

成功大學——關鍵基礎設施資安人才及技術培育基地計畫

資安人才正夯，從逼真的危機演練開始



從二〇一九年起，每兩年舉辦一次的「跨國網路攻防演練」(Cyber Offensive and Defensive Exercise, CODE)，係模擬如銀行、醫院、油、水、電等關鍵基礎設施遭到資安攻擊的應變演練，並盡可能地完整重現各種攻防實境。台灣自來水公司在二〇二三年十月舉行的跨國網路攻防演練中，扮演藍軍的角色，與來自美國、捷克及國際間好手組成的其他隊伍之紅軍進行各種情境攻防，成功抵禦嘗試駭入工業控制系統的各項資安攻擊，並針對各項緊急情況做出相對應的處置，最終獲得第一名佳績。

駭客技術日新月異，攸關民生的關鍵基礎建設更容易遭到駭客鎖定，所以各國無不投注大量資源以提升資安維護層級，在「跨國網路攻防演練」獲得好成績的台灣自來水公司，就曾經到成功大學所建置的「關鍵基礎設施資安人才及技術培育基地」受訓，為的是使用內部還原度幾近百分之百的工業控制設備機臺，模擬攻防演練。

跨校、跨域合作育才

設置在成功大學計算機中心內的基地，不只是臺灣少數培訓工業控制端人才的場域，在涵蓋煉油廠、淨水廠、發電廠及變

電所等四大關鍵基礎設施場域的模擬工廠中，建置了「蒸餾鍋爐循環系統」、「自來水淨水及供水系統」、「水閘門控制系統」、「太陽能發電監控系統」、「饋線自動化系統」等五套工業控制設備，再加上兩間資安攻防教室及一間資安戰情室，可供實務教學及資安攻防演練之用。

「如何盡可能地還原真實的關鍵基礎設施場域是我們最大的挑戰，」資訊工程系特聘教授兼計算機與網路中心主任陳培殷表示，為了還原真實的機臺設置情形，必須向有經驗的廠商請教，再與設備商不斷討論，建置出最擬真的場域；至於整體規劃與資安攻防演練方面，在經濟部工業局（現為產業發展署）設置以服務產業為主的沙崙資安服務基地前，資安人員培訓多僅著重於網路或應用層面，較少觸及設備端的人才培育，「我們派遣了師生團隊前往沙崙上課和學習，建置場域設備時，也避免與其機臺重複，才能讓兩個基地產生互補效應。」

另一方面，「我們的基地在教育部支持下成立，自然更加注重教學深度，」包括針對跨校、跨域在學生於寒暑假密集培訓的二百七十個小時／十五學分資安學程，以及針對產業人才設計的六十小時資安技術課程及十八小時資安素養課程，都會依循著「基礎」、「核心」、「實務」的步驟，循序漸進地安排課程教學。

負責教學規劃的計算機與網路中心教授李南逸進一步說明，關鍵基礎設施資安相關領域相當廣泛，除了從相關油、水、電及設備商等合作產業界邀請業師之外，與夥伴學校的互動也非

常密切，「在針對大專校院生開設之『關鍵基礎設施資安學程』中，成大的老師負責其中三門課的規劃與授課，另外如『電網資安實務專題』的課程設計和教學由臺中科技大學資訊工程系副教授兼系主任蔡家緯負責，『資訊安全管理』則由嘉義大學資訊工程學系教授陳宗和規劃，透過這樣跨校、跨領域的教學合作，藉此帶來跨域學習的學生。」

學員就業前景看好

目前已有約兩百三十多位學生參與「關鍵基礎設施資安學程」之課程，有學生甚至因而創立了「資安社」，在短短不到一年間，資安社已招收六百多名社員，部分社員還組成「BSIF SQUAD」隊伍，不僅抱回許多資安競賽獎項，更囊括全國技能競賽網路安全職類南區賽事前三名，並與十三所大專校院的資安社團共同創立「臺灣資安聯盟」(Taiwan Security Club, TSC)，辦理一次全國性的資安比賽。

陳培殷相當看好這批學生的就業前景，由於受過扎實的理論及實務基礎訓練，除了補足台灣中油、台灣電力公司、台灣自來水公司等國營事業急需的資安人才之外，進入相關儀器設備商、甚至所有需要工業控制資安人員的產業，如時下熱門的半導體業都不是問題，「我們除了開放油、水、電產業合作進行攻防演練，沒想到連檢警單位都來洽詢是否可以請我們代訓和演練，」這也證了只要根基扎得深，關鍵基礎建設的資安防禦概念，應用的產業範圍可以更為廣泛。