如何縮小CI資安防護人才缺口

◆ 華梵大學特聘教授 — 朱惠中

從俄烏戰爭經驗來看，關鍵基礎設施已成為軍事攻擊目標。強固關鍵基礎設施、強化抵禦網路攻擊能力，已成各國維護國安的重點，然許多國家正面臨著 CI 資安人員嚴重不足的困境。

資安維護為 CI 防護主軸

依據行政院「國家關鍵基礎設施安全防護指導綱要」定義，國家關鍵基礎設施（Critical Infrastructure, CI）係指公有或私有、實體或虛擬的資產、生產系統以及網路，因人為破壞或自然災害受損，進而影響政府及社會功能運作，造成人民傷亡或財產損失，引起經濟衰退，以及造成環境改變或其他足使國家安全或利益遭受損害之虞者；而其中特別重要者為 IT（資訊科技）與 OT（運營科技）安全維護。

因 CI 已是具高度吸引力的受攻擊目標，故 CI 防護主軸即為 IT 與 OT 資安之防護，本文將討論 CI 資安防護人才為何短缺及如何緩解。

CI 資安人才短缺原因

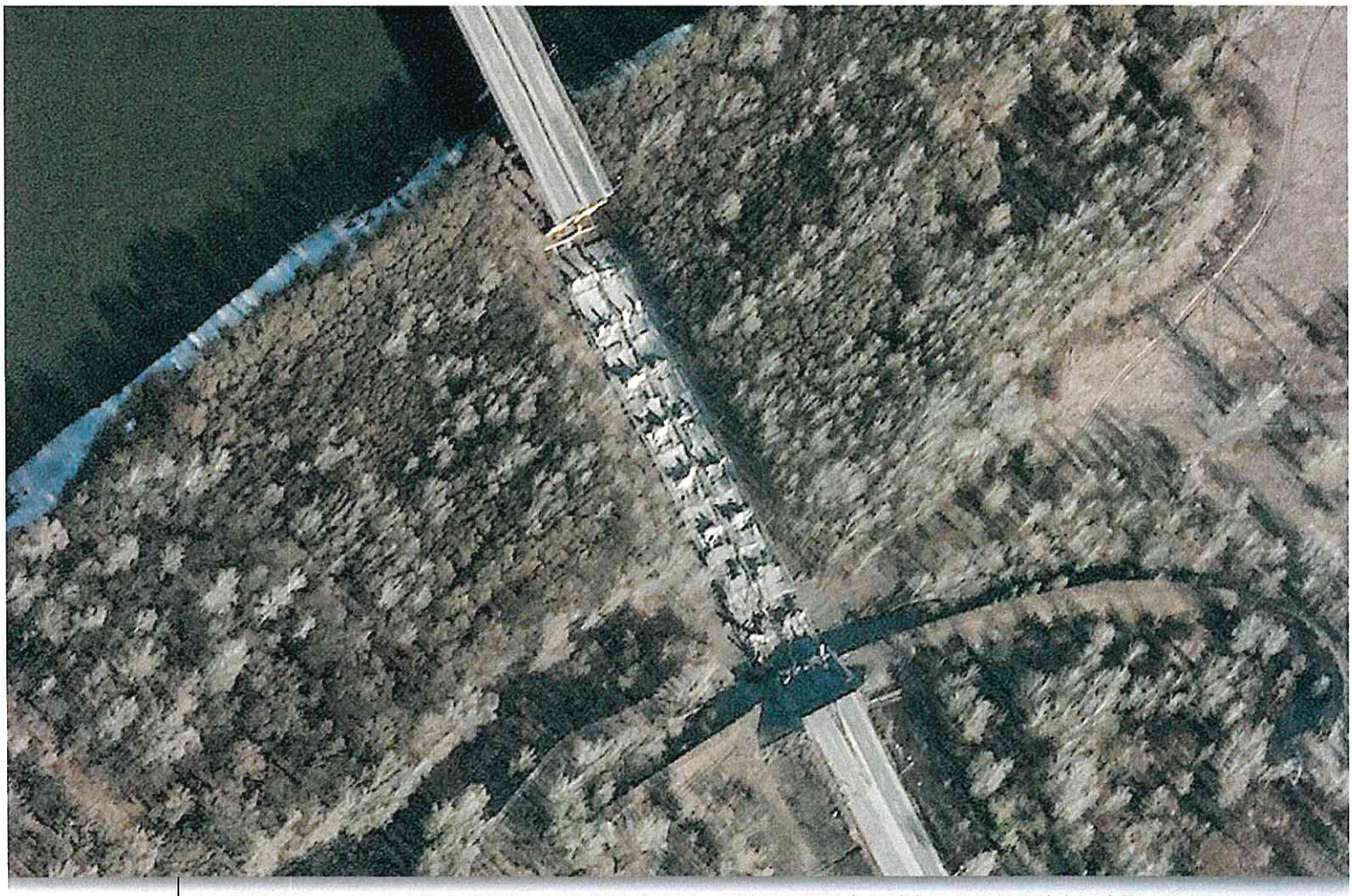
近 5 年來，各國能源（油電）、水資源、通訊傳播、交通、銀行、醫院與國防等 CI 設施遭攻擊事件不斷增加，CI 防護已由隱學變顯學。特別自 2021 年來，在疫情及俄烏戰爭雙重挑戰下，更增加 CI 資安的維護

困境，許多國家正面臨 CI 資安人員嚴重不足的危機。

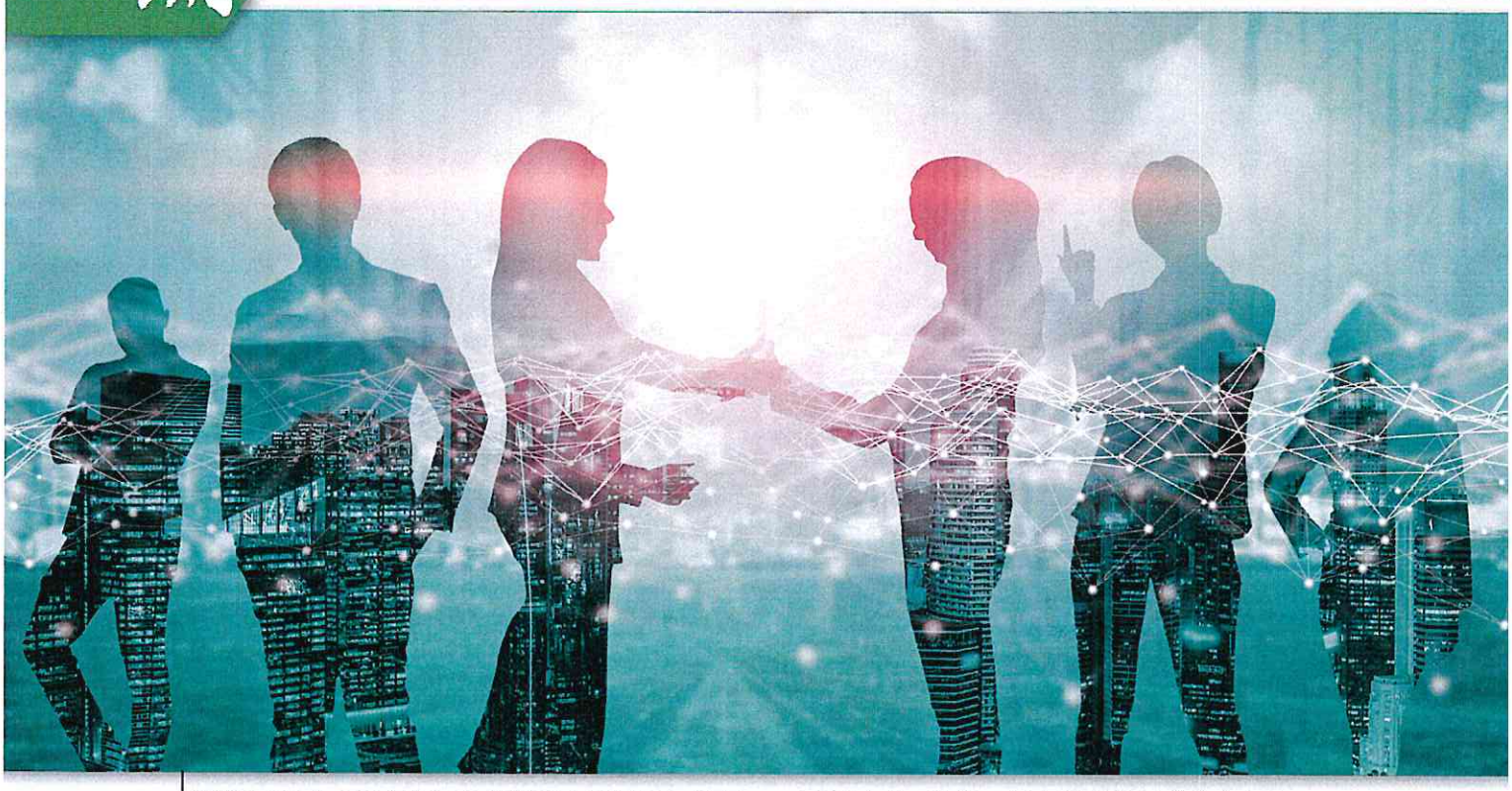
根據美國 SecuirtyWeek 報導，光 2021 年，美國就有 350 萬個 IT 資安職位空缺，而非常專業的 OT 人才更缺乏，因為 IT 擁有數十年、專業知識遙遙領先，因此擁有更大的人才庫；另根據 Pollfish 於 2021 年對 IT 和 OT 資安人員進行全球調查，90% 受訪者表示他們正在尋求僱用更多的資安人員，其中 88% 的受訪者表示很難找到合適人選。Dr. Andrew Reifers 曾列出 CI 人才缺乏原因如下：

一、資安工作的需求增加。近年來各國對 CI 的依賴度越來越高，資安威脅大幅增加且資訊設備更新（生命週期）速度太快，因此，沒有一個人可以真正成為所有這些專業的專家。

二、資安工作需有跳出框架思考的能力，並能預見還不存在的問題。擁有這種天賦的人是最有才華、最熟練的資安專家。傳統學校可以教學生技能，亦可教他們程序，但那種遠見和創造能力更像是一門藝術，不是一門教了就能學會的事情。



俄烏戰爭期間，CI 是基本的攻擊目標；圖為傑斯納河橋，因被摧毀導致市郊城市至首都基輔的交通中斷、救援物資運送受阻。（Photo Credit: Planet Labs PBC, https://www.planet.com/gallery/#!/post/desna-river-bridge）



根據 Pollfish 於 2021 年對 IT 和 OT 資安人員進行全球調查，90% 受訪者表示他們正在尋求僱用更多的資安人員。

三、資安問題解決，介於由受過專業培訓的專業人員、團隊（user）以既有技術與程序，與由專業團隊（verdor）來處理之間。

四、越來越多組織開始以聘請內部專家、外包和眾包（crowdsourcing）等方式，來解決資安人員短缺問題。

五、在早期，只要能處理資安問題，人員背景或教育水平並不重要；然隨著資安越來受企業重視，資安防護更加標準化，是否有學位或獲得認證，已成為專業資安人員的必備條件。

如何緩解 OT 資安人才欠缺

實務上來看，並無簡單解決方案可以縮小 CI 資安防護人才缺口；本文匯整國內外文獻及實例後，建議還是可從下列幾個面向來解決：

一、IT 與 OT 人員須有相同認知

近來，以 IT 與 OT 融合資安為主軸的培訓計畫已成為顯學，為增加效率及提升競爭優勢，以 IT 為基礎之技術與設備，如機器學習（Machine Learning）、大數據（Big Data）及感知器（Sensor）等，已融入 OT 網路環境中，此一發展方向固然可以滿足使用者某些需求，但亦增加了被攻擊機率及系統被入侵的風險。為降低風險，IT 與 OT 人員應有以下認知：

（一）為什麼保護 OT 是一個具有挑戰性的過程？

（二）防止攻擊並保持操作正常的基礎架構為何？

（三）OT 和 IT 人員必須相互理解對方的專業領域：在 OT 世界中，原則上是自我管理，其認為業務網路（MIS）與控制網路（CIS）是分開

的，故與 IT 交流並不普及；所以傳統上，IT 人員可能不瞭解 OT 人員所做的工作。

（四）安全人員需獲得 OT 工程師的信任：通常，IT 和 OT 人員對意外事件的看法不一樣，因為他們來自不同的背景；以停電而言，OT 營運商認為是項重要且必要的安全功能（故停電是意外），但從 IT 人員角度來看，停電則可能是潛在的漏洞或正在遭受攻擊（是異常）。

（五）OT 業務需企業整體支持。[1] OT 與 IT 在作業系統上需求有所不同，讓 OT 與 IT 具有完全不同的規範且有顯著差異，先備知識沒有交集。這些問題使 IT 與 OT 的整合更艱困複雜，故需建立一個 OT 網路團隊。

總之，當組織交叉培訓 IT 與 OT 人員時，須安排 IT 與 OT 工程師有一起實習的機會；又因 OT 系統規格種類繁多，這也讓 OT 人員擁有較長的專業生命週期，雖然他們大多數的技術都已過時（Legacy），然相處過後，資深 IT 人員應該會驚喜地發現，這些 OT 人員熟悉許多基礎技術，所以透過一起實習機會，能讓 IT 人員輕易地掌握這些 OT 網路系統的不同要求。

實習的好處是組織內 IT 員工已熟悉公司流程，並且知道在哪裡尋找到所需知識。

通常，IT 和 OT 人員對意外事件的看法不一樣，因為他們來自不同的背景。

[1] 業務和系統所有者必須了解 ICS（Industry Control System 及 Incident Command System）的風險，而後者包括管理（Administration）、規劃（Planning）、操作（Operation）、後勤（Logistic）及財務（Finance）等項目。

當組織交叉培訓 IT 與 OT 人員時，須安排 IT 與 OT 工程師有一起實習的機會，讓 IT 人員掌握這些 OT 網路系統的不同要求。

新加坡網路安全局啟動 OT 資安能力框架計畫，為 OT 資安部門吸引和培養人才奠定了良好基礎。（Source: Cyber Security Agency of Singapore, https://www.csa.gov.sg/Tips-Resource/publications/2021/operational-technology-cybersecurity-competency-framework-(otccf)）

所以企業在招聘 OT 人員時，這將是一種更省時、更具成本效益的方式，更不用說它更容易在組織的 IT 和 OT 團隊間建立出資訊共享機制。

二、資安長（CISO）應有作法

CISO 應與教育機構合作，查看是否有 OT 資安人員培訓計畫。以美國為例，目前雖無足夠課程，但許多學術機構已規劃開設跨學院和大學的課程。愛達荷州立大學已開設兩年課程，畢業生將獲得工業網路安全工程技術的副學士（An associate of applied science degree, AAS），威爾明頓大學則提供 SCADA 網路安全研究生證書，[2] 其他學校（包括高中職）亦提供 OT 安全課程，作為學生在取得資安學位時的必修學分。

三、政府所應扮演角色

新加坡政府最近在減少 CI 資安防護人才缺口方面，有了巨大進展，可作為我國的借鏡。2021 年 10 月，新加坡網路安全局（CSA）在民營企業支持下啟動 OT 資安能力框架（OTCCF）計畫，為該國 OT 資安部門吸引和培養人才奠定了良好基礎。新加坡 OTCCF 計畫旨在建立一個 OT 培訓師庫，這些培訓師將能夠開展與 OTCCF 宗旨一致的 OT 資安基礎課程。

在地緣政治局勢逐漸緊張下，美國白宮與網路安全和基礎設施安全局（CISA）更加關注 CI 的 OT 防護，美國聯邦政府的一項類似措施將有助於促進這一嶄新領域之發展。儘管 CISA 已提供培訓，但若能鼓勵公私企業更廣泛合作，不僅可滿足使用者需求，更會強化供應方的責任，因為它可以為教育工作者和培訓師提供急需的最佳實踐和全面發展的規範，此即推廣 IEC - 62443 OT 資安教育計劃的主因。[3]

四、依靠技術來提供幫助

工業環境中的資產難以檢測、管理，甚至更難以保護，尤其是在不斷擴大的連

愛達荷州立大學已開設兩年工業網路安全工程技術相關的課程，畢業生可獲得副學士的學位。（Photo Credit: Idaho State University College of Technology, https://youtu.be/-V6orz5Lx-s）

當 IT 和 OT 一起查看 OT 環境，通過使用相同的信息集，這些團隊將可以在數周內快速降低風險並增強安全性。

接設備和設備領域。技術正朝著解釋 OT 網路晦澀難懂的方向邁進一大步，一直延伸到物聯網，專為資產可見性而構建的，有助於識別物聯網中漏洞和可疑行為的無代理解決方案油然而生。實施此類解決方案，讓工作流完美集成。當 IT 和 OT 團隊一起查看 OT 環境，通過使用相同的信息集，這些團隊將可以在數周內快速降低風險並增強安全性。

尤其是透過政府、學術界以及企業內部等多個不同領域的相互合作，將可共同解決 OT 資安漏洞，特別是如能將專業知識（Domain Knowledge）、員工經驗（Institutional Knowledge），與先進技術組合並應用於 OT 網路，將更可以保護被駭客準備攻擊的關鍵 OT 環境，進而提升 OT 網路的安全性。

小錢不花，大事發生

5G、工業 4.0、物聯網興起，全球產業的工控系統吹起轉型風，圍繞著產業、CI 設施的 OT 資安已至關重要。資安領域以極快速度在發展，相關法規、技術和威脅格局正呈指數級增長。教育是百年大計，人才培育更需長期的永續發展，高教機構和企業都應及早因應，更有賴於中央政府的統籌與強力支持，建立一個國家級的 OT 培訓師庫，才是最佳解決對策。

[2] 監督控制和數據採集系統（supervisory control and data acquisition, SCADA）。

[3] IEC 62443 最早由國際自動化學會（International Society for Automation, ISA）所創立，後經審核再透過美國國家標準協會（American National Standards Institute, ANSI）以文件的型式發布。IEC 62443 現為國際廣泛採納和認可的工業自動化及控制系統（Industrial Automation and Control System, IACS）的網通安全（Cybersecurity）標準。《什麼是 IEC 62443 ？》，https://linchew.com/2021/04/ 什麼是 iec-62443。