2019 年臺灣公共行政與公共事務系所聯合會年會

暨國際學術研討會

以公私協力發展資訊安全的挑戰：以美國資安資訊分享網絡為例

王士胤[1]

摘要

在當今人類社會已十分依賴網際網路的情況下，世界各國已將資訊安全定為重要的發展方向。以美國為例，資安威脅已嚴重影響其商業利益、關鍵基礎設施安全、以及選舉結果的正當性，資安議題已從私部門的問題上升到國家安全的層次。而美國採取的資安策略中，與私部門分享資安資訊被視為是建構健全資安環境的重要基礎，美國政府企圖以公私協力的方式發展資安資訊分享網絡。

本研究以美國的資安資訊分享架構為研究對象，企圖回答美國政府與私部門雙方在資訊分享上的合作情形為何？以公私協力發展此資訊分享網絡將面臨甚麼困難？美國政府是否能有效因應，或是另有策略等問題。本研究發現，美國的資安資訊分享模式與傳統的公私協力有所不同，該模式並非借重私部門的專業，而是以私部門的資訊分享組織為中介，來傳遞政府部門所掌握的資安訊息；另一方面，在面臨私部門缺乏分享資訊的積極動機的情況下，美國政府當前的政策以擴展資訊分享網絡為優先，鼓勵私部門積極參與分享資訊反而成為次要的政策目標。

[1] 國立暨南國際大學公共行政與政策學系博士生

壹、前言

互聯網(Internet)的快速發展已使得人類社會無法與之分離，包括工業控制系統、金融交易系統、乃至近年興起的物聯網(Internet of Things; IoT)等已融入人類生活之中。互聯網使各國之間的連繫愈來愈緊密，使交易成本愈來愈低，亦使人類的物質生活水準達到前所未有的高峰。

然而，上述之榮景，乃立基於互聯網的正常運作之上，倘若網際網路遭到攻擊而延遲處理資訊，甚至停擺，則將造成國家與社會的不便，甚至危及其生存安全。由於近年來的網路攻擊事件日益猖獗，甚至出現國家級駭客 (state-sponsered hackers)的侵擾，使資訊安全不再侷限於私人公司商業間諜戰的範疇，而進階到攸關國家生存與發展的國家安全議題，因此，促進並改善資訊安全環境已成為各國所發展的重點方向。

以美國為例，根據美國的官方調查，資訊安全事件對個別企業平均每年產生的損失已達 1156 萬美元(中華民國國防部 譯，2017：311)，對美國整體經濟更造成 570 億至 1090 億美元的損失，(The Council of Economic Advisers, 2018:1)，而透過網路竊取商業、國防機密，以侵犯智慧財產權獲利的方式亦成為美國於 2018 年對中共發起貿易戰的重要原因(Office of the United States Trade Representative, 2018)。自美國總統 Trump 上任後，接連採取許多強化資訊安全的作為，包括：將網戰司令部提升為 10 個聯合作戰司令部成員之一、將國土安全部內負責資訊安全的單位，提升為聯邦層級的「網路空間與基礎設施安全局」(Cyberspace and Infrastructure Security Agency; CISA)、發布第 13800 號總統行政命令「強化聯邦網絡及基礎設施的資訊安全」等，皆可看出資訊安全此一議題在美國愈來愈受重視。然而，由於資訊安全不同於一般的安全問題，國家很難單方面提供此一公共財，而許多關鍵基礎設施以及資訊安全公司皆為私部門所有，使美國推行資訊安全的途徑不可避免地必須與私部門建立合作關係。

公私協力夥伴關係(Public-Private Partnerships; 下稱 PPPs)被視為是跳脫「新公共管理」，進入公部門、私部門、第三部門協力合作達到目標的新治理時代(New Governance)。在以往，PPPs 可以將部分非國家必要之職能委託予私部門代為經營，以提供更好的公共服務品質。然而，資訊安全問題的性質不同於過去所委外之公共服務，此問題不僅攸關私部門的商業利益，更嚴重影響國家的安全問題。如今，要將此「安全」問題由國家本職抽離而與私部門合作，便可能產生利益衝突以及課責的問題。因此，目前美國政府與私部門合作最多的部分即為共同分享資訊，較可避免上述的衝突，但亦須面對搭便車(free rider)與公私部門之間的信任問題。

本研究將著重於探討美國公部門與私部門在資安資訊分享上的合作情形，包括雙方合作分享資安資訊的方式為何？美國政府如何因應以 PPP 發展此分享架構可能遇到的挑戰？以及美國政府以 PPP 的方式發展資安資訊分享的特點。以求一窺美國資安分享的圖像，並做為我國未來發展資訊安全之參考。

貳、文獻探討

一、公私協力夥伴關係(PPP)的起源及發展

PPP 的興起源自新公共管理(New Public Management; 下簡稱 NPM)發展到新治理(New Governance)的公共行政學科典範。1970 年代的全球經濟危機，凸顯了凱因斯主義經濟政策的缺陷，政府無法處理失業率及通膨率等「雙率上升」的現象，使主張「回歸市場機制」的新自由主義興起。與此同時，行政機關的效率低落亦使得公共行政學界開始思考如何結合新自由主義的精神，以改革政府的行政部門。其結果便是將市場機制引進公共管理之內，政府部門開始重視績效管理、競爭概念以及將部分服務外包，或國有企業民營化，Savas 甚至列舉了 14 點(Savas, 2000: 111-112)公部門的缺點以支撐其民營化的論述。而 NPM 也確實對改善公部門效率、促使公部門體系的改善達等到了顯著的效果(Morgan & Shinn, 2015: 4)。在上述認為政府機關的角色定位應為「掌舵而非划槳」的情況下(Osborne & Gaebler, 1993: 34)，便開啟了私部門進入公共決策、提供公共服務的新發展方向。

NPM 雖然為政府部門帶來效率，但是依然有其缺陷。首先，NPM 所參考的的私部門績效考量，乃立基於交易利潤、投資報酬、市場利益等物質因素上。但公部門要考量的尚有公平、維護民眾權利、行政透明等價值性問題，而這是純粹利潤考量所無法顧及的(Morgan & Shinn, 2015: 4-5)；其次，NPM 被視為是新自由主義的招牌，Larsen 即認為「以 NPM 改革行政組織」只是政治人物為其利益而喊出的口號，而此口號的背後即為美國自由主義對政府的看法—政府應該縮減規模(Larsen, 2015: 126-127)，NPM 變成是信仰的口號；最後，NPM 認為小政府才是好的政府，但並沒有討論到政府的角色定位為何，例如夜警國家如何在稅收極小化的情況下負擔安全任務等問題，NPM 沒有討論到的複雜角色問題，便由新治理論述來回應此空缺(陳敦源、張世杰，2010：19)。

有別於著重「競爭」的 NPM，新治理更重視「協力」(collaborate)，由過去將私部門管理方式引進公部門組織，轉為公、私部門與第三部門的合作，即為公私協力夥伴關係(Public-Private Partnership; PPP)。此關係是建立在網絡的治理之上，由於公共問題日益的複雜化，使得公部門已無法單獨解決問題，而新公共管理的缺點浮現之後，公部門亦發現已經無法回到過去行政機關獨裁治理的時期。因此，公部門發現自己必須開始與其他部門合作，才能有效解決公共問題，也因而進入了網絡治理的概念(陳敦源、張世杰，2010：34)。

上述公共行政學科典範的背景直接造成了「必須以 PPP 發展資安資訊分享」的原因。新公共管理時期主張引進的私人企業管理，使得美國大規模地民營化其關鍵基礎設施，到了 2014 年，已有大約 90%的關鍵基礎設施是由私部門所擁有或營運(Singer & Friedman, 2014: 15)；當公共行政典範邁入新治理時期，白宮、DHS 等美國政府部門便開始提倡與私部門協力合作，以達到資安治理的目標(The White House, 2018; U.S. DHS, 2018a)。

二、公私協力發展資訊安全的源頭—關鍵基礎設施防護

對於公、私部門合作發展資訊安全的討論，始於關鍵基礎設施的保護。不同於以往的 PPPs，關鍵基礎設施防護的範疇已涉及有關國家安全事務，由於美國的關鍵基礎設施已大部分由部門擁有或營運(Singer & Friedman, 2014: 15)，使美國政府必須以 PPP 的方式來推動關鍵基礎設施的防護。

美國前總統 Clinton 在 1996 年意識到關鍵基礎設施可能成為恐怖攻擊的目標後，便下達第 13010 號行政命令以成立「總統關鍵基礎設施防護委員會」，並簽署第 63 號總統決議案，要求美國政府在 5 年內建構國家防護關鍵基礎設施的能力。在上述的總統命令中，要求加強基礎設施的實體及網路系統(中華民國國防部 譯，2017：52-53)。此階段的資訊安全僅為關鍵基礎設施防護的一個子項目。而上述之防護委員會，即已包含關鍵基礎設施營運代表(Givens & Busch, 2013: 40)，可視為發展關鍵基礎設施防護最初始的公私夥伴關係(Cavelty & Suter, 2009: 181)。

2001 年發生的 911 事件為關鍵基礎設施防護的重要轉捩點，在恐怖攻擊發生之後，美國政府意識到其關鍵基礎設施遭遇攻擊的風險遠高於其原本的判斷，因而不斷加強此方面的防護，包括成立國土安全部(Department of Homeland Security; 下簡稱 DHS)、通過「美國愛國者法案」、下達第 7 號國土安全總統指令及第 21 號總統政策指令等，逐步律定了關鍵基礎設施的主管機關及其職責，並明確列出 16 項關鍵基礎設施，以確定防護標的，(中華民國國防部 譯，2017：53-57)。

而在上述的各項政策指令中，皆提到資訊分享為發展關鍵基礎設施防護 PPPs 的關鍵要素，故有許多針對此部分的研究。有的研究指出，以 PPP 的途徑發展類似的國土安全防護有其優點，包括更有效率地聘僱人員，應用私部門的人力、技術、創新等專業資源，並建立公私互信(Busch & Givens, 2012: 7-8)。另一方面，亦有許多研究指出 PPP 在此領域面臨的許多挑戰，包括公、私部門的利益不一定相符(Dunn Cavelty & Suter, 2009: 181; Carr, 2016: 58)；分享漏洞資訊可能會造成私部門的損失(Dunn Cavelty & Suter, 2009: 181; Carr, 2016: 58)；甚至可能引來政府管制(Branscomb & Michel-Kerjan, 2006: 398) ；相反地，若持有相關資訊而不與其他私部門分享，將可提升其市場的競爭地位，因為其他私部門將無法擁有後進的優勢(Branscomb & Michel-Kerjan, 2006: 398; Carr, 2016: 58)。而政府部門則需面對機密資訊是否與私部門分享(Prieto, 2006: 414; Carr 2016: 59)；以及解決搭便車(free rider)的問題(Gallaher, Link & Rowe, 2008: 76)，亦有提出通報獎勵與參與收費，以解決搭便車問題的觀點(Vakilinia & Sengupta, 2017)。

參、研究方法與架構

一、研究方法

本研究的方法為文獻分析法，透過爬梳過往研究者之成果、美國政府官方文件、美國國土安全部以及其它資訊分享組織的網站文獻、報告等。以勾勒出美國資訊安全分享的網絡圖像，並檢視美國政府以 PPP 的方式發展資訊分享所遇到的困難，以及美國政府如何因應。

二、本文架構

本文將分五個部分，第一部分即為前言，介紹當今網路威脅發展之背景即美國政府的政策方向；第二部份為回顧 PPPs 的發展與理論，以及資安資訊分享的研究緣起及討論；第三部分為介紹當前美國資訊安全的資訊分享架構；第四部份為當前美國資安資訊分享所遇到的挑戰，美國政府的作為，以及本研究之分析；第五部分為結論。

肆、美國資安資訊分享架構

網路空間與基礎設施安全局(下稱網安局) 為負責建構美國政府機關資訊安全能力的聯邦單位。該單位不僅需負責聯邦、各州、地方等政府單位的資訊安全，亦需與國內其它利害關係行為者合作，包括關鍵基礎設施業者、資訊安全公司及其他私部門。而其中最重要的合作方式即為分享資安資訊，以下將介紹網安局的資安資訊分享架構(CISA, 2018)：

一、政府部門

(一)、資安資訊分享與協作計劃(Cyber Information Sharing and Collaboration Program; CISCP)

國土安全部的整體資安資訊分享架構主要是建立在 CISCP 計劃之上，該計劃主要目的為建立聯邦政府與關鍵基礎設施擁有者或營運者之間的資安資訊分享，並進一步建立雙方之間的信任與合作關係(U.S. DHS, 2017)。參加成為 CISCP 的計劃不需要花費任何費用，僅需簽署合作研究與發展契約(Cooperative Research and Development Agreements)，即可成為此計劃之參與者，並接收自網安局分享之資安訊息。

依據上述計劃需要，DHS 將過去資安相關情報單位整併至國家資安及通訊整合中心(National Cybersecurity and Communications Integration Center; 下稱 NCCIC)，以接收、辨識、整合、傳達各部門所通報的資安訊息(U.S. NCCIC 2018)。美國的資訊安全分享是以 NCCIC 為中心，NCCIC 與其他資訊分享夥伴

合作，如 ISACs、ISAO、SLTT 及其他單位等，各單位通報漏洞、威脅、惡意程式等資安相關資訊之後，由 NCCIC 統一彙整、確認資訊真偽後，再分享給其合作夥伴。如今，NCCIC 為網安局的下轄單位，其主要業務除了分享資安資訊之外，亦辦理資安教育訓練與演習、評估資安漏洞與風險、蒐集並分析資料、規劃並協調任務的執行、以及回應資安事件與事後復原(U.S. NCCIC, 2018: 10)。

(二)、國土安全資訊網絡(Homeland Security Information Network; HSIN)

除了上述以 NCCIC 為中心的資訊分享網絡之外，DHS 亦建構 HSIN 此一資訊分享網絡。其中除了關鍵基礎設施業者及其它私人部門外，尚包含州、地方、部落、領地等(State, Local, Tribal, and Territorial; SLTT)聯邦層級以外的地方政府部門，透過 HSIN 所分享的資訊則不限於資訊安全，尚包括關鍵基礎設施防護、緊急救難管理、蒐集情報、公共衛生等。透過 HSIN，DHS 可將其資訊分享網絡擴展至 SLTT 等地方政府，間接使 ISACs 或 ISAOs 等私部門組織獲得地方政府的資安資訊。

二、非政府部門

除了上述 DHS 所成立的 NCCIC 之外，民間部門亦有半自主[2]成立的資訊分享組織，即訊息分享與分析中心(ISACs) 及訊息分享與分析組織(ISAOs)。成立資訊分享組織的概念源自保護關鍵基礎設施的用途，尤其在 2001 年的 911 事件之後，許多 ISACs 紛紛成立，突顯其原本用以反恐之目的(U.S. General Accounting Office, 2004: 7)。如今，既有的美國關鍵基礎設施資訊分享的架構使 DHS 的資訊安全分享網絡得以建立在成熟的基礎之上，此二種組織亦為美國政府以 PPP 的方式發展資安資訊分享的重要合作對象。以下將就 ISACs 及 ISAOs 進行介紹。

(一)、資訊分享與分析組織(Information Sharing and Analysis Centers; ISACs)

ISACs 的全名應包含 Sector Based，意指此類組織是以產業別為成立的單位。各產業設立 ISACs 的動機源自於 1997 年的第 63 號總統指令(PDD-63)，聯邦政府要求關鍵基礎設施業者應成立 ISAC 以與美國政府分享相關安全訊息(National Council of ISACs, 2019a)，故從下表一可看出 ISAC 皆可對應至美國關鍵基礎設施的類別。目前有 20 個產業的 ISACs 加入國家資訊分享與分析委員會(National Council of ISACs; 下簡稱 NCI)，NCI 為各 ISAC 所組成的非營利團體，其領導階層由 ISACs 中的成員所擔任。

---

[2] ISACs 是源自於 1997 年第 63 號總統指令(PDD-63)，ISAOs 是源自年 2015 年第 13691 總統行政命令(EO 13691)，由於其成立皆為政府倡導，政府亦支持其部分營運經費(U.S. General Accounting Office, 2004: 7)，但兩種組織皆為非營利的名間組織，故本文以「半自主」來描述。

表一 美國 NCI 成員

ISAC 名稱	對應的美國關鍵基礎設施類別
汽車業	關鍵製造業部門
航空業	關鍵製造業部門、交通系統部門
通訊產業	通訊科技部門
國防產業	國防產業部門
天然氣產業	能源部門
供電產業	能源部門、核能部門
緊急救護	緊急救護部門
金融服務	金融服務部門
健康醫療	國民健康與公共衛生部門
健康保險	國民健康與公共衛生部門
資訊科技產業	資訊科技部門、通訊部門
海事	交通系統部門
多層級政府	政府機構部門
國防	國防產業部門
石油及天然氣	能源部門
房地產	金融服務部門
教育與研究	-
零售與醫院	國民健康與公共衛生部門
公共運輸	交通系統部門
水資源	水資源與廢水處理系統部門

資料來源：Critical Infrastructure Sectors，U.S. DHS，2019；Member ISACS，National Council of ISACs，2019b；作者自行整理。

成立 ISAC 最主要的目的，即為分享各產業間安全議題的相關資訊，包括硬體以及網路上的安全威脅，大部分 ISAC 全年無休地待命，使其得以提供即時的威脅資訊給成員。由於 ISAC 多為私部門依其產業別所組成，因此不同的 ISAC 有不同的經營方式。以經費來源為例，有些 ISAC 會向會員收取費用，而會員可依其需求來選擇不同的付費方案，如金融業 ISAC(FS-ISAC)、航空業 ISAC 等(FS-ISAC, 2019; Aviation ISAC, 2019)。有些 ISAC 因為其會員產業高度依賴際網路，也因此較積極發展其 ISAC，如 FS-ISAC 及 Aviation ISAC，除了上述採取使用者付費以發展其組織之外，每年皆舉辦年會，並定期提出資安簡報、研究報告等，FS-ISAC 甚至提供實習機會及獎學金來促進資訊安全的研究發展。但另一方面，亦有部分 ISAC 的營運不甚理想，如食品 ISAC 即因缺乏資訊分享，最後亦終止運作，有學者指出該產業既有的資訊分享網絡已可達到目的，而不需另一個資訊分享組織(Straw, 2008)。

(二)、資訊分享與分析組織(Information Sharing and Analysis Organizations; ISAOs)

除了上述 ISACs 之外，2015 年的總統行政命令亦要求國土安全部部長鼓勵民間建立 ISAO，以促進資安資訊分享。ISAC 與 ISAO 不同之處在於，ISAC 是以產業為成立基礎，如金融業 ISAC、航空業 ISAC 等；ISAO 的成立基礎則包含地域、產業、或其他類別，如加州資安資訊分享組織、小型供應鏈 ISAO、CyberUSA 等(U.S. ISAO Standard Organization, 2019)。

除了一般的 ISAO 之外，DHS 會透過公開徵選的方式來選擇營運 ISAC Standard Organization(ISAO-SO)的單位。ISAO-SO 的主要目標除了作為 ISAO 資訊的彙整與分享中心之外，亦成立不同議題的工作小組，以將有效的作業標準及指引提供給其成員，其中的議題包括促進 ISAO 的設立、改良 ISAO 能量、促進資訊分享、隱私與安全、國際發展、與公部門的關係、改善資訊分析能力等(ISAO Standards Organization; 2019)。

三、美國政府以公私協力發展資安資訊分享的模式

美國政府認為資訊分享是促進關鍵基礎設施安全的重要方向，因而要求關鍵基礎設施相關產業成立 ISAC，並鼓勵成立 ISAO。許多在 CISCP 資安資訊分享計劃之前即已存在的 ISACs 已營運多年，內部已建立起有效的合作機制以及互信。透過此二種既有的資訊分享網絡來分享資安資訊，使美國政府能夠不必重新建構資訊分享網絡，故能更有效地讓私部門及時獲得資安威脅情報。而這也是美國政府以公私協力發展資安資訊分享的模式。

然而，從上述的 ISAC 及 ISAO 的成立背景來看，皆為美國政府先提出成立相關資訊分享組織，ISAC 及 ISAO 才相繼成立。最初的 ISAC 是由各關鍵基礎設施所對應的產業各自成立，而要求其成立 ISAC 的原因，正是因為美國的關鍵基礎設施多已民營化。若上述設施多由美國政府透過國營企業或是其他方式所掌控，則美國政府可自其內部的行政網絡直接下達命令，要求關鍵基礎設施回報資安資訊，毋須特別要求其成立 ISAC。因此，對美國政府而言，以公私協力作為發展資訊分享的方式可說是不得已的。

此外，理想中的資訊分享網絡並非僅由政府部門分享資訊，更需要私部門的參與，透過積極的回報資訊，使整體資訊分享網絡得以獲得更充足且及時的情報。但對私部門而言，便有許多不參與資訊分享並純粹搭便車的理由，本研究便在下一部分討論。

伍、以公私協力發展資安資訊分享的挑戰

上一部分談論到 DHS 資訊分享網絡內的行為者，包括隸屬於網安局的 NCCIC、DHS 主導的國土安全資訊網絡，以及私部門成立的 ISACs 與 ISAOs 等。理想中的資訊分享模式為公、私部門發現程式漏洞、惡意軟體、或遭遇網路攻擊時，便即時回報至 NCCIC，該單位再通知參與資安資訊分享計劃的參與者，而 NCCIC 制定出回應方法以及解決方案之後，再通知各利害相關人。

然而，實際上有許多原因將導致私部門不願意主動分享資訊。若決定分享相關資訊，對該公司不僅無利，甚至可能有害。以下將探討以公私協力的方式發展資訊安全的挑戰，包括私部門可能面臨的難題、資訊分享所帶來的利弊，並檢視美國政府當前的政策方向為何。

一、以公私協力的方式發展資訊安全的挑戰

（一）、關鍵基礎設施業者的難題：追求商業利益或履行國家安全責任

「安全」此一公共財原本是由國家所提供，國家設置軍隊以保護本國不受其他外國勢力的武力威脅，國家成立警察組織以維持社會秩序，國家壟斷了國內的合法暴力的同時，也肩負起維護國家安全的責任。

然而，已大規模民營化的美國關鍵基礎設施，其業者便產生了是否需要強化自身資訊安全的問題。從公共利益的角度來看，關鍵基礎設施的運行支撐著美國社會的正常運作，關鍵基礎設施若是遭到物理或是網路攻擊，都有可能使民眾習以為常的公共服務停擺。因此，為降低關鍵基礎設施遭受網路攻擊而損害的機率，關鍵基礎設施業者自然應改善其資安防護措施，並積極參與資安資訊網路分享網絡；另一方面，以私人企業的立場而言，其最主要的目標便是獲利，並將其商業利益分配給股東，因此，私人企業重視的是成本、效益、投資報酬率等。而改善資訊安全防護，或主動分享資安資訊的成效往往無法立即顯現，使得關鍵基礎設施業主可能不願投入適當的成本以改善其資訊安全防護措施，或主動分享資安資訊。

（二）、私部門主動分享資訊的意願不高

除了上述的問題之外，對私部門而言，主動分享資安相關資訊並不一定能極大化公司的利益，甚至可能有損公司的利益、喪失客戶信任、招致政府的管制等。以下列出幾點私部門可能的顧慮。

1. 分享資訊無利可圖

如前段所述，對私人企業而言，最重要的營運目標為獲利，以對股東負責。因此，私人企業的行為邏輯可從計算其商業利益、市場地位的角度來看。對私人企業而言，資安威脅的資訊在被分享至資訊分享網絡之前是有價值的，

企業若主動分享資訊，則該企業自主發現的程式漏洞或遭受的網路攻擊，將成為其它資訊分享參與者的前車之鑑，難免造成搭便車的情形，而現今並沒有對通報資訊的企業有所獎勵；相反地，企業若不分享資安訊息，並自行發展出解決方案，則可在面臨此資安威脅的情況下領先於同業。因此，在考量分享資訊的機會成本後，私人公司可能會選擇保留該資訊，以確保其競爭地位(Branscomb & Michel-Kerjan, 2006: 397-398; Carr, 2016: 58)。

對於私部門主動分享資訊的意願而言，搭便車的影響特別重要。Gallaher等人透過訪談私人企業負責人，並將結果以經濟學模型呈現，其結果認為私人企業若本身採取積極的資安防護策略，則主動分享資訊可以降低其長期成本。但是受到搭便車者效應的影響，私人企業可能會不願意主動分享資訊(Gallaher, Link & Rowe, 2008: 76-79)。意即，若其他企業將受惠於資訊分享而不需負擔任何成本或分享義務，則握有資訊的企業便不願主動分享，儘管主動分享資訊對該企業長期而言是有利的理性選擇。故 Gallaher 認為政府應設法解決搭便車問題，以鼓勵私部門分享資訊。

2. 主動分享資訊可能損害私部門的利益

除了上述不分享資訊的有利之處，私部門亦將考量分享資訊可能對其利益所造成的損害，而如同美國政府的審計辦公室的報告所言，資訊分享的益處是難以察覺的，但它所帶來的成本與風險卻是可以預見的(U.S. General Accounting Office, 2004: 10)。

首先，若主動分享自身企業遭受網路攻擊之資訊，無異將其遭到攻擊的訊息公告周知，如此便會使供應商、採購商、其它消費者對該公司產生疑慮，對其商譽造成負面影響(Cavelty & Suter, 2009: 181)。而根據美國政府的調查，私人公司公開遭受網路攻擊後，其股價亦可能會下跌，而使其公司市值縮水(Office of the United States Trade Representative, 2018: 174)。

其次，私人公司與其顧客之間常有保密協定，分享漏洞資訊可能將使其必須揭露顧客的身分、採購項目及數量、以及其它商業機密等，而使該公司必須面對法律問題(Branscomb & Michel-Kerjan, 2006: 398)。此外，亦可能揭露企業自身的敏感資訊，例如未遵守法令標準，而引來政府對其實施管制。

最後，揭露資安漏洞資訊，更可能使原本不曉得該漏洞的駭客對其發動攻擊，而吸引來更多的攻擊。如以色列的資安服務業者 Check Point 於 2019 年 2 月公佈某知名壓縮軟體程式存在的漏洞後，便出現超過 100 種對該漏洞進行攻擊的方式(陳曉莉，2019)。Check Point 揭露漏洞的時間是 2 月 20 日，該軟體供應商釋出修補的更新檔是 2 月 28 日，使用者共有 8 天的時間暴露在威脅之下。此案例顯示，在沒有解決方案之前，揭露或分享資安訊息可能會造成更大的資安威脅。

3. 對政府部門缺乏信任

Rosenau 曾經指出公私夥伴關係成功的因素包括：認定關鍵問題並擬定計劃、責任明確、制定可達到的目標、適當的激勵、監控執行過程(Rosenau, 1999: 11-12)。但上述成功的因素是建立在公私部門互相信任的基礎之上。

美國公私部門合作分享資訊的雙方即存在信任問題。從私部門的角度來看，許多 ISAC 認為自己已經提供許多資訊給美國政府，但是對方卻對分享資訊有所保留，使私部門認為資訊分享之前，應將資訊視為籌碼(quid pro quo)，以促使政府部門釋出更多的資訊(Prieto, 2006: 414-415)。此外，對於政府部門的不信任，亦使私部門對與政府部門分享其資訊有所疑慮，尤其在前 CIA 職員 Snowden 揭發美國政府的網路監控計劃之後，更使情況雪上加霜。因此，前 DHS 副部長 Alejandro Mayorkas 在提及此事時，亦承認美國政府與私部門之間尚有鴻溝般的不信任問題須解決(U.S. DHS, 2016)。

另一方面，從政府部門的立場來說，便必須辨別何種密等的資訊可以與私部門分享、分享對象是否有足夠的安全權限得以獲取資訊、以及其是否會將機密外洩(Prieto, 2006: 41)。有些情況下，儘管分享對象具有足夠的權限以獲取資訊，但為了避免情報或是政府的行動曝光，該對象在獲取資訊後依然不能行動(Carr, 2016: 58-59)。

二、美國政府的作為

面對上述各種私部門不願分享訊息的原因，美國政府做出了一些努力。針對分享資訊可能造成的傷害，美國政府將目前的資訊通報機制設定為可匿名通報。各級政府、關鍵基礎設施業者、ISAC 及 ISAO、或其它私部門業者皆可在使用 NCCIC 網站上的通報機制時，選擇是否具名通報資安事件、惡意程式、網路釣魚等，匿名通報的機制，可降低私部門對自身商譽受損的疑慮。而對於私部門認為政府部門分享不足的問題，目前 DHS 則儘量公佈不具機密性質的情報，NCCIC 則定期發佈資安簡報、分析報告、即時威脅通知等。由於在資訊分享的公私合作之上，私部門已經對於政府部門產生不信任，因此，政府部門必須主動且積極地分享資訊，才有機會促進私部門的參與。DHS 認識到開放資訊所帶來的價值，期望藉此提升資訊分享的數量及質量(Prieto, 2006: 420)。

但對於其它問題，例如解決搭便車的情形，美國政府目前仍然沒有解決該問題的方案。事實上，DHS 目前主要的發展方向為擴大私部門的參與數量，而非鼓勵私部門主動分享資訊。由於新自由主義的經濟思想，美國政府並未立法律定關鍵基礎設施維護其資訊安全的責任(Assaf, 2008)，官員甚至認為私部門的資訊安全是其自身的責任，政府部門不應，也無法管制私部門的資訊安全(Carr, 2016: 56)。因此，美國政府的文件提到與私部門分享資安資訊時，其用詞皆為「鼓勵」、「促進」、「自願」，而非「必須」、「命令」。如「鼓勵」私部門「自願」參與資訊分享機制，以「促進」資訊分享(U.S. DHS, 2018a: 13)。而 DHS、

國防部、司法部及國家情報總監則被要求建立資訊分享機制，以與私部門分享資安訊息(U.S. Congress, 2015)。

因此，美國政府未來的資安資訊分享機制，可預見地不會出現強制律定私部門分享資安事件的規定。例如 NCCIC 在其 2017 年的年報中提及未來發展方向時，即明確指出未來的資安事件自動分享系統(Automated Indicator sharing; AIS)將以自願為原則來擴大私部門的參與。AIS 為 DHS 致力建構健全資安環境的一環，此架構可以讓參與的成員得以獲得立即的資安資訊。此架構並不強迫其參與成員分享受攻擊的資訊，分享為自願性而非義務，而資安事件通報者亦可選擇匿名通報與否，使 NCCIC 以外的成員獲得訊息時，不會知道是誰通報資安威脅、是誰受到攻擊。截自 2017 年，已有 184 個參與者加入 AIS，其中包括公部門、私部門、及 16 項關鍵基礎設施的所有業者。而自 AIS 於 2016 年成立之後，已接收並分享超過 140 萬則威脅情報(NCCIC, 2018: 29)。

三、對於政策的分析

對於美國以 PPP 作為推動資訊分享的途徑，本研究認為有部分特點及值得討論之處。包括美國的資安資訊分享模式並非傳統的公私協力；政府單位以擴大私部門的參與為優先目標，而非促進已參與單位的參與程度；以及美國政府與私部門之間尚需建構更穩固的信任關係。以下將針對上述三點進行說明：

（一）、美國資安資訊分享並非傳統的公私協力

本研究在第肆部份即指出，美國政府以 PPP 的方式與私部門合作分享資安資訊，乃源自於 90%以上的關鍵基礎設施皆以民營化，美國政府可說是不得已才與私部門合作。而其合作的方式，為 NCCIC 與各產業 ISAC 及各領域 ISAO 合作分享資安資訊。

從新公共管理到公私協力夥伴關係，其核心意涵皆為納入私部門以解決日益複雜的公共問題。透過借重私部門的積極態度、重視產出、高效率等優勢，來彌補公部門的不足。然而，本研究所關注的美國資安資訊分享 PPP 則不同於上述過往的 PPP，NCCIC 與 ISAC 及各 ISAO 之間的合作，並非借重私部門擅於提供資訊安全服務，或是擅於提供資訊分享的網絡。各 ISAC 及 ISAO 僅為美國政府傳遞資安資訊至私部門的管道，而有鑑於 ISAC 及 ISAO 的誕生皆源自美國政府政策，因此可將此二類組織的誕生視為美國政府為自己創造了傳遞資訊的管道，而非夥伴關係。

（二）、美國政府目前以擴大參與為政策目標

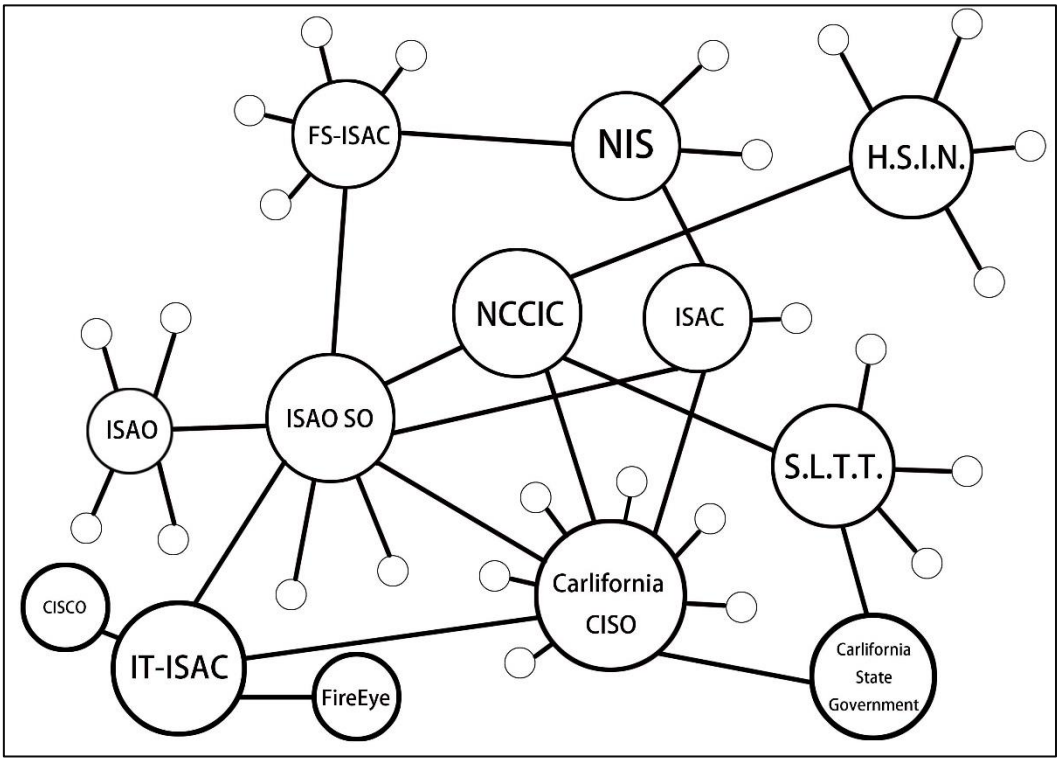
對 DHS 而言，其發展資訊安全的政策目標為降低美國社會的資安威脅。而分享資安資訊等於是向其它公、私部門的單位敲響警鐘，使各部門獲得威脅資訊並著手防範。有愈多的單位參加此架構，則 DHS 建構的資訊分享網絡就愈大，也就愈接近其政策目標。因此，對 DHS 而言，鼓勵私人企業加入資訊分享

網絡，要比鼓勵私人企業主動分享資訊來的重要，且較容易達成，因為加入資訊分享網絡是自願且毋須負擔任何成本及義務的，加入者可以純粹擔任搭便車者，接收資訊。

ISAC 也像是一種同業公會(U.S. General Accounting Office, 2004: 7)，對私人企業而言，參與 ISAC 的目的除了分享與接收產業內部的安全資訊之外，另一種同樣重要的目的可能是與其它企業維繫關係，以顯現自身在維護產業安全環境之上不落人後。同樣地，ISAO 也是同樣的情況。若從關係網絡的角度來看，參與而交流所帶來的效益，並不會低於接收威脅資訊的效益。而對參與者而言，在 ISAC 或 ISAO 所分享的資訊，是與其同業分享，而非直接與政府分享，如此可減輕上述對政府部門缺乏信任的疑慮。

透過上述 ISAC 及 ISAO 所建構的網絡，DHS 只要與此二類資訊分享組織建立資訊分享關係，即可有效擴大其資訊分享網絡，而不需與個別企業達成資訊分享協議。如下圖一所示，ISAC 及 ISAO 的資訊分享網絡將 DHS 下轄的 NCCIC、州政府、以及資安公司(Fire Eye)與網路設備商(Cisco)等私人公司串聯起來，使 NCCIC 的資安情報可以傳遞到更廣的範圍。

圖一 美國資安資訊分享網絡



資料來源：作者自行整理繪製。

對 DHS 來說，加入的單位若主動通報資安事件，則自然對整體資安環境有所幫助；若該單位不願主動分享資訊，純粹作為接收資安事件警報的搭便車者，亦有助於 DHS 達到其政策目標。

（三）、公、私部門之間尚須建構更堅固的信任關係

儘管 DHS 當前以擴展私部門參與資訊分享網絡為目標，但資訊安全確實愈來愈需要私部門的協力合作，尤其在 2016 年美國總統大選出現他國勢力的網路干預後，資安威脅已造成民主政治的危機。也因此，DHS 下轄的網安局已著手準備 2020 年選舉的資安防範，包括設立選舉 ISAC (EI-ISAC)。其它如 Facebook 等經營社群網站的私部門，亦表示願意協助相關的選舉資訊安全問題。

然而，公部門與私部門的合作顯然存在彼此之間的信任問題。以 2018 年美國期中選舉為例，Facebook、Twitter、Microsoft 等資訊業者曾主動召開會議，商討如何避免重蹈 2016 年選舉遭外國勢力干預的覆轍，並邀請 DHS 及 FBI 的相關負責人與會。但在會議中，兩位聯邦政府的代表卻表示他們沒有特定的資訊要分享，與會者甚至以「緊張氣氛」來形容該次會議(Frenkel & Rosenberg, 2018)。可看出公、私部門雙方尚須建構更深的信任關係。

陸、結論

2018 年 3 月 15 日，美國國土安全部公佈了一項網路威脅報告，內容明確指出俄羅斯政府對美國的政府機關、核能、能源、水資源等關鍵基礎設施業者發動網路攻擊(U.S. DHS, 2018b)。由於這是美國政府第一次公開譴責俄羅斯政府對其能源設施的網路攻擊(Atherton, 2018)，故此報告不僅標誌著資訊安全的重要性已上升到國家安全、外交事務的層級，公開譴責更意味著美國有意願，且已有能力採取反制的行動。

本研究的結果指出，美國以公私協力的方式發展資安資訊分享，將面臨些許挑戰。包括私部門基於自身利益的理性考量，而產生許多消極與積極的「不分享」動機。以及公、私部門之間需要更多建設信任關係的工程，以改善雙方進一步分享資訊的意願。此外，根據本研究的觀察，美國政府與私部門之間的資安資訊分享合作並非傳統的公私協力夥伴關係，私部門組成的資訊分享組織更像是美國政府為遂行政策而鼓勵建置的資訊分享管道；最後，在面對上述公私協力分享資訊的挑戰，美國國土安全部當前的政策發展方向以擴展私部門的參與數量，以建構更廣泛的資訊分享網絡為主，要求私部門主動分享資訊反而並非主要目標。

雖然以公私協力的方式發展資訊分享將面臨挑戰，但長期而言，資訊分享勢必有利於公、私部門共同對抗網路威脅。從過去的例子來看，美國許多大型金融公司在 2013 年之前曾遭遇許多阻斷式服務攻擊(denial-of-service; DoS)[3]，而金融資訊分享中心(FS-ISAC)使得金融公司與聯邦政府得以分享網路攻擊的情

[3] 意指駭客透過程式不斷要求被攻擊者的伺服器回應，以耗盡被攻擊者的網路系統資源，進而癱瘓其服務的攻擊手法。

報，並成功抵抗駭客攻擊(Daniel, 2013)；另一個例子則是 FS-ISAC 在 2017 年的勒索軟體 Wannacry 事件中，提供即時的資訊及指引給超過 7000 個會員，使其成功降低了勒索軟體所帶來的損害(FS-ISAC, 2017)。上述例子顯現資訊分享機制確實能達到共同防禦網路攻擊的效果。

今日之人類社會可說是幾乎完全依賴網路，而由於網路空間的性質有別於一般的國家實體領土，國家很難像設立陸海空三軍一般設立武裝力量來保護國內的資訊安全。因此，私部門參與分享資安資訊便成為未來重要的資安政策發展方向。目前除了美國之外，歐盟亦積極以公私協力的方式推動資訊安全，歐盟許多成員國已透過不同的公私協力方式來發展資訊安全(European Union Agency for Network and Information Security, 2018)，可見私部門在未來的資安策略發展方向是不可或缺的。因此，美國當前與私部門合作的資安資訊分享網絡所面臨的挑戰，更值得我們思考其解決之道，以完善整體的資訊安全環境。

參考文獻

專書

Galleher, Michael; Albert N. Link; Brent R. Rowe (2008). ***Cyber Security: Economic Strategies and Public Policy Alternatives***. Cheltenham: Edward Elgar Publishing.

Johnson, Thomas (2015). 網路安全：捍衛網路戰時代的關鍵基礎建設(初版)，中華民國國防部(譯)，臺北市：國防部政務辦公室。

Osborne, David. & Ted Gaebler. (1993). ***Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector***. New York: Plume Press.

Savas, Emanuel (2000). ***Privatization and Public-Private Partnerships***. New York; Seven Bridges Press.

Singer, P., Allan Friedman (2014). ***Cybersecurity and cyberwar: What everyone needs to know***. Oxford: Oxford University Press.

專書篇章

Branscomb, Lewis & Erwann O. Michel-Kerjan (2006). Public–Private Collaboration on a National and International Scale. In Philip E. Auerswald (Ed.), ***Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*** (pp. 395-403). New York: Cambridge University Press.

Larsen, Gary (2015). Forging Vertical and Horizontal Integration in Public Administration Leadership and Management. In Morgan & Cook (Ed.), ***New Public Governance: a regime-centered perspective*** (125-138). New York: Routledge.

Morgan, Douglas & Craig W. Shinn (2015). The foundation of New Public Governance. In Morgan & Cook (Ed.), ***New Public Governance: a regime-centered perspective*** (3-12). New York: Routledge.

Prieto, B. Daniel (2006). Information sharing with private sector: History, Challenges, Innovation, and Prospects. In Philip E. Auerswald (Ed.), ***Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*** (pp. 404-428). New York: Cambridge University Press.

期刊文章

Busch, Nathan E. & Austen D. Givens (2012). Public-Private Partnerships in Homeland Security: Opportunities and Challenges. ***Homeland Security Affairs, 8***(18): 1-24.

Carr, Madeline (2016). Public-private partnerships in national cyber-security strategies. ***International Affairs, 92***(1):43-62.

Dunn Cavelty, Myriam & M. Suter (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. ***International Journal of Critical Infrastructure Protection, 4***(2):179-187.

Givens, D. Austen & Nathan E. Busch (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. ***International Journal of Critical Infrastructure Protection, 6***(1): 39-50.

Rosenau, Pauline Vaillancourt (1999). The strengths and weaknesses of public–private policy partnerships. Wettenhall, Rogger (2003). The Rhetoric and Reality of Public-Private Partnerships. ***Public Organization Review, 3***(1):77-107.

陳敦源、張世杰 (2010)。公私協力夥伴關係的弔詭。文官制度季評，2(3)：17-71。

會議論文

Vakilinia, Iman& Shamik Sengupta (2017, October). ***A coalitional game theory approach for cybersecurity information sharing***. Military Communications Conference, Baltimore, U.S.

網路資源

Atherton, Kelsey (2018, March 28). It's not just elections: Russia hacked the US electric grid. ***Vox Media***, Retrieved March 25, 2019, from https://www.vox.com/world/2018/3/28/17170612/russia-hacking-us-power-grid-nuclear-plants.

Aviation ISAC (2019). Member benefit, tiers, and dues. Retrieved April 17, 2019, from https://www.a-isac.com/copy-of-join-us.

CISA (2018). Information Sharing and Awareness. Retrieved March 25, 2019, from https://www.dhs.gov/cisa/information-sharing-and-awareness-0.

Daniel, Michael (2013). Getting Serious about Information Sharing for Cybersecurity. Retrieved March 25, 2019, from https://obamawhitehouse.archives.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity.

European Union Agency for Network and Information Security (2018). Public Private Partnerships (PPP) - Cooperative models. Retrieved March 25, 2019, from https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport.

Frenkel, Sheera & Matthew Rosenberg (2018). Top Tech Companies Met With Intelligence Officials to Discuss Midterms. Retrieved March 25, 2019, from

https://www.nytimes.com/2018/06/25/technology/tech-meeting-midterm-elections.html.

FS-ISAC (2017). FS-ISAC Tips to Defend Against Ransomware. Retrieved April 7, 2019, from https://www.fsisac.com/sites/default/files/news/WannaCry%20TLP%20Whitepaper%20Ransomware%20May%202017%20FINAL.pdf.

FS-ISAC (2019). Membership Benefits. Retrieved April 17, 2019, from https://www.fsisac.com/join.

National Council of ISACs (2019a). ABOUT ISACs. Retrieved March 25, 2019, from https://www.nationalisacs.org/about-isacs.

National Council of ISACs (2019b). Member ISACS. Retrieved March 25, 2019, from https://www.nationalisacs.org/member-isacs.

Office of the United States Trade Representative (2018). Findings of Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the trade act of 1974. Retrieved March 27, 2019, from https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

Straw, Joseph (2008). Food sector abandons its ISAC. Retrieved April 17, 2019, from https://sm.asisonline.org/Pages/Food-Sector-Abandons-Its-ISAC.aspx.

The Council of Economic Advisers (2018). The Cost of Malicious Cyber Activity to the U.S. Economy. Retrieved March 27, 2019, from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

The White House (2018). National Cyber Strategy of the United States of America. Retrieved March 27, 2019, from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

U.S. Congress (2015). Cybersecurity Information Sharing Act of 2015. Retrieved March 25, 2019, from https://www.congress.gov/bill/114th-congress/senate-bill/754/text.

U.S. DHS (2016). Remarks by Deputy Secretary Alejandro Mayorkas at the 6th Annual International Cybersecurity Conference. Retrieved Apirl 15, 2019, from https://www.dhs.gov/news/2016/06/22/remarks-deputy-secretary-alejandro-mayorkas-6th-annual-international-cybersecurity.

U.S. DHS (2017). Cyber Information Sharing and Collaboration Program. Retrieved Apirl 15, 2019, from https://www.whitehawk.com/sites/default/files/2018-07/CISCP%20Overview.pdf.

U.S. DHS (2018a). DHS Cybersecurity Strategy. Retrieved March 25, 2019, from https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-

Strategy_1.pdf.
U.S. DHS (2018b). Alert (TA18-074A) : Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved March 25, 2019, from https://www.us-cert.gov/ncas/alerts/TA18-074A.
U.S. DHS (2019). Critical Infrastructure Sectors. Retrieved April 17, 2019, from https://www.dhs.gov/cisa/critical-infrastructure-sectors.
U.S. General Accounting Office (2004). Critical Infrastructure Protection: Improving Information Sharing With Infrastructure Sectors. Retrieved April 17, 2019, from https://www.gao.gov/assets/250/243318.pdf.
U.S. ISAO Standard Organization (2019). Information Sharing Groups. Retrieved April 17, 2019, from https://www.isao.org/information-sharing-groups/.
U.S. NCCIC (2018). NCCIC Year in Review 2017. Retrieved April 17, 2019, from https://www.us-cert.gov/sites/default/files/publications/NCCIC_Year_in_Review_2017_Final.pdf.
陳曉莉 (2019)。WinRAR 漏洞被揭露的第一周就有超過 100 種攻擊，2019 年 3 月 18 日，取自 https://www.ithome.com.tw/news/129402。