅。

七、 回饋

回饋是情資分享機制的重點，由情資接收者向提供者和成果分析者提供回饋訊息，以改善分析成果的相關性，實用性和格式。[35]

美國於2017年12月提出之國家安全戰略中明確指出，國家關鍵基礎設施確保貿易運作、食物新鮮、住宅溫暖及公民的生產活動與安全，美國關鍵基礎設施在網路、實體和電子攻擊的弱點意味著敵人可能中斷及擾亂軍事的指揮與管制、銀行和財金運作，電力網和通訊手段。為確保美國在網路時代的安全，政府將與基礎設施夥伴及私部門擴大合作，評估其情資需求並致力減少情資共享的障礙，如速度與分類級別。亦將運用投資來提升美國分析、偵測網路攻擊的能力，以保護所屬公民的自由和隱私。[36]在此戰略下，ISAC在關鍵基礎設施聯防中分析與分享的角色就更加顯得重要。迄今，美國已設置20個ISAC，其範圍涵蓋化學、商業設施、通訊、重要製造業、水壩、國防工業、緊急勤務、能源、金融服務、糧食與農業、政府設施、衛生保健與公共衛生、資訊科技、核反應爐(含原料與廢料)、運輸系統、供水與廢水

[35] Homeland Security, “Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community, Office website of Department of Homeland Security,” https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf, (2019/3/11).

[36] Whitehouse, “National Security Strategy of the United States of America,” https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, (2019/2/25).

系統等關鍵基礎設施領域[37]，計有：汽車ISAC(Automotive ISAC)、航空ISAC(Aviation ISAC)、通訊ISAC(Communi- cations ISAC)、國防工業ISAC(Defense Industrial Base ISAC)、天然氣分配ISAC (Downstream Natural Gas ISAC)、電力ISAC(Electricity ISAC)、緊急事務管理與應變ISAC(Emergency Management and Response ISAC)、金融服務ISAC(Financial Services ISAC)、醫療ISAC(Health ISAC)、保健整備組織ISAC (Healthcare Ready)、資訊科技ISAC(Information Technology ISAC)、航海ISAC (Maritime ISAC)、州際ISAC(Multi-State ISAC)、國防ISAC(National Defense ISAC)、石油與天然氣ISAC(Oil and Natural Gas ISAC)、不動產ISAC(Real Estate ISAC)、研發與教育網路ISAC(Research and Education Network ISAC)、零售與觀光ISAC(Retail and Hospitality ISAC)、地面及公共運輸ISAC(Surface Transportation, Public Transportation and Over-the-Road Bus ISAC)、水資源ISAC(Water ISAC)。

從上ISAC範圍即可以看出，ISAC的設立考量了領域內資訊系統與產業運維的特性，以交通為例，就區分了航空、航海、地面運輸3個ISAC，如此便可依其產業特性提供會員需要的服務，民間組織或公司亦可依其業務性質成為其中一個或數個會員。在20個ISAC中，與國防相關的計有國防工業領域ISAC(Defense Industrial Base ISAC, DIB ISAC)及國防領域ISAC(National Defense ISAC, NDISAC)等2個項目。國防工業領域被視為美國國家關鍵基礎設施領域之一，國土安全部將其定義為：「國防工業領域為一全球性的工業綜合體，能夠研究、開發、設計、生產、交付和維護軍事武器之系統、子系統和元件的設計，生產，交付和維護，以滿足美國的軍事需求。」[38]DIB ISAC的主要工作為蒐集、分享及分析關於網路或實體事件的安全議題，包含威脅和入侵資訊以及最佳安全實作方案，並增進其組織面對安全威脅、漏洞和意外的應變與降低風險能力[39]；而國防領域ISAC與美國國土安全部、美國國防部、聯邦調查局網路安全部門等機構結合策略夥伴，主要任務除了威脅情資的分享與分析外，在於提升國防工業及其戰略合作夥伴的安全及復原能力，並協助所屬會員建立運用安全的資料數據、工具與服務，以及安全實作的能力。[40]

我國資安資訊分享與分析中心的發展與政策演進

我國為推動資通安全基礎建設工作，於2001年成立「行政院國家資通安全會報(資安會報)」，並推動四個階段、各階段分別為期四年的資安重大計畫：

第一階段為 2001 年至 2004 年，目標為「建構資安防護體系，完成政府機關分級機制」，首先致力於推動政府機關(構)的整體資安防護體系，將政府機關區分為國防、行政、學術

[37] National Council of ISACs, “MEMBER ISACS,” https://www.nationalisacs.org/member-isacs, (2019/2/28).
[38] Homeland Security, “Defense Industrial Base Sector,” September 22 2015, https://www.dhs.gov/cisa/defense-industrial-base-sector, (2018/12/11).
[39] DIB ISAC, “Mission Statement and Objectives,” http://www.dibisac.net/dibisac_web_0618_003.htm, (2018/12/11).
[40] National Defense ISAC, “National Defense ISAC,” https://ndisac.org/, (2018/12/11).

、事業 1(水、電、石油、瓦斯)、事業 2(交通、通信、網路、航管)、事業 3(金融、證券、關貿)、事業 4(醫療)等 7 個不同屬性類別。而每項屬性類別下再區分「重要核心單位」、「核心單位」、「重要單位」及「一般單位」等 4 個等級，依各單位的等級及重要性提供不同的資安工作要求與支援，以確保運用有效的資源完成資安防護工作。此外，亦針對關鍵基礎設施的資訊系統推動資訊安全管理制度，並要求建置異地備援系統及通過國際資訊安全管理系統驗證。

第二階段為2005年至2008年，目標為「健全資安防護能力，成立國家資安監控中心」，將教育體系納入資安防護體系，並重新界定分級作法。另外，於2004年12月建立國家資通安全防護管理平臺(National Security Operation Center, NSOC)，統一監控政府23個機關的資安防護。

第三階段為2009至2012年，目標為「強化資安整體應變能力，精進通報應變機制」，此時我國政府逐步將推動資安的經驗推廣至民間和企業，並於2009年11月建置「政府資安資訊分享與分析中心(Government Information Sharing and Analysis Center, G-ISAC)」，作為政府的資安資訊交流與情資分析處置平臺。

第四階段為2013年至2016年，目標為「加強資安防護管理二線監控機制與資安情報分享」，此階段建立了跨機關與部會的資安事件關聯分析機制，以自動化方式掌握政府機關遭受資安攻擊的全貌，並自2013年起每年均挑選政府機關與關鍵基礎設施實施網路攻防演練，以驗證政府機關和關鍵基礎設施對資安事件的通報作業、應變程序與聯防機制。[41]

2016年12月，我國總統於駭客年會HITCON發表了「資安即國安」的政策宣言，將資訊安全的政策提升到了國家安全的高度，行政院依政策指導於隔年提出「8大資安旗艦計畫」，規劃由各相關部門建立能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等8個ISAC。[42]另考量資安情資數量與日俱增，且來源管道越趨多元，於2018年成立「國家資安資訊分享與分析中心(National Information Sharing and Analysis Center, N- ISAC)」，確立情資格式標準化與系統自動化的分享機制，奠定了跨領域即時、精準及完整分享威脅情資的基礎(如圖一)。

我國的 ISAC 除了 2009 年成立的政府 ISAC 外，其他的領域 ISAC 均於 2017 年至 2018 年間建置完畢，相較美國雖發展起步較晚，然在規劃過程中充分參考各國資安聯防體系、關鍵基礎設施防護及相關政策的發展經驗，對於 ISAC 的建置規劃具有明確的指導和任務劃分，如 2017 年初的「國家資通安全防護整合服務計畫：領域 ISAC 實務建置指引」中，對於即將成立的能源等 8 個領域 ISAC 及國家 ISAC(N-ISAC)的責任和角色均有所規範，另對於領域 ISAC 的服務項目、本身應有的資安防護要求、情資交換格式也有清楚的律定，使我國的資安

[41]〈國家資通安全發展方案(106 年至 109 年)〉(臺北市)，行政院資通安全會報，2017 年 7 月 11 日，頁 18-22。
[42] 王宏仁，〈蔡英文：資安就是國安〉《iThome》，https://www.ithome.com.tw/news/112836，(檢索日期：2018 年 10 月 4 日)。

威脅情資分享框架能有效運作(如表一)。

圖一 我國政府 2017 年 8 大資安旗艦計畫

資料來源：黃彥棻，〈尋找臺灣資安新動能系列報導：2017 年政府資安預算編列 25 億元，歷年最高〉《iThome》，https://www.ithome.com.tw/news/110923，(檢索日期：2019 年 3 月 11 日)。

表一 ISAC 服務項目參照列表

項次	服務項目	領域ISAC辦理說明
1	資安情資分享	必要項目
2	威脅與弱點分析	必要項目，或與外部組織合作辦理
3	國際交流	可選擇項目
4	資安教育訓練	必要項目，針對關鍵基礎設施領域辦理訓練
5	緊急情況合作	必要項目
6	資安事件通報	可與其他單位或組織合作辦理(領域電腦緊急應變中心
7	資安事件協助處理	可與其他單位或組織合作辦理(領域電腦緊急應變中心
8	資安監控與偵測	可與其他單位或組織合作辦理(領域資安監控中心)
9	其他	由領域ISAC自行評估

資料來源：行政院國家資通安全會報技術服務中心，〈國家資通安全防護整合服務計畫：領域 ISAC 實務建置指引-附件 3〉，2017 年 3 月，頁 10。

此外，行政院國家資通安全會報於2017年7月提出的「國家資通安全發展方案(106年至109年)」中，明訂由行政院資安處與國防部負責執行「建立跨域資安聯防機制」工作項目以下的

子項目-「結合國內產業與民間社群能量，建立國內外公私協防機制」，以提升整體資安防護機制，保衛數位國土安全。而其中分年工作進程計有以下2項：

一、每年參與國內、外重要資安聯防活動或會議，並爭取國內、外資安聯防合作專案，建立互惠機制。

二、持續建立國內、外資安組織聯繫管道，以促進資安情資交流與合作。[43]

而鑒於資訊網路安全對國家的威脅性，已具有從過去的竊取情報逐漸轉化為主動攻擊的趨勢，關鍵基礎設施防護對於國家安全、政府運作、公共安全與經濟民心的穩定有顯著的影響，如關鍵基礎設施遭受破壞，可造成政府失能、社會失序及國防漏洞，儼然已成為我國的非傳統安全威脅，國防部於2017年國防報告書亦將「強化資通電作戰能力，確保作戰指管及關鍵基礎設施安全」納為軍事戰略目標，復於2018年10月令頒「國防網路戰略」，將「確保安全的國防網路環境」列為國防網路戰略目標之一，並將運用國際、跨部會分享機制發揮預警機制，以及推動與各部會、資安機構實施跨區域聯防作為達成國防網路戰略目標的重要手段，以確保國防網路運作。因此，相較於美國國防ISAC及國防工業ISAC的設立，我國雖未成立國防領域相關的ISAC組織，但國防部亦投入資安聯防工作，擔任確保關鍵基礎設施安全的角色和責任。

建置國防領域資安資訊分享與分析中心之重要因素

我國面臨的資安威脅環境與挑戰既艱險又廣泛，綜觀美國與我國ISAC的相關政策起源與發展，美國在2003年國土安全總統7號指令即明訂國防工業為其國家關鍵基礎設施，並由國防部負責業管；而我國的國家關鍵基礎設施安全防護指導綱要僅將能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等8大領域列為關鍵基礎設施，並未納入國防相關領域。[44]面對複雜的國際與兩岸情勢及資安威脅與挑戰，且考量重大政策「國艦國造」與「國機國造」的關鍵研發整合單位如國家中山科學研究院、漢翔公司均未與國防部建立資安聯防機制。本研究即以參考美國經驗，整併其國防領域ISAC及國防工業領域ISAC的功能，由國防部業管，籌建我國的國防領域ISAC，以結合民間國防工業的供應鏈企業，打造資安威脅情資互享與早期預警的平臺。以下就國防領域ISAC建置的重要因素分為作業人力素質、情資分析機能、系統安全措施及情資分享策略等四個構面提出建議，以為後續建置之參考：

一、作業人力素質

人力素質為資安單位運作的基礎，一位專業的資安人才，首先要具備的就是縝密的思考能力，才能在複雜的軟體平台、硬體設備及網路系統的多項活動紀錄中找出異常徵侯及攻擊

[43] 同註 41，頁 37。
[44] 同註 13，頁 3。

態樣，同時還須兼具抗壓耐力，方能以積極主動的態度和縝密的邏輯能力來分析與應對即時的資安狀況。[45]此外，我國「資安管理法」已於2018年5月11日三讀通過，[46]資安人員除了必須隨著資安技術與產品的推陳出新，吸收各種最新的攻擊手法及防禦技巧外，更必須具備相關法律之觀念。為了推展ISAC的資安工作，適當的配置專責資訊專業人力與投入經費資源實屬必要，並透過管理階層實施適當的授權與權責區分，才能提升整體資安工作執行的品質及績效。[47]針對國防領域ISAC的作業人員應具備的資安素養，建議如後：

(一)攻擊技術分析能力

在現今面臨的多種網路攻擊手法中，其中最大的挑戰就是面對進階持續威脅(Advanced Persistent Threat, APT)攻擊。APT是針對特定組織所做出複雜且多方位的攻擊，且經常由跨國的駭客來發動，主要針對目標為政府機關，意圖藉此取得特定的國家機密資訊。然而自2011年起，跨國駭客組織開始將攻擊目標自政府機關擴展至大型企業組織，網路攻擊除了造成財務損失，更因個人資料外洩而損失大量的賠償金額[48]。而當攻擊規模再向上提升時，駭客攻擊可能將其能力結合軍事行動，如將目標指向國家關鍵基礎設施，將使損害情況更為複雜，甚至嚴重擾亂政府的應變作為。[49]

從現今受駭案例來分析，APT攻擊通常可分為4個階段程序：

1.引誘使用者：找出目標內部使用者可能有興趣的資訊，並製作出魚叉式釣魚郵件。

2.暗藏漏洞／弱點：在釣魚郵件內夾帶惡意文件或網址，當使用者不小心開啟文件或網址時，攻擊者就能獲得使用者電腦的內部連線。

3.植入惡意程式：一旦內部連線建立，攻擊者將會植入惡意程式至使用者電腦中，該程式使攻擊者可直接或透過遠端中繼站存取使用者電腦的資料。

4.建立秘密通道：惡意程式持續探索使用者電腦並竊取機敏資料，並開啟反向連結，將資料傳到攻擊者指定的外部IP。[50]

各階段的駭客攻擊行為都有其特徵，ISAC的資安人員唯有透過不斷蒐整、紀錄及分析駭客的攻擊行為與態樣，掌握最常利用的系統弱點與行為特徵，建立攻擊行為特徵資料庫，並於每次的事件應變處置後，依據事件分析與數位鑑識成果，進一步優化行為資料庫，以便於往後提早進一步檢測出駭客的攻擊行為和企圖，因應不同入侵手法研擬及制定出相對應的

---

[45] 林宜隆，花俊傑，〈資安攻防人才核心知識領域之探討〉《電腦稽核期刊》(臺北市)，第 22 期，中華民國電腦稽核協會，2010 年 7 月，頁 81。

[46] 〈資通安全管理法三讀通關，條文搶先看〉《iThome》，https://www.ithome.com.tw/news/123362，(檢索日期：2018 年 11 月 29 日)。

[47] 蕭瑞祥，吳振煒，鄭哲斌，〈國安機關推動資安治理現存問題與落差因素分析之研究〉《電腦稽核期刊》(臺北市)，第 30 期，中華民國電腦稽核協會，2014 年 7 月，頁 23。

[48] 季祥，樊國楨，韓宜蓁，〈進階持續性威脅之防護與認知初論：根基於黑暗首爾資訊安全事故及其防禦方法〉《前瞻科技與管理》(桃園市)，第 5 卷第 2 期，國立中央大學，2015 年 11 月，頁 108。

[49] 同註 20，頁 112。

[50] 廖珮君，〈網路攻擊防禦新趨勢-分析 AP、使用者與內容〉《資安人》，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7204，(檢索日期：2018 年 11 月 17 日)。

防禦策略，達到即時防堵與通報之目的。[51,52]

(二)弱點掃描能力

依據ISO27005資安風險管理標準的定義，單一或多個資產內之弱點，可能會造成資產被單一或多個威脅所利用，如果該資產對於組織和企業具有價值，則會進而影響其業務的持續運作。系統內部的弱點可使駭客利用系統的服務功能及存取機制達到所望的目標，而成功的利用弱點必須具備以下3個條件，首先是系統本身具有弱點，其次為駭客對弱點的存取，最後是駭客具備利用漏洞的能力。[53]

各類的資安風險可透過資安人員依據組織內部的資安政策，在系統開發及上線階段，運用弱點掃描工具，及早發現系統缺陷並予以分析，並依照軟體開發商提供的修補建議或運用其他防範措施實施修補，以提升系統開發階段及維運階段的安全管控作為，並降低資安風險。[54,55]此外，我國在「行政院資通安全會報通報應變處理作業流程」中，亦將弱點掃描列入「事前安全防護」階段的必須項目：「應依資通安全防護需要，執行入侵偵測、安全檢測及弱點掃描等安全檢測工作，並訂定系統與資料備份管理辦法，以做好事前防禦準備。」以確保資安防護策略落實執行。[56]

因此，對於ISAC人員而言，在威脅情資的分析過程中，善用弱點掃描的技術可以幫助他們了解設備或整體系統是否存在漏洞，進而提供會員修補弱點的建議，或是協助提供因應對策，確保將弱點所造成的風險損害降到最低。

(三)威脅評估能力

威脅評估能力為攻擊技術分析和弱點掃描兩種能力的結合，再加上ISAC資安人員對於國防領域系統特性的了解。為達到早期預警的目標，當ISAC收到威脅情資後，需針對攻擊手法予以分析，再依照國防組織或國防產業相關企業的系統特性，找出可能被滲透的弱點，如此才能有效評估該筆威脅對於系統、產業、乃至於軍事單位的影響程度與範圍，並準確判斷各項通報情資的優先順序和急迫性，進而達到情資研析和分享的效果。

(四)系統監控與管理能力

當ISAC所屬系統完成建置後，必須確保其運作必須符合相關的法規要求、契約義務或是組織決策者所界定的管控措施及各項決定。在作業上，系統管理人員管理系統的部署、組

---

[51]〈資安事件防禦與應變能力〉《資安人》，https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=8687&pages=2，(檢索日期：2018 年 11 月 17 日)。

[52] 同註 45，頁 84。

[53] Jeff Hughes, George Cybenko, “Three Tenets for Secure Cyber-Physical System Design and Assessment,” Cyber Sensing 2014 Proc. Of SPIE Vol.9097, 90970A, 2014, p.3.

[54] 陳則仁，〈弱點掃描網站服務之分析與應用〉(臺北：大同大學資訊經營研究所碩士論文，2017 年)，頁 10。

[55] 林志聰，〈使用程式碼安全檢測改進軟體品質：以國稅再造專案為例〉(桃園：健行科技大學碩士論文，2014 年)，頁 35。

[56]〈國家資通安全通報應變作業綱要〉《行政院國家資通安全會報》，https://www.nicst.ey.gov.tw/News_Content.aspx?n=626B7A2643794AB0&sms=C43ECA251722A365&s=612B40E3812D5F2D，(檢索日期：2018 年 11 月 17 日)。

態、維護和監控，如變更管理、容量管理、備份管理、日誌管理、軟體管控及更新等作業，系統管理人員需肩負起系統維運的責任，並依組織的維運政策及管理架構，確保所有管控措施均依規定執行，如透過監控系統日誌、事件記錄、網路流量變化或各項程序運作等手段，分析、判斷異常徵侯並即時反應，以人為監控及管理彌補系統在技術上無法克服的缺陷，確保系統持續正常運作並提供服務。[57,58]

二、情資分析機能

ISAC作為各類資安威脅情資的交換與匯集組織，必須先行了解其所屬會員的資訊需求，並評估當前資訊是否需要進一步的分析和驗證作業，或是否需結合其他額外的知識，以及是否應該與其他領域的ISAC共享。此外，依據分析的結果，ISAC尚需評估受威脅的目標與群體，並擬定防護措施建議，以做為資安情資分析的產製結果[59]，以下就ISAC的情資分析機能提供3點建議：

(一)發揮早期預警功效

企業與組織對於惡意程式攻擊的資安防護措施包括：建立早期預警系統、監控可疑網路連線及主機活動、布建資安防禦縱深、對內部機敏資料建立監控機制與存管政策，以及企業或組織內部應定期執行社交工程攻擊演練等作為。[60]而其中惟有早期預警機制具備最充分時間，提前消弭或降低資安風險。

而針對早期預警的資訊內容，國防領域ISAC應分享給國防產業研發整合單位及相關民間企業的預警情資，應包含：已知的網路或系統的脆弱性與弱點、有關進行中的攻擊事件或潛在威脅之預警(但不提及受害單位)，以及因應特定攻擊型態的策略等3項。如此才能達到早期預警的功效，有助於其他單位或組織先期作好防範未然的工作。而在預警情資中不提及受害單位，可改善國防領域ISAC所屬會員因考量名譽受損進而對受害事件不予通報的心態，不僅對受害單位有所保護，亦加強主動通報的意願，進而提升預警與聯防的效果。[61,62]

(二)提供防護對策建議

在網路發達且資訊快速流通的現代，對ISAC這樣的資安單位而言，可能每日都得面對大量的資安更新訊息、資安新聞、資安攻擊手法等訊息發布，ISAC資安人員需對相關資安資訊進行驗證，整合最新資訊與其他知識分析並產生成果。再依據分析結果來判斷威脅影響與

---

[57] 同註 41，頁 153。

[58] 簡華慶，〈網路資訊戰所扮演角色及因應策略之研究〉《國防雜誌》(桃園市)，第 27 卷第 1 期，國防大學，2012 年 1 月，頁 137。

[59] 黃俊泰，〈美國關鍵基礎設施防護(CIP)建構資訊共享環境之研究〉(臺北：國立臺灣科技大學碩士論文，2017 年)，頁 126。

[60] 吳嘉龍，〈針對勒索病毒惡意程式攻擊網路風險管理與資訊安全防護技術研究〉《危機管理學刊》(高雄市)，第 14 卷第 2 期，中華民國危機管理學會，2017 年，頁 29。

[61] Arnaud De Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michele Ledgerwood, “Cyber Threats and Information Security: Meeting the 21st Century Challenge,” Centre for Strategic & International Studies Press, 2001, p.15.

[62] Farn.K.J., Fung.A.R.W., A.C.Lin, “Recommendation of information sharing and analysis center,” Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003, p.169-174.

風險，設計、擬定適切的對策或管制機制，甚至考量防護對策所產生的額外作業成本是否高於風險發生所須付出的代價。如此，方能在資安事故發生前，針對可能發生的營運衝擊規劃有效的防護措施，並對相關可能受威脅單位或組織提出建議對策，而在事故發生時，ISAC所屬會員才儘速處置，控制住可能的災害損失。[63,64]

(三)運用人工智慧

人工智慧的發展協助資安領域開闢新的前景，可協助資安人以自動化的方式處理重複性的工作，如歸納與分析大量的資料。一旦將人工智慧技術導入資安防護系統，便可將基礎的資安任務交由人工智慧來處理，如資產收集、資產驗證、稽核、合規性(Compliance)、資通安全事件與後續追蹤等。而ISAC的專業資安人員便可專注在困難度或重要性較高的任務上，如更重要的資安風險與重大事件的細部分析，抑或是防護對策的規劃與設計，以提高運作效益。[65]

三、系統安全措施

隨著企業與組織營運對於資訊系統的倚重，資訊系統已成為企業與組織的重要資產，系統的安全性亦逐漸受到重視，為了符合組織的資訊安全政策及維持組織的正常營運，防範資訊與系統免於多種威脅的攻擊，確保資訊的機密性、可用性及完整性是極為重要的。資訊系統上所有保護資訊處理與交流的機密性、完整性與可用性手段均可視為資訊系統之安全性。[66]就國防領域 ISAC 而言，為維持迅速的預警機制、針對國防組織或國防產業相關企業的系統特性評估威脅並提供有效的防範對策，在處理、蒐集與分析各項資安情資的過程中，可能觸及所屬會員的營業祕密、個人資料、系統或資安架構的弱點與參數、研發或生產的關鍵數據與資料，甚或是軍事機密。因此，國防領域 ISAC 本身的平臺亦可能成為惡意人士攻擊的目標，其系統安全措施及相關管控作為，對於確保國防領域 ISAC 的功能發揮及所屬成員的資訊安全都顯得至關重要。我國的領域 ISAC 實務建置指引中，雖未將國防領域列入適用對象之一，亦將系統安全列為 ISAC 平臺維運管理的重要項目之一，[67]以下就系統安全措施提出幾項建議：

(一)導入安全軟體發展生命週期

安全軟體發展生命週期(Secure Software Development Life Cycle, SSDLC)是將安全因素植入傳統軟體開發的各個階段中，將軟體發展生命週期劃分為6個階段，分別為需求

[63] 許建隆，〈以資安聯防構築完整金融資安防護〉《台灣銀行家雜誌》(臺北市)，第 95 期，台灣金融研訓院傳播出版中心，2017 年 11 月，頁 15。
[64] 蔡淑蘭，〈關鍵基礎設施情資分享-美國之例與我國未來方向〉《科技法律透析》(臺北市)，第 29 卷第 7 期，資訊工業策進會科技法律研究所，2017 年 7 月，頁 36-37。
[65] 黃勝雄，〈數位安全發展與建議〉《國土及公共治理季刊》(臺北市)，第 5 卷第 4 期，國家發展委員會，2017 年 12 月，頁 49。
[66] 林錦俊，〈滲透測試於委外資訊系統安全性驗證之研究〉(臺北：國防大學管理學院碩士論文，2008 年)，頁 9。
[67]〈國家資通安全防護整合服務計畫-領域 ISAC 實務建置指引-附件 3〉(臺北市)，行政院資通安全會報，2017 年。

(Requirement)、設計(Design)、開發(Development)、測試(Testing)、驗收(Acceptance)、維運(Deployment/Maintenance/Disposal)等6項，並在每個階段中，由資安人員參與技術及行政上的決策，執行必要的稽核、監控與測試，確保軟體在開發過程中即導入安全性的思維，進行安全性的分析、規劃設計與執行安全控制措施，以達到軟體安全的目標。[68]而非當軟體完成開發後，才開始考慮處理系統安全性、漏洞和風險等議題的補救措施。

我國行政院亦於2013年將「推動政府組態基準及訂定安全軟體發展生命週期(SSDLC)參考指引」列為「國家資通訊安全發展方案(102年至105年)」的重點工作項目，[69]並將SSDLC的概念納入於「資訊系統委外開發RFP資安需求範本」，做為政府機關於資訊系統委外工作，訂定建議徵求說明書(RFP)時，系統資訊安全需求之參考依據。[70]

(二)強化機密資料防護

資訊機密性係為使資訊不可用或不揭露給未經授權之個人、個體或者團體，以保護資訊不被非法存取或揭露。由於 ISAC作為領域情資交流的中心，所獲得的情資可能涉及企業的商業機密、個人資料及其他可能影響商譽的資訊。因此ISAC能否有效的確保資訊的機密性，對於所屬會員的情資分享意願，以及其他企業、組織加入體系的意願均有重大的影響。為妥善防護機密資料，組織必須具有完整的考量和規劃，針對資料的內容和影響性完成分級標示，並律定每個等級資料的對應防護措施及作為，相關的手段有存取與驗證機制、檔案與傳輸加密、資料銷毀、備份、活動紀錄保存、實體環境與硬體的防護、內容去識別化等，透過整體的考量和統一的規劃，確保機密資料都在安全的框架運行並符合政府機關相關的資安法規。[71]如此，方能增進領域所屬會員對於ISAC的信任，加強主動提供威脅情資的意願。

(三)採用共通準則評估採購設備

共通準則(Common Criteria, ISO/IEC 15408)為進行資通安全產品評估及驗證時所遵循之共同標準，依其定義之評估保證等級(Evaluation Assurance Level, EAL)判定產品之安全等級，EAL共有7個等級，最低等級為EAL1，依序至最高等級為EAL7，以作為評估及驗證資通安全產品安全性與功能性之依據。共通準則所驗證的內容涵蓋資通安全產品發展的整個過程，橫跨初期產品設計(Design)、生產(Production)、交付(Delivery)及運作(Operation)等不同階段。而所驗證的安全程度係依據申請者所提供產品安全功能之評估保證等級(EAL)，證明申請者宣稱其資通安全產品可達之功能等級，其驗證結果可作為公司或組織內涉及安全事務的相關人採

[68] 陳振楠，伍台國，林宜隆，廖繹敦，〈威脅模型風險評估機制之建構於安全軟體開發生命週期探討〉(高雄：第二十三屆國際資訊管理學術研討會(ICIM2012))，2012 年 5 月 9 日，頁 4。
[69] 同註 41，頁 21。
[70] 行政院國家資通安全會報，「資訊系統委外開發 RFP 資安需求範本」文件開放下載，2016 年 7 月 5 日公告，https://www.nicst.ey.gov.tw/News_Content3.aspx?n=E8A3CADF59C2DC49&sms=C254FFD10CAFF809&s=2054A0D4623FA608，(檢索日期：2018 年 12 月 3 日)。
[71] 同註 58，頁 137。

購或架設系統時的安全參考文件，以保障系統擁有者及使用者的基本資訊安全。[72]

共通準則(Common Criteria)對於系統的發展及資安產品的採購是有用的導引，可協助評斷廠商所宣稱的安全性和其實際可以達到的安全狀況。而我國政府亦於2009年起開始對於通過共通準則認證之產品優先選購採用。[73]因此，ISAC系統設計團隊在完成系統規劃後，對於系統的組成設備可參考共通準則的指標，審慎選擇要採購的資安設備，確保所獲得的產品能夠符合系統整體規劃的目標及資安防護需求。

(四)定期實施稽核

資訊系統稽核係透過檢查和評核組織內資訊系統的日常運作和慣例，檢核該系統是否合乎組織資安政策的要求，包括安全性、資料完整性、運作效率等，並依稽核結果適時地提供改進建議，以合理確保組織的資安政策得以持續且有效的實施。[74]定期的稽核除了能檢核ISAC系統是否符合組織的資安政策外，以可做為評估資安政策運作是否有效的參考，亦可提早發掘資訊安全管理的風險因子，利於因應作法的擬定並及早改善。

四、情資分享策略

現今資安威脅情資的數量既龐大且複雜，相互分享有助於機關或組織應對並從中找出聚焦的重點，掌握資安事件的全貌。因此，機關或組織不僅需要具備蒐集資安威脅情資的能力，更要有情資分享能力，與其信任夥伴分享資安威脅情資，建立情資分享策略，以共同防禦網路威脅[75]，以下就威脅情資的分享策略提供數點建議：

(一)結合國防產業供應鏈

隨著產業環境的資訊化，經過分析近年來的網路攻擊趨勢，發現相同產業之業者所遭受的網路攻擊手法與模式往往具有高度的關聯性。而網路犯罪者也常鎖定特定產業目標做為目標，攻擊手法也常就產業的特色及產業對於資訊科技的共同應用來進行針對性之設計。因此，有必要結合產業內的資安情資作分享。[76]而美國亦於2003年的「確保安全網路空間的國家戰略(The National Strategy to Secure Cyberspace)」提出，網路空間的威脅來源對象非常廣泛，如可能是恐怖分子、犯罪團體或是某個國家，同時社會依賴網路的程度日益增加，處理網路安全問題已非單一政府部門或機關組織可以獨立處置，必須擴大政府與私人企業的合作來

[72] 楊麗貞，〈以共同準則落實資訊確保之探討-以S壽險公司之「旅行平安險網路投保系統」為例〉(臺北：淡江大學碩士論文，2006 年)，頁 12。
[73] 董重華，〈以 CNS15408 為基礎建構資訊設備安全評估模型之研究–以防火牆為例〉(臺北：中國文化大學碩士論文，2012 年)，頁 5-13。
[74] 林益正，〈以資安保證因應個資法衝擊〉《資訊安全通訊》(高雄市)，第 16 期第 3 卷，中華民國資訊安全學會，2010 年 7 月，頁 154。
[75] 陳建智，詹偉銘，鄭棕翰，黃秀娟，張光宏，周國森，〈一種利用網路流量資訊擴展網路威脅情資的系統〉《前瞻科技與管理》(桃園市)，第 6 卷第 2 期，國立中央大學，2016 年 11 月，頁 64。
[76] 趙龍，〈如何因應近年來常見的資安威脅〉《證券服務》(臺北市)，658 期，臺灣證券交易所，2017 年 4 月，頁 10。

有效應對網路安全威脅。[77]

因此，國防領域ISAC必須運用策略，強化與民間組織產業的合作，提升國防產業供應鏈中的相關成員願意加入及自願提供威脅情資的意願，孰悉領域資訊系統的特性，使ISAC有效掌握威脅情資，並迅速分享給其他國防領域的會員，整合解決產業共同的資安問題，降低每個組織所承受的資安風險。[78]

(二)建立情資分級存取制度

威脅情資的內容本身或許具備一定程度的機敏性，如涉及受駭單位的系統架構、商業機密、個資隱私甚至是國安議題，不一定適合ISAC所有會員存取參用。因此，在威脅情資分享的過程中，必須依照情資的機敏性和影響程度來標示保護措施級別和限制可授權存取的對象。目前我國及各國資安組織大多使用紅綠燈協定(Traffic Light Protocol, TLP)來標示威脅資訊所需的保護措施級別和授權存取限制。TLP是由國際資安事件緊急應變小組(FIRST)所定義，由獲得授權的威脅情資接收者使用，並使用四種顏色來表示不同程度的敏感度和相對應的共享資訊注意事項。其中紅色代表情資接收者原則上不得分享，僅在原始資料已被公開的場合做分享；橙色是接收者僅能在組織內部必要的範圍內進行分享；綠色是可於組織內部和合作夥伴分享，但不得公開分享；白色是得任意分享，不受限制。[79]

我國的電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team & Coordination Center, TWCERT/CC)於「企業資通安全事件通報應變作業綱要」中，亦運用TLP定義做為資安事件通報情資分享的分級存取限制標註，並明定在通報情資分享前將與通報單位或當事人確認通報內容與分級存取限制標註是否合宜，確認無誤後始能分享予第三方單位參考運用，[80]以避免威脅情資分享作業引起不必要的洩密風險和其他負面效應。

(三)暢通情資交流管道

國防領域ISAC可和不同性質的資安組織建立交流管道，如國軍現有的資安監控中心(Security Operation Center, SOC)和電腦緊急應變中心(Computer Emergency Response Team, CERT)分別負責國軍內部資安事件的監控、通報與應變工作，國防領域ISAC可和前述單位建立情資交流管道，協助事件分析工作，並彼此間互相回饋訊息，以增進工作效益。此外，國內其他領域的ISAC及國外同性質領域的ISAC，亦是可以建立橫向交流管道的對象，除了威脅情資的交換外，也可適度的共享分析資源與資安工作經驗，提升作業能量，建立廣泛的資安交流網，達到早期預警、早期防處的功效。

---

[77] 陳育正，〈美國網路安全防護經驗對我國網路安全情勢之啟示〉《國防雜誌》(桃園市)，第 30 卷第 3 期，國防大學，2017 年 5 月，頁 80。

[78] 陳宏鈞，〈資訊安全管理系統之資訊分享控制措施及相關實務研究-根基於重要民生基礎建設〉(臺北：中國文化大學碩士論文，2012 年)，頁 24。

[79] 同註 64，頁 36。

[80]《企業資通安全事件通報應變作業綱要》(臺北市：臺灣電腦網路危機處理暨協調中心，2017 年 6 月 30 日)，頁 7。

結論

自從愛沙尼亞網路戰爭發生以來，伴隨著資訊科技的普及化和各領域產業營運的資訊化，資訊安全對於國家和社會福祉的影響亦趨重大，已經到了會嚴重威脅國家安全的程度，其衝擊範圍之廣泛、型態之複雜，實有賴政府與民間組織攜手合作。環顧我國正在「國防自主」的政策指導下遂行「國艦國造」與「國機國造」，當此之際，防護自主產能與研發關鍵文件的資訊安全更顯重要。本文透過探討美國與我國的ISAC起源和相關政策的演進，以及正在面臨的資訊科技轉型與資安威脅，藉此提出參考美國經驗建置我國國防領域ISAC的建議，以及建置國防領域ISAC的重要因素，期望作為後續執行之參考。

國防領域 ISAC 的確立，除了能增加國軍的資安威脅情資獲得管道，進而提升防護作為外，更能結合支援國防的非官方組織與企業，確保我國國防產業供應鏈的資訊安全，最後將整個國防領域的資安預警機制和國家 ISAC 等其他資安機構鏈結起來，打造穩固、暢通的威脅情資交換網路，進而共同防護國家關鍵基礎設施。

參考文獻

一、 《國家關鍵基礎設施安全防護指導綱要》(臺北市：行政院，2018 年 5 月 18 日)。

二、 〈國家資通安全發展方案(106 年至 109 年)〉(臺北市)，行政院資通安全會報，2017 年 7 月 11 日。

三、 〈國家資通安全防護整合服務計畫：領域 ISAC 實務建置指引-附件 3〉(臺北市)，行政院資通安全會報，2017 年 3 月。

四、 《企業資通安全事件通報應變作業綱要》(臺北市：臺灣電腦網路危機處理暨協調中心，2017 年 6 月 30 日)。

五、 Thomas A. Johnson 著，黃文啟譯，《網路安全-捍衛網路戰時代中的關鍵基礎設施(Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare)》(臺北：國防部政務辦公室，2017 年)。

六、 方鴻春，〈我國關鍵基礎建設安全防護〉《清流月刊》(新北市)，2 月號，法務部調查局，2009 年。

七、 季祥，樊國楨，韓宜蓁，〈進階持續性威脅之防護與認知初論：根基於黑暗首爾資訊安全事故及其防禦方法〉《前瞻科技與管理》(桃園市)，第 5 卷第 2 期，國立中央大學，2015 年 11 月。

八、 陳建智，詹偉銘，鄭棕翰，黃秀娟，張光宏，周國森，〈一種利用網路流量資訊擴展網路威脅情資的系統〉《前瞻科技與管理》(桃園市)，第 6 卷第 2 期，國立中央大學，2016 年 11 月。

九、 趙龍，〈如何因應近年來常見的資安威脅〉《證券服務》(臺北市)，658 期，臺灣證券交易所，2017 年 4 月。

十、 United States Government Accountability Office, “WEAPON SYSTEMS CYBERSECURITY: DOD Just Beginning to Grapple with Scale of Vulnerabilities,” October 9 2018.

十一、 Idaho National Laboratory report INL/EXT-06-11464, “Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research,” 2006.

十二、 Arnaud De Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michele Lidgerwood, Cyber Threats and Information Security: Meeting the 21st Century Challenge, New York: Centre for Strategic & International Studies Press, 2001.

十三、 Jeff Hughes, George Cybenko, 2014.“Three Tenets for Secure Cyber-Physical System Design and Assessment”, Cyber Sensing 2014 Proc. Of SPIE Vol.9097, 90970A.

十四、 Bashir Aliyu Yauri, Joshua Abah, January 2016.“Mitigating Security Threats in Virtualized Environments,” IJCSNS International Journal of Computer Science and Network Security, VOL.16, No.1.

十五、 Farn. K. J., Fung. A. R. W., A. C. Lin, “Recommendation of information sharing and analysis center”, Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, ROC.

作者簡介

李建鵬中校，中正理工學院電機系 87 年班、國管指參班 101 年班，曾任電子官、修護組長、通參官、資參官、電戰官，現任國防大學國防管理學院國管中心人力及資訊管理組教官。

狄學謙少校，國防大學理工學院資工系 96 年班、陸軍通資安全正規班 102 年班、國防大學陸軍指揮參謀學院 108 班，曾任系管官、分隊長、電修官、資網官。