出國報告（出國類別：開會）

參加北約網路衝突國際會議CyCon
出國報告書

服務機關：數位發展部資通安全署

姓名職稱：邱俊惟副組長

蘇煒哲科長

派赴國家：愛沙尼亞

出國期間：**113** 年 **5** 月 **26** 日至 **6** 月 **2** 日

報告日期：**113** 年 **8** 月

摘 要

北約合作網路防禦卓越中心（NATO Cooperative Cyber Defence Centre of Excellence，CCDCOE）係由跨國及跨產業專家所組成，其總部設置於愛沙尼亞首都塔林，提供北約及成員國資安防禦技術、策略、運作及法律方面之諮詢建議，該中心常年舉辦資安教育訓練、研討會、演練等活動，並透過教育、研發、經驗分享及協商等活動，加強北約成員國及合作夥伴資安防禦之能力。CCDCOE 主辦之網路衝突國際會議（CyCon）最早於 2009 年開始辦理，該會議彙集了來自全球知名資安專家學者，並吸引了各國政府、業界和學術界共同參與，促進成員國間充分交流資安議題。

第 16 屆「CyCon 2024」係 113 年 5 月 28 日至 5 月 31 日於愛沙尼亞首都塔林舉辦，以「Over the Horizon」為主題，包含 1 天工作坊及 3 天研討會議，會議議程主要為網際空間議題，主軸圍繞於烏俄戰爭帶來的地緣政治衝突，探討網路於國際衝突中所扮演角色，並從政策、技術及法律面向出發，分享網路行動框架發展、多域作戰能力、跨國合作以及公私協力等議題，共同面對地平線上之各種資安威脅與挑戰，本報告說明本屆會議重點及發現，並提出與會心得與建議，作為主管機關日後推動資安政策及法制規劃等相關工作之參考。

目 次

壹、目的

CCDCOE 成立於 2008 年 5 月 14 日，該中心任務係透過教育、研發、經驗分享及跨國協商等，強化北約成員國及合作夥伴於資安防禦、合作及情資共享能力。該中心作為資安相關事務權威智庫，於戰略、法律、運營和技術領域提供北約組織成員國資安專業知識，其定期舉辦有網路衝突安全會議（International Conference on Cyber Conflict, 簡稱 CyCon）、紅軍十字軍演練（Crossed Swords）及鎖盾演練（Locked Shields）等國際知名活動，並邀請法律專家和政策顧問編撰《塔林手冊》，作為網路戰爭之規範法典。

多年來，CCDCOE 為網路防禦領域提供了全面的視角，持續推動北約國家將網路防禦納入國家治理能力，包含技術、戰略、運營和法律等面向，而 CyCon 作為網路防禦和資安技術、法律、政策、戰略和軍事之重要國際會議，吸引志同道合之國家共襄盛舉。本次第 16 屆 CyCon 研討會亦邀集各國軍方、政府機關及技術單位代表參加與會，計有 600 多名政府代表及專家學者共同研討網路世界衝突問題及因應對策，其 CyCon 所蒐整論文集係由 IEEE 協助，為確保相關學術及研究品質，每年主辦單位係於前一年度 10 月公開徵集研究論文，並由專家學者審查投稿文件，通過審查之論文再依主題區分為決策、法律及技術等面向，邀請作者擔任 CyCon 講者，而本次研討會特收錄我國國家資通安全研究院針對我國運用 AI 於資安檢測等相關研究報告，並由王偉哲研究員進行分享，拓展我國於資安防禦之能見度。

貳、會議經過

一、**會議日期：**2023 年 5 月 28 日至 5 月 31 日，共計 4 日

二、**會議地點：**愛沙尼亞塔林

三、**與會人員：**超過 50 個國家或地區， 600 多名機關代表、法律和技術專家學者。

四、**參與場次表：**

日期	參加場次
5 月 28 日	National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices
	AI in Virtual Manipulation
5 月 29 日	CyCon 2024 Opening Remarks and Cyber Commanders' Panel
	Cyber Threat Intelligence: Public Private Cooperation（Strat）
	Emerging Technologies in International Law: Discussing the Impact of AI and Autonomous Weapons（Law）
5 月 30 日	Cybersecurity and Securing your Critical Infrastructure and Defense Sector
	Algorithms to Armies: How AI Shapes National Security and Cyber Defence
	Compute to Compete: Cloud, AI, and Strategic Competition over Digital Infrastructure
	Future Foresight: Visions of Cyberspace, Methodologies, and Applications（Strat）
	Safeguarding Against Data Misuses in Modern Conflicts（Law）
5 月 31 日	ASIC and QUANTUM Technologies serving National Cybersecurity
	Cyber Defence and Strategic Competition: Adjusting to Unpeace
	Key Questions and Approaches to Building Cyber Resilience
	Closing Keynote

五、會議重點摘要

（一） National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices

1.講者：Dr Ágnes Kasper, Tomohiro Mikanagi, Kerli Veski, John Schabedoth, Dr Talita Dias, Prof. Kubo Mačák.

2.重點摘要：

本次研討會旨在討論各國制定網路空間國際法之國家立場時所面臨主要法律及政策問題，提出對網路背景下關鍵國際規則和原則的解釋，本場工作坊係由英國 Exeter 大學國際法 Kubo Mačák 教授主持，並邀集 CCDCOE 法律處處長 Ágnes Kasper 博士、日本外務省國際法律事務局局長法律顧問兼總幹事 Tomohiro Mikanagi、愛沙尼亞外交部法律司司長 Kerli Veski、德國聯邦外交部網路外交和安全政策協調人員 John Schabedoth、英國皇家國際事務研究所 Talita Dias 博士共同與會討論，會中發表國家立場於法律和政治上之重要性，以及對國際法發展之影響，從而闡述制定國家立場所涉及主權和其他程序問題，以及各國在制定這些立場時面臨的主要法律和政策困境。

會議指出現有國際法針對網路環境的規範仍然是有限的，負責任之國家雖會制訂行為準則並具有約束力，包含官方公開聲明、出版物及政府法律意見書等，針對違反規定之行為，其應負擔相應之國際責任，然而並無強而有力的規約，足供規範其他國家於網路空間之行為，導致部分國家為此爭論不休，此外，在廣泛的國際法中，各國不僅受有國際法管轄制度，其他如維也納條約法公約、日內瓦公約等國際條約亦為管制手段之一，以達到國家行為之問責制度，惟許多國家否認國際法之適用性，由於大量數據跨境傳輸，網路世界難以界定領土主權，造成現有國際法或條約制度適用之困難，例如對他國關鍵基礎設施實施攻擊並造成損害，可能涉及侵犯主權領土，且基於網路行為多樣化，其影響程度各有不同。然《塔林手冊》仍於一定程度提供國際法於網路環境一般性原則，以解決國家於網路空間活動所涉及國際法問題。

圖 1 會議過程

（二） AI in Virtual Manipulation

1.講者：Dr Eduard Barbu, Dr Gundars Bergmanis-Korats, Dmytro Plieshakov, Dr Yukai Zeng

2.重點摘要：

本次研討會係由北約戰略通信卓越中心高級專家 Yukai Zeng 博士主持，並由 Tartu 大學自然語言處理（NLP）專業研究員、北約戰略通信卓越中心首席科學家 Gundars Bergmanis-Korats 博士，以及 Osavul（AI 科技公司）首席執行官兼聯合創始人 Dmytro Plieshakov 與會，共同討論人工智慧於虛擬操作之應用。

會議著重探討人工智慧於資訊戰日益增長之重要性，並指出其應用於戰略通訊之作用，並將認知效應與動態活動連結起來，於此種情形下，人工智慧技術發展大大影響了資訊環境，與會專家提出人工智慧在戰略應用中日益增強之實際影響，特別是人工智慧機器人及大數據之使用，亦為防禦方帶來新的挑戰和機會。此外，會議另提出人工智慧技術造成近期資訊戰

策略之轉變，包括人工智慧於以色列-哈馬斯衝突、烏俄戰爭等武裝衝突應用，其利用社群媒體平臺作為宣傳工具，企圖帶來更廣泛影響，並透由本次分享加深我們對人工智慧為虛擬操縱和資訊戰領域之理解，剖析其所帶來之複雜挑戰。

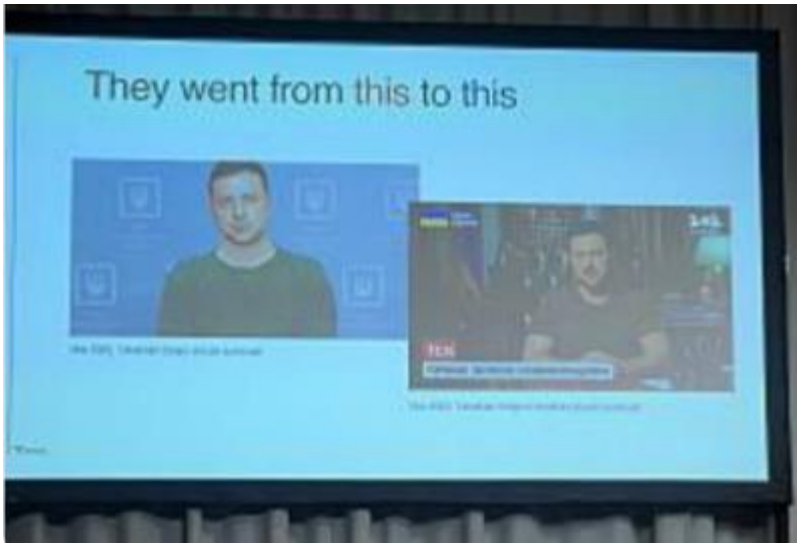

圖 2 深偽影片應用於烏俄戰爭

（三） CyCon 2024 Opening Remarks and Cyber Commanders' Panel

1.講者：Maj. Gen. Kimura Akitsugu, Maj. Gen. Ana Duncan, Lt. Gen. Kevin B. Kennedy, Vice Adm. Javier Roca, Dr Mart Noorma

2.重點摘要：

每年來自盟國和北約成員國 30 多名國家齊聚塔林參與 CyCon 會議，分享各國建設國家資安防禦所面臨之挑戰和機遇。本次會議係由 CCDCOE 主席 Mart Noorma 博士為本次第 16 屆 CyCon 開場，並邀集日本自衛隊網路防禦司令部（JCDC）司令官 Kimura Akitsugu 中將、澳洲國防部網路司令部司令 Ana Duncan 少將、美國空軍網路司令 Kevin B. Kennedy 中將，以及西班牙聯合網路空間司令部司令 Javier Roca 中將共同與會。

首先西班牙 Javier Roca 中將表示於數位時代中，政府及私人企業都極

度依賴網路，該國海軍不論通訊、導航或者作戰系統皆須仰賴安全可靠的網路環境，因此為強化防禦機制，需引入相關技術外，更需打破政策或法律之限制，從過去知悉情資轉換為分享之責任，以對抗危機或衝突。日本 Kimura Akitsugu 少將亦提及，日本防衛省於 2024 年投入 AI 之預算達到 9800 萬歐元，用以進行自動化決策、分析及社群媒體等，並著重於關鍵基礎設施、供應鏈及太空之網路安全。而澳洲 Ana Duncan 少將表示該國考量地緣戰略情況，成立了網路空間司令部，並提出各國政府須負起責任且遵循法律道德之原則，執行網路維運相關事務。最後，美國空軍網路司令 Kevin B. Kennedy 中將說明，對於全球合作夥伴來說，網路領域至關重要，未來將持續應用 AI 技術來防止對手的攻擊，達到識別、定位、並採取相應的行動。

此外，針對近期烏俄戰爭也帶來不同面向之具體經驗，例如關鍵基礎設施防護、網路攻擊、認知作戰等攻擊手法，各國亦討論到網路作戰人員與一般作戰人員所需技能不同，因此會有相應之培訓方式，例如美國係採集中訓練並以模組化課程方式，迅速引入所需技能，而 CCDCOE 亦有舉辦鎖盾演練（Locked Shields），參加人員計有 500 多人，最後各國也討論到留任留才之作法，例如軍民轉換制度、職能培訓機制，以及提高待遇等方式，期能留住軍方適任人才。

圖 3 CCDCOE 主席 Mart Noorma 博士

圖 4 會議過程

（四） Cyber Threat Intelligence: Public Private Cooperation （Strat）

1.講者：Neil Ashdown, Dr Jamie Collier, Geirr Andrew Trotter, Miriam Howe

2.重點摘要：

本次會議係由 BAE Systems 數位智慧國際諮詢主管 Miriam Howe 主持，並由倫敦皇家霍洛威大學 Neil Ashdown 博士、Google Cloud 歐洲首席 Mandiant 威脅情報顧問 Dr Jamie Collier 及挪威國家網路安全中心首席運營官 Geirr Andrew Trotter 共同與會。講者論及隨著網路服務盛行，各國關鍵基礎設施提供者多由私部門運營，私部門具有多樣化特性，包含惡意軟體、逆向工程，乃至於外語專業等由不同專業知識及技能人員所組成，並握有相關情資，而政府角色已經轉變為情資蒐集者，又同為情資之分析者，考量軍方作為層次分明且具有指揮的統一性，與私部門環境相當不同，公私二者之間具有不同特性，爰此，與會人員提出公私協力下所面臨之挑戰，包含政府如何推動私部門當責，進而促使私部門保護自身資安，對其所維運之關鍵基礎設施負起安全管理責任，並要求資安事件回應及分析，以利 ISAC 或其他機構彙整分析資訊，方能達成共享情資。相較一般公司而言，跨國企業因可能面臨中國、蘇俄勒索軟體及地緣政治關係等風險，更為重視資安。

實務上私人公司與國家網路中心建立合作關係時，需事先達成協議，但與初次合作之私人企業合作時，常出現分享意願較低、公司規模不足、不清楚情資分享界線等問題，因此事前需培養關係，當事件發生時國家協助提供所需資訊，事後分享情資，透過長時間合作、相關經費投入，並建立國家與私人信任之合作關係。最後，講者分析於國家衝突下政府因國家利益而驅動，私部門則基於利潤而採行相關措施，公私部門從競爭到危機，所蒐集情資終將流向政府機關，逐一分析公私協力合作之可能性。

圖 5 挪威國家網路安全中心首席營運官 Geirr Andrew Trotter

圖 6 會議過程

（五） Emerging Technologies in International Law: Discussing the Impact of AI and Autonomous Weapons （Law）

1.講者：Dr. Jonathan Kwik, Prof. Scott Sullivan, 王偉哲, Taylor Woodcock, Prof. Kubo Mačák,

2.重點摘要：

因應人工智慧技術整合至武器系統中，人工智慧和自主武器等新興技術的快速發展，此變化正在重塑國際法，其有可能對軍事行動中的決策和指揮責任產生重大影響。而本次工作坊小組係由英國 Exeter 大學國際法教授 Kubo 主持，並由國家資通安全研究院研究員王偉哲、T.M.C. Asser 研究所博士後研究員 Jonathan Kwik、美國軍事學院 Scott Sullivan 教授、阿姆斯特丹大學博士研究員 Taylor Woodcock，共同討論新興技術發展對國際法影響。

首先由資安院王偉哲研究員介紹我國資安法要求納管機關之資安管理作為，討論將 AI 技術應用於安全性檢測等法遵應辦事項，透過自動化分析有助於機關產製報告、改善分析，以強化機關資安管理，惟相關技術使用如有損害事件發生時，該技術無法成為責任主體，因此供應商或使用者之角色皆有可能為究責主體。為此，我國現行尚無相關立法，後續將逐步建立

相關法制作業，並提供低風險的人工智慧技術列表等，仍是未來需持續努力推動之方向。

接著 T.M.C. Asser 研究所博士後研究員 Jonathan Kwik 分享人工智慧支援軍事活動，其所涉及國際人道法之相關問題，AI 應用於軍事方面係以自主武器系統為最大宗應用，例如音樂播放平臺會隨著自身音樂聆聽習慣，透過 AI 識別模式及演算邏輯建立專屬的音樂清單。又如美國及以色列刻正利用 AI 技術建置即時作戰情報引導系統，以自動建立軍事決策及行動，而這些武器是否合於國際人道法之規範，過去十年內仍然爭論不休，其中主要爭點為代理權關係及責任主體，因此使用這些技術應用於軍事決策，仍需考量人道主義以及其他文化關係之衡平。此外，人工智慧缺乏透明度或可解釋性，使用者往往過度依賴演算法，但無法了解資料產製之原因，爰此，AI 技術所做成決策與個人所為決策有本質上的不同，國家透過人工智慧所為軍事活動，仍需審慎評估其法律關係。

美國軍事學院 Scott Sullivan 教授提到人工智慧與自主武器之影響，於以色列-哈瑪斯衝突中，以色列利用人工智慧技術提高打擊目標數量，並透過該技術自動分析軍事情資是否屬實，而其決策過程宛如黑盒子，自動化武器系統如何區分戰鬥人員和平民，往往難以直接得知其運算過程，以加拿大為例，該國於法律規定指揮官需採取適當措施來保護平民或民用物資，於軍事行動使用 AI 技術仍需小心謹慎，以免擴及平民及其財產，相關規定應廣泛要求至各國，方能履行基於國際人道法之法遵義務。

最後，由阿姆斯特丹大學博士研究員 Taylor Woodcock 分析自主武器攻擊範圍，其與網路攻擊具有程度上差別，網路攻擊所產生結果傾向資料破壞，與國際人道法所稱「攻擊」有所不同，因此於會議中分析自主攻擊定義及決策之時點，其認為「攻擊」為特定的軍事行動，於空間或時間受有接近性之限制，進而從法律層面分析軍事行動應用人工智慧於自主武器之攻

擊行為及次數。

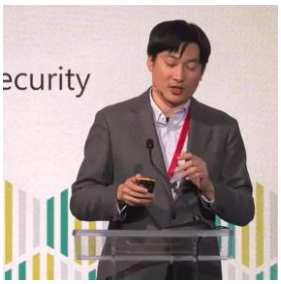

圖 7 國家資通安全研究院王偉哲

圖 8 會議過程

（六） Cybersecurity and Securing your Critical Infrastructure and Defense Sector

1.講者：Jeff Foley, Siemens, Digital Industry

2.重點摘要：

西門子數位工業部經理 Jeff Foley 分享關鍵基礎設施和國防單位之工控領域資安，考量現行製造業、食品、製藥、水資源及其他公共事務等皆需仰賴工控系統，其威脅日益劇增，而工控系統由於資產生命週期、相異性、注重可用性，以及保護風險等 4 個因素，造成工控資安相對脆弱，雖然歐盟網路韌性法案（Cyber Resilience Act）及 NIS2 指令已將強化關鍵基礎設施之保護作成規範，惟大多數公司僅著重法規之合規性，強調形式主義，實質上並未將人力經費等資源成本投入至 OT 資安防護作為，故其防護成效仍然有限，講者以美國為例，歐巴馬於 2015 年簽署法案要求保護關鍵基礎設施，確保電力系統之安全，甚至需提供文件、設定或其他資料佐證資安管理作為，惟真正促使電力公司落實資安原因為後續發生資安事件時，每天最高可能被處以 100 萬美元罰款，敦促公司需有效強化其資安管理作為，此外，講者列舉了 IEC 62443、NIST CSF2.0、ISO27001、ISO27002 等作為資安標準或者框架，提供關鍵基礎設施提供者加以遵循。

其次，講者提出如何應用 AI 技術於 OT 之自動化弱點更新，並舉例有公司執行自動化更新後，造成系統停電失效，也因此組織針對弱點並非僅僅執行修補，更需考量 OT 系統之特殊性，審慎評估更新後所造成影響。此外，西門子公司於 2018 年提出信任憲章（Charter of Trust），作為業界致力於提升資安之共同憲章，並制定 10 項關鍵原則供業界加以遵循，其中最為重要的原則為保護個人和企業的數據、防止對人員、企業和基礎設施造成損害，以及在數位世界中建立信任等 3 項原則，並將 SSDLC 概念融入產品開發，其將 IT 和 OT 之資安標準放在一起比較，相較 IT 重視系統之靈活性，OT 更注重系統可擴展性及可用性。最後，講者介紹零信任技術將防禦從靜態的、基於網路邊界，轉移到使用者、資產和資源，並分享專為 OT 環境協定設計之偵測工具，使用 OT 自動化即時偵測和自動回應等操作，以提升 OT 資安防護。

圖 9 講者 西門子經理 Jeff Foley

圖 10 會議過程

（七） Algorithms to Armies: How AI Shapes National Security and Cyber Defence

1.講者：Amy Hogan-Burney, General Manager and Associate General Counsel for Cybersecurity Policy & Protection, Microsoft

2.重點摘要：

微軟網路安全政策與保護總經理兼副總法律顧問 Amy Hogan-Burney 分享 AI 於國家安全與資安之應用，該公司目前掌握到伊朗、中國、蘇俄等駭客組織所展開的密碼攻擊，企圖破解身分驗證機制，微軟目前已追蹤約 300 種不同的資安威脅，其中包含勒索軟體或出於經濟考量之駭客組織，甚至是國家層級資安攻擊，尤以蘇俄及伊朗之攻擊行為最為顯著，攻擊對象包含政府、關鍵基礎設施或其他非政府組織等。就蘇俄來說，駭客集團所攻擊對象不限於烏克蘭(48%)，並包含烏克蘭盟友，例如 NATO 成員國(36%)、歐洲各國（4%）等，依照微軟針對駭客組織分類方式，針對風暴（Storm）集團所做的攻擊，多為電子郵件或釣魚郵件等社交工程攻擊，並利用漏洞等多樣化方式植入勒索軟體，以攻擊組織之資通系統，且其威脅影響力日益增長。此外，微軟也觀察到駭客組織利用 AI 生成的內容，包含深偽影片、靜態圖片 、大型語言模型發動社交工程，或改進軟體腳本開發有效惡意軟體等新興資安威脅，試圖跟上防禦方腳步，甚至在其之前發動攻擊，因此微軟致力與政府機關或其他私人機構合作，確保組織擁有更好的數據情資來源、良好的基礎設施，以及更多創新保護。而防禦方亦可善用 AI 技術於事件彙整、影響評估、腳本逆向工程、回應處理等 4 個面向。最後，講者提到微軟於 2024 年 2 月與 OPEN AI 合作分享情資，分析相關威脅並採行適當行動以快速因應，後續亦將持續發展人工智慧創新並促進競爭，履行法律規定義務，與客戶、社區和國家合作，推動人工智慧合作夥伴關係，積極主動地解決問題。

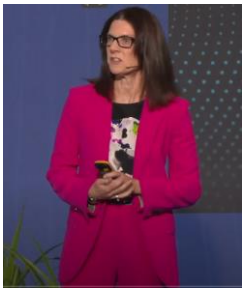

圖 11 講者 Amy Hogan-Burney

圖 12 會議過程

（八） Compute to Compete: Cloud, AI, and Strategic Competition over Digital Infrastructure

1.講者：Julia Carver, Taylor Roberts, Emma Schroeder, Max Smeets, Trey Herr

2.重點摘要：

本次會議係由 American 大學國際服務學院全球安全與政策助理教授 Trey Herr 主持，並由牛津大學歐洲網路安全研究員和政治學講師 Julia Carver、Intel Corporation 全球安全政策總監 Taylor Roberts、大西洋理事會副主任 Emma Schroeder、蘇黎世聯邦理工學院安全研究中心高級研究員 Max Smeets，共同討論雲端服務、AI 和數位基礎設施之戰略競爭。

在當前的戰略競爭時代，數位基礎設施通常係以國家或跨國公司聯繫在一起，無論是全球規模的雲端服務或是新興之人工智慧技術，從現代銀行至軍方武器系統，一切皆需依賴數位基礎設施。對這些基礎設施的存取控制及限制之競爭，正密切地劃分戰線，甚至於國際盟友和夥伴之間亦是如此，而優先主導半導體、人工智慧支援的大規模數據處理和雲端基礎設施等業者，將為國家和公司創造更多經濟和戰略優勢。

未來計算能力只會變得更加重要，成為國家安全及公共服務之核心技術，因此越來越多國家通過制定國家戰略來應對這場技術競爭，透過投資關鍵技術來建設自身能力，支援國內雲端服務發展，並分配政府資源以加速人工智慧的發展，同時將關鍵技術作為國家之戰略資源。

圖 13 American 大學助理教授 Trey Herr

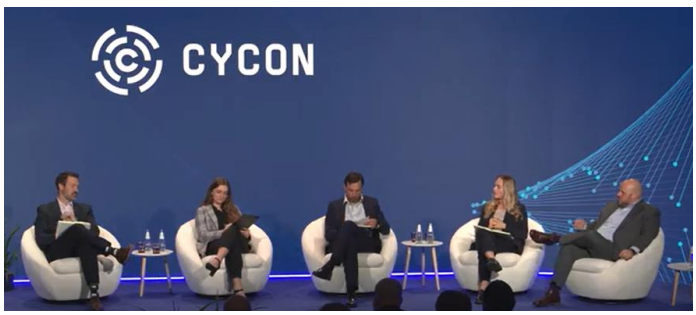

圖 14 會議過程

（九） **Future Foresight: Visions of Cyberspace, Methodologies, and Applications（Strat）**

1.講者：Ludovic Chaker, Chris Fall, Prof. Herb Lin, Giacomo Persi Paoli, Ingrid Winther

2.重點摘要：

本次會議係由挪威武裝部隊 Ingrid Winther 主持（CCDCOE 前挪威特使），並由法國軍備部副部長 Ludovic Chaker、MITRE Corporation 應用科學副總裁 Chris Fall、史丹佛大學 Herb Lin 教授、聯合國裁軍研究所安全和技術方案負責人 Giacomo Persi Paoli 共同與會，討論網路空間的願景、方法和應用。

全球網路日益複雜，這 20 年來電腦計算能力大幅提升，也促使用戶數不斷攀升，而有心人士可能透過應用程式、網路服務等作不當利用，因此各國都需要為未來做規劃，政策制定者擬定戰略以因應未來技術發展及風險可能性，並提出更好的應對措施，諸如 6G 的發展、AI 技術應用，將對使用網路空間之個人、社群，乃至於政府國家都將造成影響，形成新的地緣政治關係。其中法國政府為因應未來趨勢，預計組建一支「紅隊」，將招募科學家、軍事專家和未來學家等，透過角色扮演或其他方式，預測 2030 年至 2060 年的潛在威脅，以及敵對勢力可能採用的攻擊行動，因此法國政府順勢提出「Combat Horizon」計畫，其涵蓋 6 個月至 10 年之時間範圍內，致力於工業、科技領域之戰略預測，並為 2024 年奧運做準備，防範激進勢力、間諜情蒐乃至於國家網路安全戰略預為準備，提出戰略預測和應用於網路衝突的未來，以及實踐之創新方法。

圖 15 史丹佛大學 Herb Lin 教授

圖 16 會議過程

（十） Safeguarding Against Data Misuses in Modern Conflicts（Law）

1.講者：Tatjana Grote, Petra Mahnič, Anastasia Roberts, Hele Jonsson

2.重點摘要：

本次會議係由 Telia Company 副總裁兼集團隱私、安全和 AI 法律主管 Hele Jonsson 主持，並由 Essex 大學博士研究生 Tatjana Grote、歐盟理事會法律顧問 Petra Mahnič、獨立法律顧問 Anastasia Roberts 與會，共同討論防止現代衝突中資料濫用問題。

網路運營可以利用各種技術來產生效果，於烏俄戰爭中，透過軍事網路行動中收集之個人數據可用於恐嚇對手、傳播虛假資訊、破壞敵對政營士氣等，相關技術也可以用來操縱甚至對平民造成傷害，舉例而言，美阿戰爭中，美國武裝部隊建置生物辨識資料庫，其登載了 80%阿富汗人相關資訊，以阻止叛亂份子之活動，同樣這些情況亦出現於以色列、巴勒斯坦、伊拉克，甚至是烏克蘭地區之武裝衝突，此種對他國資料蒐集及控管之問題，涉及國際人權之問題，而國際人權法（International Human Rights Law，IHRL）、國際人道法或日內瓦公約等，主要由條約、主權國家之間的協定組成，對於締約國間具有約束力之法律效力，而武裝部隊雖然控制了部分領土，對個人數據的使用也不能不受限制，仍然具有資料使用上應遵循之義

務，包含相關數據不得用以傷害或懲罰個人，並需注意不得違反上述相關規定，惟現行規定仍有未明之處，例如隱私權與表意之自由權於國際人道法並無直接規範，尤其戰爭時期平民仍然需要資訊以保護自己，例如安全區、疏散路線及醫療資訊等，避免被錯假訊息侵擾或干預重要資訊發布等，而國際人權法主要規制一國在和平時期對其人民的行為，傳統上被視為與衝突期間國際人道主義法規範之行為有所不同。儘管這二者法律目的不同，但於某些議題仍可達到互補甚至是重疊規範，該小組透過討論分享網路空間軍事心理行動之法律框架，以及武裝衝突時期的數據保護。

圖 17 Telia Company 副總裁 Hele Jonsson

圖 18 會議過程

（十一） ASIC and QUANTUM Technologies serving National Cybersecurity

1.講者：Luca Iuliano, Dr Roberto Piazza

2.重點摘要：

在本次演講中，講者重點提到各國必須做好風險的安全評估，以保護「網路邊界」和「Physical access」（包括 SCADA、OT 和物聯網），而 Telsy 公司開發之技術將有多種應用方式，包含安全微晶元、專用積體電路（ASIC）、量子密鑰分發、加密器和決策智慧等，其技術應用於行動裝置、無人機控制、鐵路系統，以及其他關鍵基礎設施等，並介紹該公司將 ASIC

和 QUANTUM 技術應用於國家網路安全。

圖 19 講者 TIM Group Telsy 工程總監 Luca Iuliano

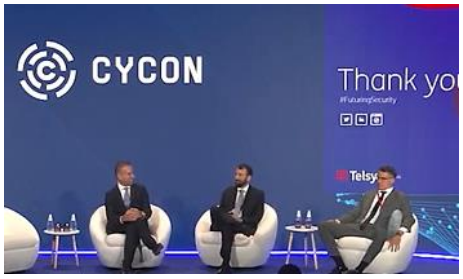

圖 20 會議過程

（十二） Cyber Defence and Strategic Competition: Adjusting to Unpeace

1.講者：Prof. Greg Austin, Dr Emily Goldman, Christian-Marc Liflände r, Dr Claire Kwan

2.重點摘要：

本次會議係由盧森堡於 CCDCOE 之高級國家代表 Claire Kwan 博士主持，並由雪梨科技大學兼任教授 Greg Austin、美國網路司令部戰略專家 Emily Goldman 博士、北約新興安全挑戰司網路和混合政策科科長 Christian-Marc Liflände r 共同與會，討論資安防禦和戰略競爭以適應不和平。

在烏俄戰爭的背景下，各國開始關注到軍事於網路空間能力之發展趨勢，每年於資訊與網路安全投入相關預算，且更為重視網路韌性，日本、澳洲軍事單位將招募更多人員從事資安相關工作，除此之外，日本將編列 5 億美元預算，投入 AI 技術於網路運營，甚至是國家安全與國防相關事務，而中國因應相關情勢變化，於今年 4 月組建了信息支援部隊，勢必對我國、美國及其盟友造成威脅，且不應指望中國採行與和平時期相同之網路行動，雪梨科技大學兼任教授 Greg Austin 直言中國將以高度的心理戰為主導，並對我國關鍵基礎設施展開多波攻擊。此外，此次烏俄戰爭中，蘇俄於網路空間遭受歷史最強大的網路聯盟攻擊，包含美國、北約盟國、烏克蘭等，相較

蘇俄於實體上之堅強軍事實力，其網路空間之實力相對脆弱，同樣中國目前觀測到的網路空間實力仍有所欠缺，但北約聯盟亦有待加強之處。

美國 Emily Goldman 博士指出網路行動已與外交息息相關，敵對勢力可於不冒軍事風險之前提下，利用網路攻擊帶來國家相當損失，尤其武裝衝突後之惡意活動皆屬常規，因此美國於烏俄戰爭後反思，如何減少戰略損失或是阻止資安事件發生，提出公私合作強化夥伴關係，共享相關情資，以因應對手各種威脅。隨著數位發展，網路空間已成為各國活動舞臺之一，除了北約聯盟外，亞太亦有日本、印度、美國及澳洲組成聯盟，共同強化於網路空間之行動，該小組討論了網路空間持續緊張局勢、後續軍民合作、立法框架，以及在國家安全和個人公民自由之間取得適當平衡。

圖 21 講者

Claire Kwan 博士

圖 22 會議過程

（十三） Key Questions and Approaches to Building Cyber Resilience

1.講者：Jim Richberg

2.重點摘要：

本次演講係由 Fortinet 網路政策主管和全球現場首席資訊安全官 Jim Richberg 分享網路韌性已成為國家戰略和國際上日益重視之課題，講者分享其 40 年來參與資安工作，以及制定戰略和實施之經驗，並針對提升網路韌性之方法提出 5 項原則，第一為瞭解關鍵技術趨勢，盡可能做到技術上能因應之工作，例如零信任、SOC 自動化等；第二、針對威脅持續驗證資安需求，政府或關鍵基礎設施提供者需注意身分驗證管理、存取控制、漏洞

修補、網路分段，並制定及實施資安應變計畫等；第三、利用具有廣泛適用性之安全解決方案，評估相關方案成本效益及影響力，例如採行零信任技術、網路安全網狀架構，並以誘捕技術發現駭客或敵對勢力等；第四、認知到 AI 於大數據之應用，現行 AI 判別技術逐漸成熟，可用於預測等自動化判釋，縮小勞動力不足或個人專業技能所帶來影響，但需注意 AI 技術也同時帶來前所未有的能源需求；第五、對安全設計的新興關注，IT 設備製造商有責任為產品進行安全設計，不論北約或者美國皆重視供應鏈安全，於今年 RSA 亦由業者簽署相關文件，致力於實現產品安全。綜上，講者透由上述 5 點原則分析現有技術趨勢將更有成效解決未來技術所面臨機遇挑戰和風險，以及相關因素對資安之影響。

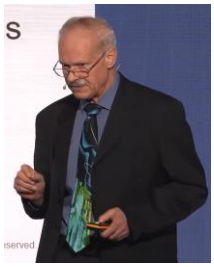

圖 23　講者 Jim Richberg

圖 24　會議過程

（十四） Closing Keynote

1.講者：Prof. Herb Lin

2.重點摘要：

史丹佛大學教授 Herb Lin 首先提到網路空間之威脅，可區分外部威脅及內部威脅，外部威脅包含蘇俄、中國、伊朗、北韓或者恐怖組織、跨國犯罪集團等，而內部威脅包含不肖組織成員、國內極端組織、易受騙消費者、媒體等，這些威脅所採取手段可能有網路攻擊、竊取資訊、間諜程式、錯假訊息，甚至透過人工智慧增強對手能力，並減弱我方適應力。此外，隨著系統功能的增加，必然帶來程序相關事務的複雜性，但人們對於管理程序資

訊之認知有其上限，並且考量複雜系統有許多潛在的交互作用及影響，勢必對安全性造成影響，因此簡化與重新設計業務流程有其必要性，以獲得相同級別功能而其程序相對簡單之系統。講者對此提出實現安全性及韌性之方法，除以功能需求設計系統外，亦需於開發時從需求面要求安全地設計系統，並且在性能要求及安全性之間進行權衡。

其次，講者分享到現今訊息之生態系統中，好與壞的訊息皆非常豐富，使用者於評估和使用資訊時可能會犯下錯誤，舉例而言，搜索引擎係根據受歡迎程度，而非以事實相關性回饋結果，也因此社群媒體增強了虛假、誤導或無價值訊息之可見性，此種以低成本與大量人群溝通，且無需承擔責任，乃為現行威脅之一。

接著，講者論及軍事背景下 AI 技術之威脅，以及對於軍事行動的影響，例如透過自動化或機器人技術，改進了紅隊及兵棋推演，將更有效區分或針對目標，其次係來自對手的戰略威脅，其利用 AI 技術達到持續監視機關或戰略部隊，提高分析能力等，再者說明自身使用 AI 之風險，例如有缺陷或不適當之技術部署，將造成分析偏誤或過度依賴，且其具有缺乏可解釋性、可理解性之特性，皆有可能增加使用者風險。最後，講者提到組織治理必須相應調整，高層主管應了解安全基礎知識，而首席執行長則需要於功能性及安全性間作出權衡，理性思考相關 AI 技術應用，並評估其所帶來的風險。

圖 25 講者 Herb Lin 教授

圖 26 會議過程

參、心得與建議事項

本屆 CyCon 會議主題為「Over the Horizon」，各成員針對全球國家安全及資安議題，包含 AI、關鍵基礎設施安全、網路韌性等進行討論，主軸圍繞於地平線上各種衝突，包含烏俄戰爭帶來的地緣政治威脅，探討各國於網路空間所扮演角色。此外，因應新興科技發展趨勢，各國政府機關代表、專家學者亦於會議中討論 AI、後量子密碼等技術所帶的數位衝擊與影響，包含國家戰略規劃、技術因應作為，以及法制衝擊影響評估等。透過本次會議觀察國際資安政策演變，據以檢視我國資安法制發展現況，滾動檢討現行機制，進而提出前瞻發展方向，相關重點及建議如下：

1. 技術面：人工智慧技術發展、關鍵基礎設施威脅

因應人工智慧技術快速發展，該技術將成為各國國家安全及公共服務之核心技術，透過 AI 識別模式及演算邏輯建立，可減低所需勞動力，大幅提升作業品質，甚至用以支援軍事活動，惟近期地緣政治衝突中，觀察到敵對勢力利用 AI 技術進行網路攻擊，包含製作更為擬真之釣魚郵件、大型語言模型發動社交工程攻擊、自動開發有效惡意軟體，甚至透過深偽影片、擬真圖片等方式，企圖操作民意及影響輿情，面對日益複雜的網路攻擊，國家應制定國家戰略或資通安全發展方案來應對這場技術競爭，透過投資關鍵技術來發展自身能力，支援國內雲端服務發展，並分配政府資源以加速人工智慧的發展，同時將關鍵技術作為國家重要戰略資源。

而各國關鍵基礎設施安全，包含製造業、食品、製藥、水資源及其他公共事務等領域大多依賴工控系統，由於工控系統的資產生命週期、異質性、可用性以及風險等 4 個因素，使得工控系統的資安相對脆弱，為此，歐盟網路韌性法案（Cyber Resilience Act）及 NIS2 指令已經對強化關鍵基礎設施保護制定規範，但大多數關鍵基礎設施提供者僅關注於

法規之合規性，實際上並未將人力和經費等資源投入到 OT 資安防護上，因此建議關鍵基礎設施提供者應遵循 IEC 62443、NIST CSF2.0、ISO27001、ISO27002 等資安標準及框架外，並可評估使用 OT 環境協定設計之偵測工具，利用自動化即時偵測和自動回應等操作，以提升 OT 資安防護。

此外，弱點修補管理仍為組織應注意重點之一，現今駭客組織已趨向專業化及組織化，透過社交工程郵件、勒索軟體等攻擊手法，以獲取更大報酬，直至漏洞無法再利用，爰此，除應強化供應鏈安全管理外，並將 SSDLC 融入至系統開發生命週期，此外，各中央目的事業主管機關針對特定類型資通系統（包含工控系統）之防護基準，應持續要求納管對象加以落實，包含漏洞管理、網路區隔、定義邊界等，後續並由中央目的事業主管機關透過稽核或演練方式，加強檢視關鍵基礎設施資安防護基準落實程度。

2. 政策面：公私協力、資安人才培育

因應烏俄戰爭，各成員國逐漸關注到地緣政治對網路空間之威脅，由於數位時代中，不論政府及私人企業都極度依賴數位服務，為強化相關防禦機制，應課責公私部門負有情資分享責任，考量私人企業係基於利潤而驅動，而國家須為國家整體利益採行相關作為，因此應完善政策及立法，強化公私協力合作，以對抗危機或衝突。對此，我國資安法納管機關除應依資通安全情資分享辦法進行情資分享外，應持續推動非公務機關加入 TWCERT/CC，結合產官學研各界資安能量，建立跨國網路安全情資共享管道，共同提升我國私部門資安聯防與應變能力。

此外，各國考量到關鍵基礎設施防護、網路攻擊、認知作戰等風險趨勢，諸如中國、澳洲、日本政府機關或軍事單位皆相應之組織調整，惟政府或軍事單位所需資安人員、網路作戰人員與一般企業資安人員所

需技能不同，且考量資安人才不足為各國所面臨問題，後續除應建立模組化課程，提供在學、在營及在職所需技能，並強化軍民轉換制度、職能培訓機制，以及提高待遇等方式，期能達到留任留才，並完善我國資安人才生態系。

3. 法規面：AI 立法、網路行為當責性

AI 技術用以自動化分析資安情資，有助於機關執行決策，提升分析效果，並強化機關資安管理，惟損害事件發生時，AI 技術無法成為責任主體，仍須透過立法加以規範，考量人工智慧技術缺乏透明度或可解釋性，倘使用者過度依賴演算法，而無法了解資料產製之原因，甚有技術濫用之虞，因此後續應建立風險列表，透過資安分級及防護措施，確保系統穩健性及安全性外，更須尊重基本權利及文化價值，避免不公平及歧視，且針對人工智慧產出結果應予以適當資訊揭露或標記，以強化其透明及可解釋性，俾利使用者評估可能風險，並了解對相關權益之影響。

此外，網路空間與各國息息相關，由於大量數據跨境傳輸，網路世界難以界定領土主權，造成現有國際法或條約制度適用之困難，且考量國際法針對網路環境的規範仍然是有限的，仍須由各國制訂行為準則，並針對違反規定之行為，負擔相應國際責任，包含武裝衝突中應避免利用 AI 技術傳播虛假資訊，使一般民眾人身財產造成損害，或對他國關鍵基礎設施實施攻擊之行為，可能涉及侵犯主權領土，由於網路行為多樣化，其影響程度各有不同，各國有義務告知在其管轄下的個人行為的法律效果及影響，以符合國際人權法、國際人道法、日內瓦公約等相關規範，而《塔林手冊》仍然於一定程度提供國際法於網路環境一般性原則，以解決國家於網路空間活動所涉及國際法問題。

4. 深化國際合作

近期烏俄戰爭、以色列-哈馬斯衝突，乃至於我國與大陸地區之地緣政治關係，皆屬本次會議討論重點之一，尤其大陸地區於今年 4 月組建信息支援部隊，推測其可能採行進一步之網路行動，勢必對我國、美國及其盟友造成威脅，為此，CCDCOE 除持續透過教育、研發和協商等方式，加強北約成員國及合作夥伴在網路防禦方面之能力、合作及資訊共享外，亞太亦有日本、印度、美國及澳洲組成聯盟，共同強化於網路空間之行動。

而本次會議特由國家資通安全研究院針對我國運用 AI 於資安檢測等相關研究進行報告，以增加我國於資安之能見度，後續除應持續深化與北約聯盟、CCDCOE 交流合作外，我方亦介紹我國的前瞻資安探索會議（Advanced Cybersecurity Exploration Conference, ACE ），將於今年 11 月於臺北舉辦，我方誠摯邀請各夥伴派員參加，或可參加主題演說發表，各友方表示會將進行評估、考慮指派適當人員出席等，俾後續推動資安政策交流合作。

圖 27 本國參與會議人員合影

圖 28 我方參與人員致贈 CCDCOE 主席 Mart Noorma 博士禮物合影