行政院及所屬各機關出國報告
(出國類別：開會)

赴德國參加「第 17 屆國際關鍵資訊基礎設施安全會議」出國報告

服務機關：內政部警政署
姓名職稱：黃亭翰專員
杜志強警務正
出國地區：德國慕尼黑
出國期間：2022 年 9 月 12 日至 9 月 18 日
報告日期：2022 年 12 月 12 日

摘　　要

「第 17 屆國際關鍵資訊基礎設施安全會議」（The 17th International Conference on Critical Information Infrastructures Security,CRITIS）創設於 2006 年，每年定期舉辦年會，本(2022)年於德國慕尼黑舉辦，邀集關鍵基礎設施安全領域的學術界人士、企業及政府組織，提報關鍵基礎設施防護領域最新研究，並置重點於關鍵資訊基礎設施。

觀察 2022 年俄烏戰爭(俄羅斯與烏克蘭)，關鍵基礎設施為敵方攻擊、奪取、控制之首要目標，國安單位應以「內防突變、外防突襲」作為強化關鍵基礎設施韌性最高指導原則，並協同關鍵基礎設施主管機關改善弱點，確保關鍵基礎設施安全。為瞭解國際最新防護政策與作法，本署派員與會以汲取最新知能。

目錄

壹、目的

「第 17 屆國際關鍵資訊基礎設施安全會議」（The 17th International Conference on Critical Information Infrastructures Security）創設於西元 2006 年，每年定期舉辦年會，本(111)年於德國慕尼黑舉辦，邀集關鍵基礎設施安全領域的學術界人士、企業及政府組織，提報關鍵基礎設施防護領域最新研究，並置重點於關鍵資訊基礎設施。

關鍵基礎設施(Critical Infrastructures)係指公有或私有、實體或虛擬的資產、生產系統以及網絡，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。

關鍵資訊基礎設施(Critical Information Infrastructures)係止涉及關鍵基礎設施核心業務運作，為支持該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 DataAcquisition)。

本署 2022 年指派黃亭翰專員及杜志強警務正與會，透過本次出訪機會吸收.關鍵資訊基礎設施領域新知，強化我國關鍵基礎設施安全防護能量。

圖 1 第 17 屆 CRITIS 於德國慕尼黑聯邦國防軍大學舉行

貳、會議議程

本次會議自 2022 年 9 月 14 日(星期三)至 9 月 16 日(星期五)計 3 日，會議議程如下：

2022 年 9 月 14 日(星期三)	
時間	內容
1300-1330	Welcome Address Chair：Leonard Kunczik
1330-1500	Keynote：EU-Hybnet Paivi Mattila Keynote：SANCTUM Christian Despres Chair：Dieter Budde
1500-1530	Coffee Break
1540-1615	Plenary Saeid Nahavandi Chair：Maximilian Moll
1730	Munich Walking Tour

2022 年 9 月 15 日(星期四)			
時間	內容		
0830-0850	Threat-driven Dynamics Security Policies for Cyber-Physical Infrastructures.	An Empirical Evaluation of CNC machines in Industry 4.0.	Modeling Hierarchical Structure of Effective Communication Factors in Cyber Incident Response.
0850-0910	Towards a Layer Model for Digital Sovereignty：A Holistic Approach .	Root Cause Analysis of Software Aging in Critical Information Infrastructure.	An Assessment Model for Prioritizing CVEs in CRITIS in the Context of time and Fault.
0910-0930	Strategic Anticipation in Crisis Management Through the Lens of Societal Values.	High Data Throughput Exfiltration through Video Cable Emanations.	Mapping and Simulating Cyber-Physicals Threats for Critical Infrastructures.
0930-0950	A Water Security Plan to Enhance Resilience of Drinking Water Systems.	Dataset Report：LID-DS 2021.	Building Collaborative Cyber-Security for Critical Infrastructure Protection：Empirical Evidence of Collective intelligence

			Information-Sharing Dynamics on Threat Fox.
1000-1030	Coffee Break		
1030-1200	Plenary：Plenary Horia-Nicolai Theodorescu Plenary：Isto Mattila Chair：Stefan Pickl		
1300-1330	Physical and Hardware Issues in Cybersecurity.	Elections, Technology, and the Pursuit of Integrity：The U.S. Landscape.	
1330-1350	Make Your IT Infrastructure More Secure by Controlling the DNS Traffic.	Is There a Relationship between Cybersecurity Level and Electricity Outages in Norway？	
1350-1410	Solutions & Best Practices on Transactional Data Security Level.	Emerging Importance of Cybersecurity in Electric Power Sector as a Hub of Interoperable Critical Infrastructure Protection in the Greater Metropolitan Areas in Japan.	
1410-1430	Hardware and Firmware Supply Chain Security Risks in ICS/SCADA Environments.	Energy Security in the Context of Hybrid Threats：The Case of the European Natural Gas Network.	
1430-1500	Coffee Break		
1500-1630	Plenary：Daniel A. Nussbaum Plenary：Katharina Rob Chair：Bernhard Hammerli		
1800	Conference Dinner		

2022 年 9 月 16 日(星期五)		
時間	內容	
0830-0850	The Understanding of Vulnerability of Critical Infrastructure.	Identifying Residential Areas Based on Open Source Data：a Multi-Criteria Holistic Indicator to Optimize Resource Allocation During a Pandemic.
0850-0910	Design and Justification of a Cybersecurity Assessments	Automatic Concrete Bridge Crack Detection from Strain Measurements： a

	Framework for IoT-based Environments.	Preliminary Study.
0910-0930	Security in SCADA System：a Technical Report on Cyber Attacks and Risks Assessment Methodologies.	Prediction of the Passenger Load After High-Crowded events Based on Historic Data.
0930-0950	Cybersecurity in the Railway Sector .	
1000-1200	Plenary：Bernhard Tellenbach Plenary：Maximilian Moll Chair：Wolfgang Hommel	
1215-1300	Technical Forum Chair：Jochen Amrehn	
1315-1400	Energy Security and Complex Cyber Operations Chair：Daniel A. Nussbaum	
1400-1700	High Level SAS-Energy Security Workshop Chair：Arnold Dupuy	

參、會議重點摘要

一、 關鍵資訊基礎設施風險管理

(一) 新興科技推進數位轉型，同時導致關鍵資訊基礎設施威脅事件層出不窮，該設施除強化資訊科技資安防護外，應建立以風險為導向之措施，防範駭客攻擊事件。

(二) 風險管理在於瞭解未來不確定因子，與確定各種因子所需支付的成本，風險管理的重心在於設法探求一個平衡點，在此一平衡點上取得最為經濟的結果。風險管理步驟如下：

1、建立風險管理體系，定義風險分析對象。

2、進行風險辨識，找出需要管理的風險，使用系統性方式廣泛搜尋。

3、風險分析，確認現行的機制，找出風險發生的機率及影響性並區分風險等級。

4、風險處理，找出並評估應對風險的方法，研訂處置計畫並執行。

5、協商溝通，建構利害關係者之間的雙向對話，而非決策者單方向將訊息傳送給利害關係者。

二、 德國關鍵基礎設施防護戰略

德國關鍵基礎設施防護戰略以國家、社會及企業共同行動為指導原則，國家與其他私人企業或組織合作制定分析及防護策略，該戰略由德國聯邦民防及災難援助辦公室(Federal Office for Civil Protection and Disaster Assistance,BBK)制定，首先將關鍵基礎設施定義為對一個國家的社會和經濟至關重要的組織，若無法順利營運將嚴重危害公共安全與社會運行。該戰略評估現有措施，並提出建構不同方式及進一步改善關鍵基礎設施防護的作法，主要區分為 3 個面向，預防和減災、建構備援系統及應變能力、強化自我防護能力。

三、 瑞士強化資安防護之挑戰與成功經驗分享

瑞士 2022 年截至第 32 週為止發生的資安事件計有 641 件，其中以網路詐欺(419 件)佔了 65%。為強化資安防護，瑞士聯邦國防、民防及體育部(Federal department of defenc,civil protection and sport)在 2017 年開始推動 CYD 計畫(CYBER-DEFENCE COMPUS)，主講者 Berhard Tellenbach 教授最後結論如下：

(一) CYD 計畫有效強化瑞士的整體資安防護。

(二) 資安研究和創新不是無中生有，需要公私部門合作。

(三) 瑞士政府為了克服相關資安議題挑戰，採取以下方法

1、 建立專門實驗室。

2、 推動獎學金計畫召募國內外人才。

3、 舉辦黑客松競賽(Hackathons)廣邀各領域高手參與集思廣益，解決當前新興資安議題，例如電動車的物聯網安全(IOT SECURITY)

4、 資安工作成功經驗可以指引後人走在正確的道路。

圖 2 瑞士蘇黎世大學教授 Bernhard Tellenbach 談論瑞士政府推動 CYD 計畫

四、 關鍵基礎設施防護脆弱性之研究

(一) 對於關鍵基礎設施脆弱性根因(ROOT CAUSE)可以分成 3 個部分來討論：

1、 容量(capacity)：著重在關鍵基礎設施可維持運作或服務的最重要功能，關注於任務內容的辨識、支援系統的辨識、關鍵基礎設施相依性等議題，這些均與關鍵基礎設施的核心資產、裝備和人員有所關連。

2、 能力(competence)：和內部員工的知識和技能有關，包含操作和管理的屬性，例如維持關鍵基礎設施運作的內部人員責任區分、溝通機制、組織架構、後勤支援制度、外在環境知識等。

3、 成效(performance)：可以視為關鍵基礎設施在各項情況展現的能力以及公私部門合作防護的成效。體現在關鍵基礎設施各項資源(支援)管理的執行成效。

(二) 結論：

1、 關鍵基礎設施脆弱性應該按照系統的特徵或屬性分開評估。

2、 關鍵基礎設施脆弱性評估從以預防為主的途徑逐漸轉變為韌性為主的途徑。

3、 關鍵基礎設施的韌性很大一部分取決於脆弱性辨識的過程是否確實執行。

4、 關鍵基礎設施的脆弱性根因辨識應該從更寬廣的領域去思考，將過去發生過的事件納入考量，這些需要從容量、能力和成效等因子作全面的分析。

圖 3 華沙大學博士候選人 Amelia Tomalska 談論關鍵基礎設施防護脆弱性之研究

五、 混合式威脅和關鍵基礎設施領域-促進關鍵基礎設施實體之情資分享以強化脆弱性和風險評估

本議題主要探討歐盟推的 EU-HYBNET 計畫（授權泛歐網路對抗混合威脅計畫,Empowering a Pan-European Network to Counter Hybrid Threats）。該計畫旨在強化現有的歐洲網路以應對混合式威脅(威脅可能包含政治、經濟、外交、軍事、情報、網路等領域)，並確保關鍵基礎設施的持續運作。透過建構歐洲從業者和其他相關參與者的共同需求以實現。最後增強相關混合式威脅的應對能力、學術研究、創新研發及人員培訓工作。

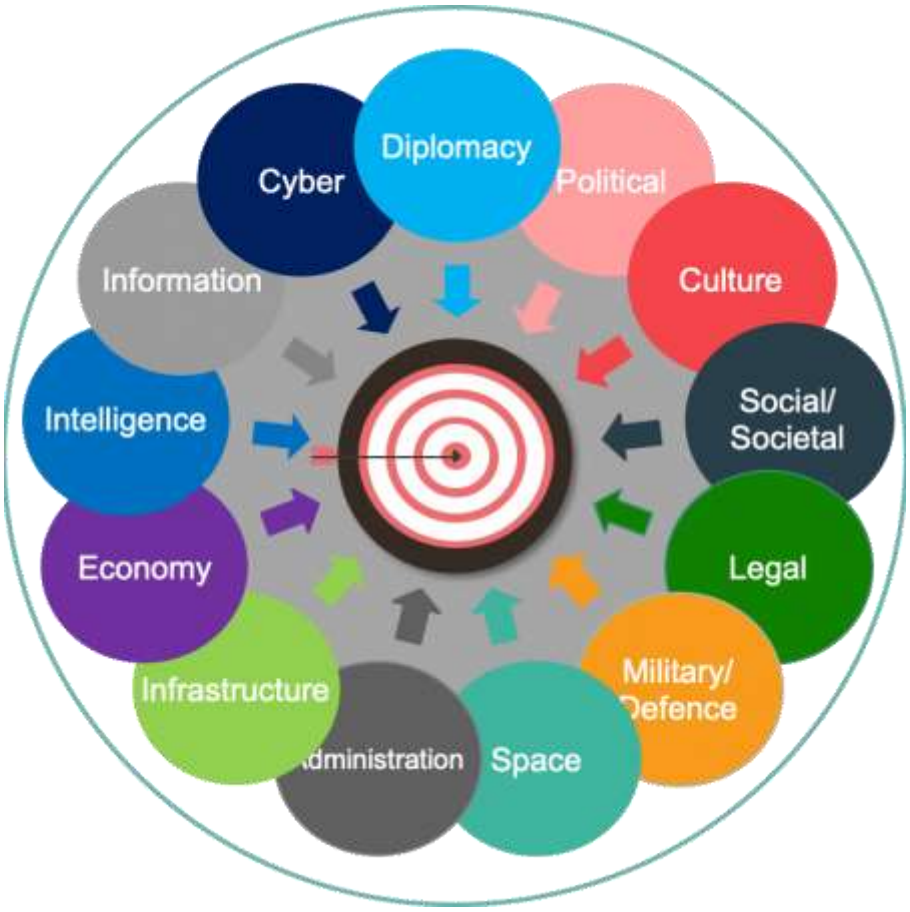

圖 4 混合式威脅領域類別

來源：EU-HYBNET 官網 https://euhybnet.eu/about/#concept

肆、心得

非常感謝內政部警政署給我們這個機會出國獲得新知並促進國際交流，國際關鍵資訊基礎設施安全會議自 2006 年舉辦迄今已逾 15 年，研究領域跨及關鍵基礎設施領域中如先進能源系統規劃、工業控制系統資安防護、城市韌性與減災研究、交通運輸系統安全、設施脆弱性分析與評估、物聯網安全、大數據與人工智慧研究等，並提供平臺供各領域專家、學者聯繫感情，交換實務經驗與心得，以及辦理兼有教育訓練之性質的各式研討會及論壇，並就當前重要資安防護、關鍵基礎設施韌性強化等議題，建立共識、傳遞新知，實對全球關鍵基礎設施整體防護能量之提升，提供相當大的助力。

伍、建議

一、 推動關鍵基礎設施公私部門合作，強化安全意識與反恐應變能力

誠如前述歐盟推動 EU-HYBNET 計畫，瑞士政府推動 CYD 計畫，強化公私部門合作，以因應關鍵基礎設施將面臨之混合式威脅，本署將尋找關鍵基礎設施辦理反恐安全演訓，邀集相關私部門參與，並利用機會進行安全宣導，強化私部門安全意識及危險徵候辨識能力，以降低未來重大危安事件造成之傷害。同時藉由演訓重新審視警察機關應變警力是否充足？現有裝備能否因應實務所需？演訓中獲取的經驗，可作為未來制定標準作業流程之參考。

二、 協助本署駐警之關鍵基礎設施強化脆弱點檢視

本署派駐機場、港口、電力、水庫等重要關鍵基礎設施之警察機關主責治安維護，轄區設施舉凡實體安全維護、犯罪預防、人為危安事件應變及刑案偵辦等係警察職責所在，依問題導向警政理論，針對治安問題採取 SARA 策略如下：

(一)掃描（Scanning）：確認問題(人、事、時、地、物)。

(二)分析（Analysis）：找出問題的範圍、性質和成因。

(三)回應（Response）：針對問題制定因應策略。

(四)評估（Assessment）：評估處理問題的成效。

未來本署責請所轄警察機關協助關鍵基礎設施管理單位針對脆弱點建議設置科技設備，並調整崗哨位置、巡邏路線或增加巡邏班次、巡簽點，以完善安全防護網。

陸、結語

關鍵基礎設施是國家發展的重要基石，正如蔡總統在本(111)年國慶演說提及打造韌性國家，其首要任務就是建立具有韌性的經濟與產業，而確保關鍵基礎設施安全為強化韌性不可或缺的一部分。警察機關在防護關鍵基礎設施扮演了重要角色，未來本署將持續推動與設施管理單位及其他國安單位建立良好的合作機制與默契，以提升關鍵基礎設施整體安全防護能量。