假訊息之案例分析與行動策略

行政院外交國防法務處處長 譚宗保

隨著網路科技及社群媒體推波助瀾，假訊息氾濫造成世界各國面臨國安、資安及民主法治的挑戰。行政院為因應此嚴峻課題，責由羅政務委員秉成邀集行政院外交國防法務處、資訊安全處、教育科學文化處、科技會報辦公室、內政部、法務部、教育部、通傳會等機關單位，組成專案小組，針對國外比較法制進行研究，並採取符應我國生態體制的行動策略。

川普無論在競選期間或當選後，皆經常指控媒體製造假新聞。

防制假訊息危害（以下簡稱防假）的法制作為，最高指導原則就是秉持多元民主價值、維護言論自由，因此，在法律問責必要性的前提下，使相關法律規範的要件明確化、責任合理化。獨立審判法院是最後仲裁者，有法律保留原則及司法審查原則把關，將可避免侵犯言論自由的範疇。

本文將針對國內外案例及先進國家法制進展介紹，並說明政府提出的防假策略、法制作為及行政措施：

案例分析

一、國際案例

假訊息（disinformation）已成為「數位野火」（digital wildfire），從恐怖主義蔓延到全球治理失敗，恐怖主義及暴力犯罪分子，利用網路平臺，散布假訊息，製造社會恐慌及對立，威脅自由民主發展之根基。

（一）美國

2016 年美國總統大選遭外國勢力以假訊息影響傳言甚囂塵上，牛津大學電腦宣傳專案小組研究揭露，俄羅斯「網路研究局」（IRA）透過社群平臺，製造或轉載假新聞打擊民主黨候選人，暗助川普當選。另川普於競選期間，也數度指控與其意見相左媒體製造假新聞，並指稱為全民公敵。

（二）英國

愛丁堡大學研究指出，2016 年英國脫歐公投期間，俄羅斯被控涉嫌利用 419 個虛假的推特（Twitter）帳號，發布與英國脫歐有關貼文、假訊息，試圖影響脫歐公投結果，干擾英國政治發展。

（三）法國

2017年法國總統大選，俄羅斯駭客與美國極右派分子，試圖以散布大量假訊息方式操弄大選，如謠傳馬克宏在海外擁有祕密帳戶等。牛津大學研究指出，選前法國 Twitter 上政治相關貼文中，1/4 是假訊息，刻意散播「極端意識形態或陰謀論」消息。

（四）瑞典

依牛津網路研究中心發布《Twitter 與瑞典 2018 年選舉》研究報告顯示，所有 Twitter 分享的選舉訊息，有高達 1/3 為假訊息，操作移民議題衝擊選舉結果，使兩大聯盟皆無法取得國會過半數席次，產生國會僵局。

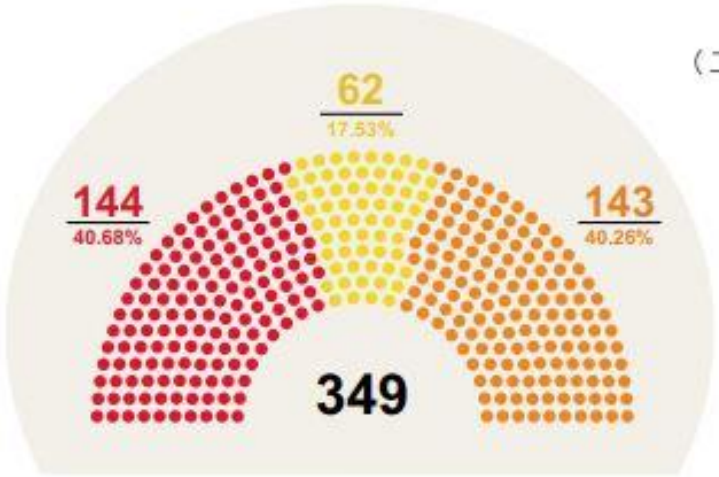
業者以衛生紙漲價的假訊息進行不實促銷，影響交易秩序與消費者權益。（圖片來源：小草，https://www.flickr.com/photos/in_future/40757186332）

二、國內案例

（一）2018年2月底爆發「衛生紙之亂」，業者藉由衛生紙漲價的假訊息，進行不實促銷，影響交易秩序與消費者權益，遭公平會裁罰。

（二）2018 年 823 南部豪雨成災，蔡總統搭乘雲豹裝甲車勘災，那姓男子於臉書張貼 LINE 截圖，假冒國軍雲豹裝甲車駕駛，稱陪同救災裝甲兵荷槍實彈。

★ 刑事局（偵查第九大隊）據報追查，依偽造文書及侮辱公署罪將那姓男子移送高雄地檢署偵辦。



因假訊息操作影響選舉結果，使瑞典的兩大聯盟皆無法取得國會過半數席次，產生國會僵局。（Source: https://en.wikipedia.org/wiki/2018_Swedish_general_election）

國防部針對謠言發布澄清稿，並依法提告散播者。（圖片來源：國防部發言人臉書粉絲專頁，https://www.facebook.com/MilitarySpokesman/photos/a.457847624278561/1987988894597752/?type=3&theater）

東森新聞因報導錯誤防疫資訊遭 NCC 裁罰，動植物防疫檢疫局事發後針對此案再次說明正確防疫資訊加強宣導。（圖片來源：動植物防疫檢疫局 - 防疫小尖兵臉書粉絲專頁，https://www.facebook.com/baphiq.tw/photos/a.1528096367463980/2185898035017140/?type=3&theater）

（三）2018 年 9 月燕子颱風肆虐日本，關西機場因水患關閉，臺北大學游姓學生在 PTT 發文，散布大陸領事館派車至機場內接送大陸遊客的假訊息，造成網路霸凌現象。

★ 游姓大學生遭警方認定散布謠言違反〈社維法〉，移送南投地方法院，但法官認為謠言內容未造成民眾生命威脅，不符〈社維法〉有影響公共安寧之情形的構成要件，裁定不罰。

（四）2018 年底高雄市長選舉造勢，邱姓立委擔任旗山場造勢晚會主持人，拿麥克風喊「感謝大家嘸（沒有）離開」，但媒體報導邱喊「大家麥（不要）離開」。

★ 因媒體報導提供不正確資訊，違反事實查證義務，且未妥善更正，遭通傳會裁罰 20 萬元。

（五）非洲豬瘟疫情，政府宣導民眾收到疫區豬肉製品應送檢疫機關處理，媒體卻錯誤報導「網傳淘寶消費送豬肉腸，建議煮熟食用或丟棄」。

★ 因報導內容未正確傳達防疫資訊，恐造成防疫漏洞，形成公共秩序危害，遭通傳會裁罰 20 萬元。

外國法制趨勢

近年來歐美先進國家之防假策略，因傳統媒體的自律機制失靈，已改採取法律規範，避免民主法治的基礎潰堤。「他山之石，可以攻錯」，謹介紹如下：

一、修改相關法規

國　家	美國	法國	英國
法規名稱	2017 年《誠實廣告法》草案	2018 年《反資訊操縱法》	2018 年下議院 DCMS 委員會提出假訊息管理之建議報告
主管機關	聯邦選舉委員會（FEC）	最高視聽委員會（CSA）	選舉委員會（EC）、資料保護委員會（ICO）、競爭及市場管理局（CMA）、數位文化暨體育部（DCMS）、通訊管體局（Ofcom）
規範對象	社群媒體平臺	社群媒體平臺、廣播電視與報章雜誌的電子平臺	社群媒體平臺與科技公司、廣告業者、企業與個人捐贈之選舉政治獻金
規範內容	1. 政治廣告資訊須公開揭露。 2. 不限於美國境內業者，只要數位平臺在過去 12 個月內的大多數月分，每月有超過 5 千萬位美國訪客或用戶即適用。	1. 僅規範選舉日前 3 個月，至開票日為止。 2. 候選人可要求法院 48 小時內決定是否刪除假訊息。 3. 應建置使用者舉報假訊息之系統。	1. 政府應召集專家小組，建立透明標準來評鑑網站。 2. 建議 ICO 加強個資保護，可針對平臺業者徵收規費。 3. 建議增加違反選舉法之罰款，並調整政治廣告費的限制規範。

二、訂定專法

國家	德國	馬來西亞
法規名稱	2018 年《社交網路強制法》（NetzDG）	2018 年《反假新聞法》（實施半年後廢除）
主管機關	聯邦司法及消費者保護部（BMJV）	經由一般司法訴訟程序（警察機關逮捕、檢察官起訴）處理
規範對象	以電信媒體服務提供商為主，不包含新聞編輯平臺	任何人，對其擁有、保管、控制之內容若涉及假訊息，知悉時需立即移除
規範內容	1. 社群媒體具有雙重查核機制，一為 NetzDG，一為社群媒體平臺內規與共同商業服務條款。 2. 公然違法（恐嚇、毀謗、宗教、種族歧視），業者須 24 小時刪除或封鎖。 3. 非公然違法（灰色地帶），業者有 7 日處理時間。 4. 違反 NetzDG，最高可罰 5,000 萬歐元。	1. 散播者之責任擴及外國人、境外媒體。 2. 假若馬來西亞或其公民受到假訊息影響，無論散播者是否在境內，又或是否為馬來西亞公民，皆可對其加以處罰。

資料來源：行政院科技會報辦公室

我國防假法制作為

一、假訊息的性質

（一）傳遞快速：依據美國麻省理工大學媒體實驗室針對 Twitter 上超過 300 萬用戶進行研究，發現假訊息的傳播速度，竟是正確訊息的 6 倍。

（二）查證困難：很多假訊息複雜並涉及專業知識，查證、辨識難度高。

（三）虛實混雜：假訊息通常會真假訊息並存，讓人信以為真，造成判斷困難。

（四）惡意 VS 無意：惡意或無意傳遞假訊息，違法意識之認定不易。

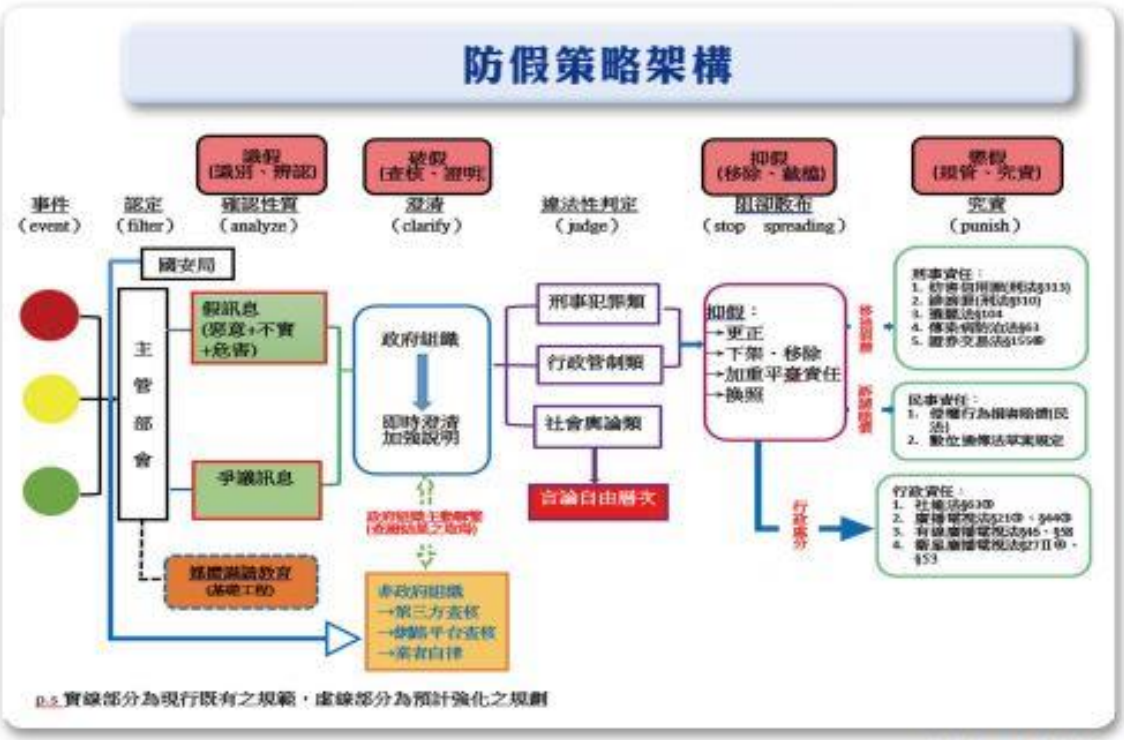
二、法律定義

關於「散播謠言或不實訊息」，行政院專案小組參照法院判決歸納出惡、假、害三要素。以「【故意】散播【有關傳染病流行疫情／影響市場糧食交易價格…】之謠言或不實訊息，足生損害於公眾或他人者，處【罰鍰／罰金】」之參考模版檢討修正既有法律。

三、目標與原則

防假策略從識假、破假、抑假、懲假四個構面著手，秉持「透明、公開、信賴」、「即時、正確、有效」、「法制與科技並重」、「安全與人權兼顧」之原則。

從以下防假策略架構圖中，可清楚瞭解面對假訊息事件發生、因應到結束，各權責機關在危機流程管理中必須扮演之角色定位及運作脈絡，並在不同階段中採取適切對應之行動策略。



資料來源：筆者自製

四、法律之盤點與修正

目前行政院已進行二波法案修正，主要針對法律構成要件及罰則合理性進行檢討，分別於去（2018）年12月及今年4月經院會通過送請立法院審議，並列為本會期最優先審議法案。

第一波修法條文	內容
《農產品市場交易法》第6條、第35條	故意散播影響農產品交易價格之謠言或不實訊息，足生損害農產品運銷秩序者。
《糧食管理法》第15條之1、第18條之3	故意散播影響市場糧食交易價格、主管機關執行糧食產銷或收購公糧計畫之謠言或不實訊息，足生損害農民收益或消費者權益者。
《傳染病防制法》第63條、第64條、第64條之1、第65條、第66條	散播有關傳染病流行疫情之謠言或不實訊息，足生損害於公眾或他人者。
《核子事故緊急應變法》第31條之1	散播有關核子事故之謠言或不實訊息，足生損害於公眾或他人者。
《食品安全衛生管理法》第46條之1	散播有關食品安全之謠言或不實訊息，足生損害於公眾或他人者。
《災害防救法》第41條	• 明知為有關災害之不實訊息而通報。 • 散播有關災害之謠言或不實訊息，足生損害於公眾或他人者。
《廣播電視法》第20條之1、第21條、第42條之1、第43條、第44條、第45條	• 增訂製播新聞之電視事業或其他經主管機關指定之廣播事業應設置自律規範機制。 • 製播新聞如違反事實查證原則致損害公共利益，應將該新聞送請事業設置之自律規範機制調查後，再送請主管機關審議。
《公職人員選舉罷免法》第51條、第51條之1、第51條之2、第110條 《總統副總統選舉罷免法》第47條、第47條之1、第47條之2、第96條	• 競選、罷免廣告之刊播者、出資者姓名等資訊應公開。 • 禁止境外（外國、陸港澳）資金資助競選、罷免廣告，為他人向平台委託刊播者負資金來源合理查證、提出切結義務。

第二波修法條文	內容
（刑法）第251條、第313條	以廣播電視、電子通訊、網際網路或其他傳播工具犯罪傳送影響物價之不實資訊或損害他人信用者，加重其刑至1/2。
《陸海空軍刑法》第72條	• 意圖散布於眾，捏造或傳述軍事上之謠言或不實訊息。 • 以廣播電視、電子通訊、網際網路或其他傳播工具傳播關於軍事上不實訊息者，加重其刑至1/2。
《公民投票法》第20條之1、第20條之2、第20條之3、第43條之1	• 公投廣告刊播者、出資者姓名等資訊應公開。 • 禁止境外資金資助公投廣告，為他人向平台委託刊播者負資金來源合理查證、提出切結義務。

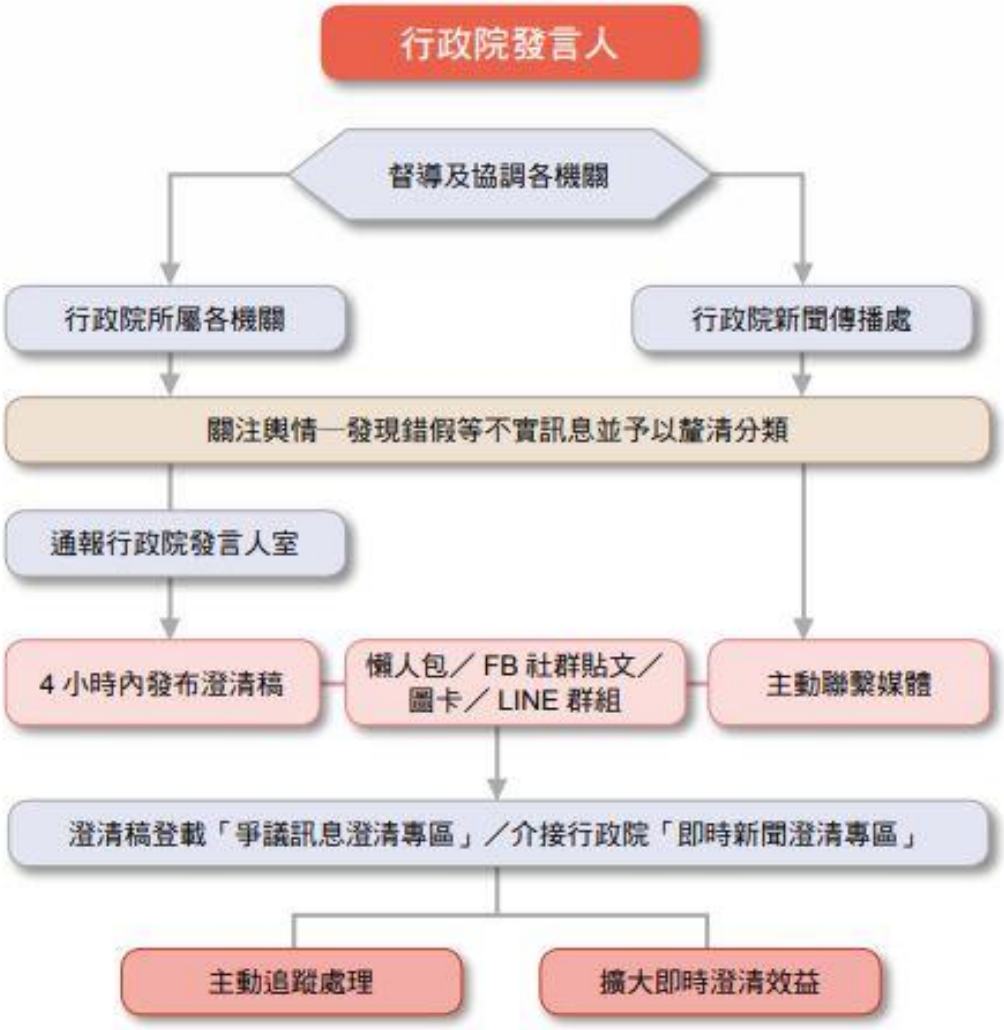
防假行政措施

一、媒體識讀教育提升免疫力

媒體識讀教育是最基礎的工程，必須培養公民對於媒體及網路資訊的識讀能力，讓每個人有獨立的判斷能力，建立自我的免疫系統。另也必須從學校教育、政府部門及公私協力方面，推動媒體素養的強化。

二、提升政府部門澄清機制的效率

政府應提升澄清說明的效率，由行政院設置單一窗口，作為民眾回報假訊息之受理管道。各部會成立專責組織，加強人力、專業、資源，提升因應假訊息的即時反應能力及有效澄清方法，與行政院的單一窗口形成防護網，區域聯防、多頭並進。強化即時新聞澄清機制之流程如下：



三、持續監理廣電媒體落實自律

通傳會未來將針對廣電媒體查證流程，就《衛星廣播電視法》第 27 條及《廣播電視法》草案第 20 條之 1 與第 21 條處理程序暨判定參考準據具體明確化，並掌握處理時效。另該會將積極強化監理廣電媒體落實內控機制及自律，並輔以資訊揭露及他律等機制，同時根據前揭具體明確化準據強化法遵落實。

四、公私協力推廣事實查核

目前臺灣已成立專業第三方的事實查核中心，民間也有「真的假的 Cofacts」專案、「美玉姨」的 LINE 帳號、「蘭姆酒吐司」、「MyGoPen」的闢謠帳號。政府各部會澄清資訊將採取結構化及開放格式，以利於第三方查核機構快速自動接取，達到即時自動澄清之目的。

結語

2019 年 3 月無國界記者組織發布「中國追求的世界傳媒新秩序」，指出中共近 10 年透過購買外媒公司、業配廣告及孔子學院宣傳等控制境外資訊的方式，侵蝕西方民主國家的基礎，成為「特洛伊木馬政策」。瑞典哥德堡大學研究計畫指出，在調查的 179 個國家中，臺灣遭受外國假訊息攻擊程度世界第一。

中共藉由散播假訊息模式對臺灣進行心理及輿論系統的認知作戰，因此，面對此種資訊戰和超限戰的國安議題，中央和地方政府必須攜手合作，透過建構識假、破假、抑假、懲假四面防護網，結合全民力量投入防假運動，形成防禦民主的陣線，才能在這場「無煙硝」戰爭中勝出，鞏固及深化我國民主制度。

本文摘自清流雙月刊中華民國2019年7月 號P4-P13

關鍵基礎設施之脆弱點簡介

華梵大學特聘教授 朱惠中

清流 MJIB

關鍵基礎設施之脆弱點簡介

◆ 華梵大學特聘教授 — 朱惠中

地緣政治角力下，關鍵基礎設施成箭靶。各國八成以上的關鍵基礎設施，都是仰賴工業控制系統來執行自動化作業，因此，工控系統若防護失靈，將衍生國安危機。

工控系統為關鍵基礎設施運作主軸

關鍵基礎設施（Critical Infrastructure, CI），已由隱學變成顯學，為強化 CI 防護的有效性，必須瞭解 CI 弱點，亦即訂定其韌性（Resilience），以提高當資安問題發生時 CI 的可用性，並為主管階層進行資安風險管理相關決策時，提供各種必要的資訊。又因超過 80% 的 CI 是依賴工業控制系統（Industrial Control System, ICS）來執行其自動化作業，故 ICS 實為 CI 主軸，本文彙整國內外的相關文獻，匯整出 ICS 之相關脆弱點，供讀者參考。

目前幾乎所有 CI 運轉均由電腦化控制 ICS 來運作，因此 ICS 安全關係到國家的戰略安全；圖為航空交通管制設施，亦與 ICS 運作息息相關。

早期設計的 ICS 都是在封閉性獨立環境中使用，然現今系統大多會以網路互聯，隨著資訊技術的進步，資安威脅亦急遽提升。

工控系統脆弱點　影響國家安全

脆弱點（弱點）是指資訊系統、系統程序，控制或威脅來源可以被利用來使原設計之功能無法達成。911 事件後，美國國家科學院研究調查指出，目前美國幾乎所有 CI（電力、水源、交通、通訊與能源供應等）運轉均由電腦化控制 ICS 來運作，因此 ICS 安全可說關係到國家的戰略安全。

一般來說，**ICS 所面臨的安全風險，主要來自早期設計的 ICS 都是在封閉性獨立環境中使用**，並未設想到會以網路互聯，所以較少考量資安上的防護。而在網路開源社群興起與各類攻擊方法精進下，讓有心人士有更多管道能取得這些封閉性系統內的相關資訊；復以 ICS 掌握著許多國家的重要基礎建設，當然也就成為敵對國家網軍，或極端勢力的攻擊目標。

綜前所述，工業自動化生產領域在享受開放、資訊技術及網際網路技術帶來的進步、生產率提高與利益大大增強的同時，也面臨著越來越嚴重的安全威脅。

美國工業控制系統網路緊急應變小組（ICS-CERT）於 2016 年曾進行評估顯示，ICS 弱點包含邊界防禦、功能管理（最小功能）、認證機構管理（授權管理）、身分識別與驗證、最低權限以及資源分配等 6 大弱點，其中又以邊界保護不足為最普遍的弱點。

美國 NIST 的 ICS 脆弱點分類

美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）針對 ICS 之弱點，於政策面與程序面、架構面與設計面、配置面與維護面、實體面、軟體發展面以及通訊與網路架構面等面向均提出看法，說明如下（整理自 NIST SP 800-82 第 2 修訂版）：

一、ICS 政策面與程序面弱點

（一）ICS 之安全政策不足：ICS 弱點通常源於政策不足或缺乏。

（二）缺乏 ICS 安全訓練意識宣導：沒有具體 ICS 政策與程序來進行宣導或訓練，將無法期待員工可維持安全之 ICS 環境。

（三）缺少或缺乏 ICS 設施執行指南：設備執行指南應該保持最新狀態，並且隨時可用。

（四）缺乏安全政策執行之行政機制：執行安全的工作人員應負責管理文件化之安全政策與程序。

（五）缺乏對 ICS 安全控制之審查：應透過程序及時間表，確認安全程序被正確地執行。

（六）沒有 ICS 緊急應變計畫：缺乏緊急應變計畫將導致停機時間延長與生產損失。

ICS 設施執行指南應保持最新狀態，並隨時可用；且執行安全的工作人員應負責管理文件化之安全政策與程序。

（七）缺乏配置變更管理政策：導致無法管理高度脆弱的硬體、韌體與軟體。

（八）缺乏適當的存取控制政策：存取控制實施取決於策略是否正確地模擬其角色、職責與授權。

（九）缺乏足夠之認（驗）證政策：沒有認證政策，未經授權的存取更有可能發生。

（十）事件檢測與回應計畫與程序不足：快速檢測事件能減少損失與破壞，故須保留數位鑑識證據，降低被利用的弱點數與恢復 ICS 正常服務。

（十一）缺乏關鍵組件之備援（份）：缺備援（份），導致發生故障可能性增加。

二、ICS 架構面與設計面弱點

（一）架構與設計之安全性考量不足：設計時即應將安全性納入 ICS 架構中，包含使用者的識別與授權，存取控制機制，網路拓撲以及系統配置完整性。

（二）允許不安全架構之演變：ICS 的網路基礎設施經常依據業務需求進行開發與修改，須考慮因變更而產生潛在的安全影響。

（三）沒有定義安全邊界：沒有明確定義 ICS 的安全邊界，就無法確保安全控制被部署或正確配置，將可能導致未經授權的存取發生。

（四）非控制流量的控制網路使用：控制與非控制流量具不同的要求，因此，若在單個網路上同時擁有兩種流量使得網路配置更加困難。例如，非控制流量可能會無意中消耗控制流量需求的資源，從而導致 ICS 功能中斷。

（五）ICS 網路未提供網路控制服務：ICS 網路所使用的 IT 服務如 DNS 及 DHCP，可能無法符合 ICS 所需的可靠性與可用性。

（六）事件資料收集不足：數位鑑識分析取決於收集和保留足夠的資料，如果沒有正確的資料收集，可能無法找出導致安全事件發生的原因。

三、ICS 配置面與維護面弱點

（一）硬體、韌體與軟體未受配置變更管理：缺少配置變更管理程序可能導致安全漏洞產生，為了妥善保護 ICS，應準確列出系統中的資產及其目前配置設定。這些程序對於營運持續與災害復原計畫至關重要。

（二）作業系統與供應商軟體修補，直到安全漏洞被發現後才執行：由於 ICS 軟體與基礎 ICS 間的緊密結合，變更時必須經歷耗時的回歸測試；此測試和之後發布更新軟體需要時間，因此提供了長時間的漏洞。

（三）作業系統與應用程式沒有被維護，或供應商拒絕修補弱點：過時的作業系統和應用程式可能包含漏洞；

數位鑑識分析取決於收集和保留足夠的資料，如果沒有正確的資料收集，可能無法找出安全事件發生的原因。

安全修補程序甚至可能不支援於過時作業系統的 ICS。

（四）安全變更測試不足：對沒有測試的硬體、韌體與軟體的修改，可能危及 ICS 的正常運作，因此，應發展測試變更的全影響記錄程序。

（五）不足的遠端存取控制：ICS 可能需要遠端存取，因此必須加強控制遠端存取功能，以防止未經授權的使用者存取 ICS。

（六）不當的配置使用：不正確配置的系統，可能會開啟不必要的連接埠與協議，增加漏洞產生；使用預設配置，通常亦會暴露出漏洞。

（七）關鍵配置沒有回存或備份：ICS 配置設定回存程序可防止 ICS 配置資料意外遺失。

ICS 可能會遠端存取，因此須加強控制遠端存取功能，防止未經授權的使用者存取 ICS；且須設定適當的存取控制權限，避免使用者的權限太高或太低，造成運作失衡。

（八）移動設備資料未受保護：弱敏感資料（例如密碼）被儲存在筆記型電腦和行動裝置內，當這些設備遺失時，系統安全性可能受到損害。

（九）密碼的產生、使用與保護沒有依據政策執行：違反密碼政策與程序可能會增加 ICS 漏洞產生。

（十）不足的存取控制應用：指定不當的存取控制，可能導致 ICS 使用者的權限太高或太低。

（十一）不正確的資料鏈結：ICS 資料儲存系統可能與非 ICS 資料源相連，可能導致資料從某個資料庫被自動複製到其他資料庫。

（十二）未安裝或更新惡意程式防護措施：惡意程式防護措施必須被安裝與更新至最新之病毒碼。

（十三）未充分測試惡意程式保護措施：在沒有充分測試惡意程式保護措施的狀況下，可能會影響 ICS 的正常運作。

（十四）阻斷服務：ICS 軟體可能容易受到 DoS/DDos 攻擊，導致經授權的存取系統被阻止或系統功能被延誤。

（十五）沒有安裝入侵偵測（防禦）系統：IDS（IPS）軟體可以防止各種攻擊，包括 DoS 攻擊，並識別受攻擊主機，例如感染蠕蟲的內部主機。

（十六）沒有維護日誌：沒有正確維護日誌，導致無法追查安全事件發生原因。

四、ICS 實體面弱點

（一）未授權之人員可實際存取設備：ICS 設備存取應僅限於必要人員。

（二）射頻、電磁脈衝（EMP）、靜電放電、停電和用電尖峰：ICS 硬體易受射頻、EMP、用電量影響，導致指令中斷，或對電路板的永久損壞。

（三）缺乏備用電源：沒有備用電源，一但停電將導致 ICS 關機。

（四）環境控制的喪失：溫度與濕度變動，可能導致 ICS 損壞。

（五）不安全的實體連接埠：不安全的連接埠，會讓未經授權的 USB 儲存設備連接。

五、ICS 軟體發展面弱點

（一）不正確的資料驗證：當 ICS 軟體無法正確驗證使用者輸入資料時，可能導致緩衝區溢位、命令注入以及目錄路徑穿越漏洞等。

（二）預設狀況下，未啟用安裝的安全功能（SIS）：若未啟用或至少被識別已被停用，那麼與該產品一起安裝的安全功能將無效。

（三）認證、權限與存取控制不足：未經授權存取配置和程式軟體將可能會損壞設備。

ICS 硬體易受用電量影響導致指令中斷，須確保備用電源充足，避免停電導致 ICS 關機。

六、ICS 通訊與網路架構面弱點

（一）未使用資料流控制：資料流控制能允許哪些資訊流通，防止資訊洩露。

（二）防火牆不存在或配置不正確：缺乏正確配置的防火牆，使敏感資料受到竊取。

（三）防火牆與路由器紀錄不足：沒有維護日誌，導致無法追查安全事件發生之原因。

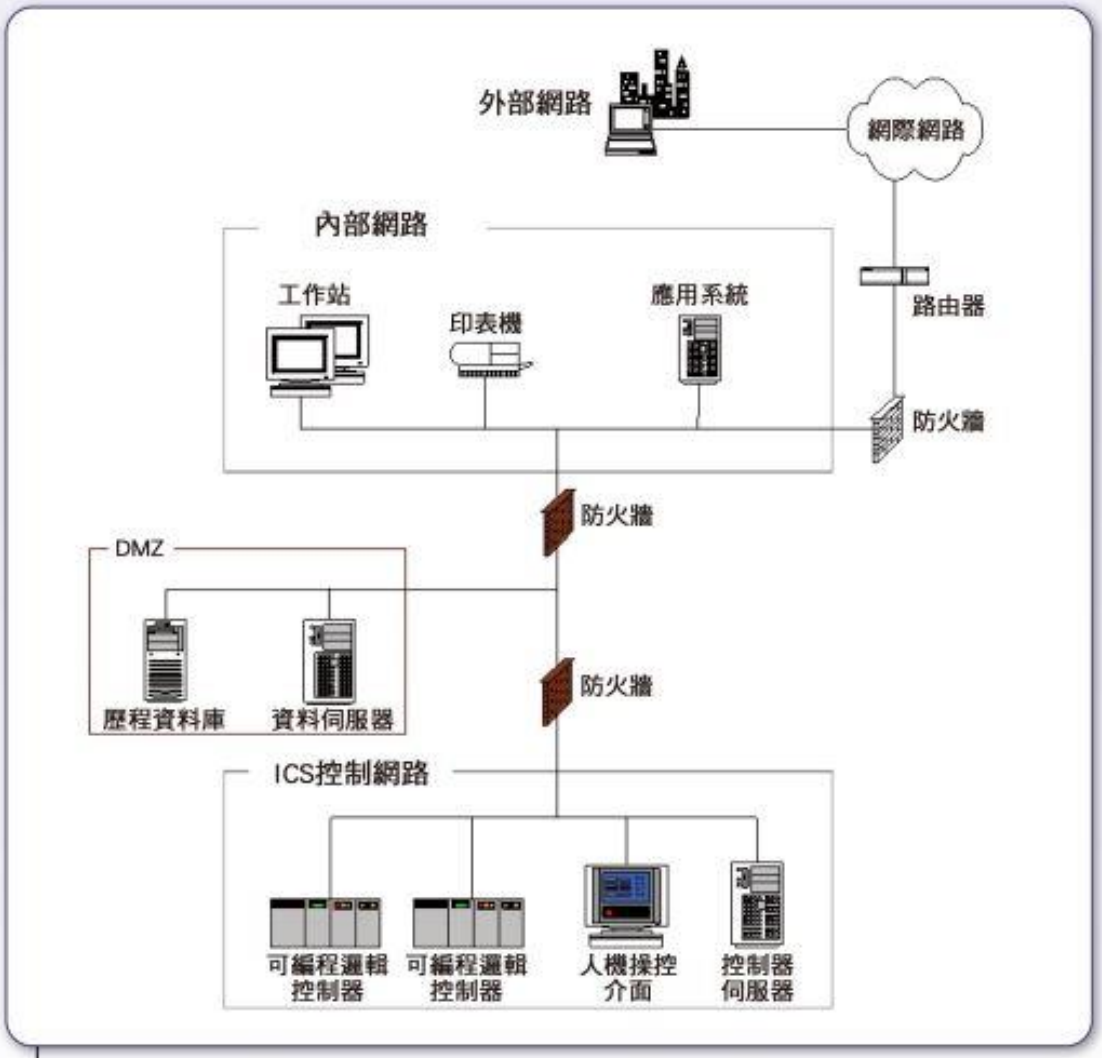
（四）標準、通訊協定使用明文傳輸：透過 ICS 網路活動的監聽，可以解碼資料傳輸。

（五）使用者、資料或設備的驗證不符合標準或不存在：許多 ICS 協議沒有任何級別的驗證，沒有身分驗證，會導致資料錯誤或欺騙設備的情況發生。

（六）使用不安全的 ICS 協議：ICS 協議通常具有很少（或沒有）安全功能，例如身分驗證和加密，會導致額外漏洞產生。

（七）缺乏完整性的通訊檢查：大多數 ICS 協議中沒有完整性檢查，為了確保完整性，ICS 可以使用提供資料完整性保護的低層協議（例如 IPsec）。

（八）缺乏無線網路使用者與存取點間的認證：需在無線使用者端和存取點之間進行較強的相互認證，以確保使用者端不會連接到惡意無線基地臺。



單一防火牆在遭受大量攻擊時，可能面臨功能喪失或效能降低等情況，建議架設兩道防火牆，分別對內部網路與ICS控制網路進行封包過濾，強化安全防護能量，提升防禦能力。（資料來源：NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf；國土安全辦公室，https://ohs.ey.gov.tw/Page/6C4A1386ACBA6734）

（九）無線使用者端與存取點間的資料保護不足：敏感資料在無線使用者端和存取點間應使用強化加密來保護，確保競爭對手無法獲得未經授權的存取。

結論

「知己知彼，百戰百勝」，故ICS保護必須滿足兩個要求，即安全性（Safety）—知道自己的弱點，及可用性（Security）—如何保護自己免受傷害。

本文摘自清流雙月刊中華民國112年3月 號P46-P52