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：鄭欣明副署長

林逸塵副組長

李敏瑜分析師

派赴國家：愛沙尼亞

出國期間：112 年 5 月 28 日至 6 月 4 日

報告日期：112 年 8 月

摘 要

網路衝突安全會議(CyCon)最早於 2009 年由北約合作網路防禦卓越中心(Cooperative Cyber Defence Center of Excellence, CCDCOE)開始辦理。CCDCOE 總部設置於愛沙尼亞首都塔林，由跨國與跨產業專家所組成，主要任務是結合跨學科的網路防禦研究、辦理資安培訓、演練活動及相關議題研究，以支援北約及其成員國，並提供北約組織成員國網路防禦技術、策略、運作及法律方面之諮詢建議，促進成員間在網路安全議題能夠充分交流。

第 15 屆「CyCon 2023」於 112 年 5 月 30 日至 6 月 2 日於愛沙尼亞塔林舉辦，以「Meeting Reality」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，探討在承平時期及危機衝突時期之可採取因應作為。「Meeting Reality」主要是呼應烏克蘭戰爭帶來新的地緣政治衝突，各國夥伴結盟共同討論在此背景下面臨之挑戰。本報告說明本屆會議重點及發現，並提出與會心得與建議，可作為日後主管機關後續推動相關工作之參考。

目 次

壹、目的

北約合作網路防禦卓越中心(Cooperative Cyber Defence Center of Excellence, CCDCOE)總部設置於愛沙尼亞首都塔林，是一個執行網路防禦議題研究之組織，用以支援北約及其成員國的智庫，該組織由跨國與跨產業專家所組成，提供北約組織成員國網路防禦技術、策略、運作及法律方面之諮詢建議。

CCDCOE 會員多達 31 國，除定期推動教育訓練、研究計畫、編撰塔林手冊(Tallinn Manual)及會員國間資安治理框架外，並舉辦知名國際性活動，如網路衝突安全會議(International Conference on Cyber Conflict, 簡稱 CyCon)、紅軍十字軍演練(Crossed Swords)及鎖盾演練(Locked Shields)，本次 CyCon 為第 15 屆，該研討會邀集各國軍方、政府機關及技術單位代表共同參與，研討在網路世界的衝突問題及因應策略。

經過 CCDCOE 的多年經營，CyCon 在全球積累了相當高的知名度及專業性，每年會吸引超過 50 個國家或地區，超過 600 名決策者、意見領袖、法律和技術專家齊聚一堂，以跨學科領域來應對當前網路安全挑戰。每年主辦單位在前一年度 10 月公開徵集研究論文，再由資安學者團進行稿件審查，由主辦單位從中依主題區分為決策、法律及技術面向，並邀請作者擔任 CyCon 講者進行分享。

貳、會議經過

一、**會議日期：**2023 年 5 月 30 日至 6 月 2 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，超過 600 名決策者、意見領袖、法律和技術專家。

四、**參與場次表：**

日期	參加場次
5 月 30 日	Building Partner Capabilities for Cyber Operations.
	Lessons from Cyber Capacity Building: How to Make a Difference in Preventing and Combating Cyberattacks
	Follow the White Rabbit ... If You Can
5 月 31 日	Side meeting
	Train As You Fight
6 月 1 日	Threat Is in the Air
	Technical Novelties on the Battlefield
6 月 2 日	Tech Finale – The Evolution of OT Targeting Malware: From CrashOverride to Pipedream
	Tech Finale – Asset and Configuration Management to Support Cyber Security Strategic Goals

五、會議重點摘要

(一) Building Partner Capabilities for Cyber Operations

1.講者：Mark Montgomery

2.重點摘要：

美國網路空間日光浴室委員會(The Cyberspace Solarium Commission, CSC)成立於 2019 年，該組織倡議「保護美國網絡空間不受具有重大衝擊的網路攻擊」，該委員會提供美國政府在網路空間議題下政策建議，該委員會講者 Mark Montgomery 在會中分享美方如何建構夥伴能力，

透過多項計畫支持，如軍方對軍方的支援計畫、外國軍事資助計畫、網路指揮部與網路演練計畫及雙邊資安合作協議等方式，美方首先辨識資安關鍵元素、對關鍵資源進行排序，再投入對應支援，並建議夥伴將建構能力納入政府政策，並呼籲應對關鍵基礎建設清單進行優先排序，盤點各主管機關是否有支持的計劃及資源，美方鼓勵積極推動雙邊及多邊演練，提供聯盟夥伴訓練計畫及資源，協助建構網路攻擊能力等項，會議中並多次以美國與臺灣合作為例，展現協助建構夥伴能力之決心及行動。

圖 1 講者 Mark Montgomery

圖 2 會議過程

(二) Lessons from Cyber Capacity Building: How to Make a Difference in Preventing and Combating Cyberattacks

1.講者：Eduardo Izycki, Jorge Mora-Flores, César Moliné Rodríguez, Tomáš Minárik, Ian T. Brown

2.重點摘要：

該場次係邀集多位講者共同分享，包含巴西、美國及捷克等政府代表，會中有羅馬尼亞資安領域專家共同分享，現有威脅越來越有組織、更有國家隊出現，因此資安事件影響層面也越來越廣，政府在面對重大資安事件時，例如當勒索軟體衝擊到機關服務或設施時，常是跨領域且不易修復的，僅靠一己之力進行防禦或復原實屬不易，並以自身經驗分享，政府需要花費很多時間才能復原系統之可用性，甚至部分系統將無法完全復原，惟有

建立防禦聯盟，使聯盟間提供資安事件技術支援、情資分享，才能對相關事件有所因應。以美國為例，雖美方具有領先發展中國家之資安能力，但透過協助查調資安威脅的過程，可蒐集駭客組織或惡意程式之特徵，美方以此特徵用在傷害發生前，在駭客潛伏期間辨別出國內受害清單並做出因應措施。爰面對此類具規模、重大衝擊之網路攻擊，惟有依靠防禦方的聯合協作，集結國際間公部門、私部門的力量，才能在遭遇攻擊的當下儘速應變及復原，降低衝擊損害的影響程度。

圖 3 講者群

圖 4 會議過程

(三) Follow the White Rabbit ... If You Can

1.講者：Andrea Pompili

2.重點摘要：

講者 Andrea Pompili 提出以 AI 支援安全資訊與事件管理(Security Information and Event Management, SIEM)，透過 AI 可協助用戶在眾多原始資料，客製化組織威脅類別，即時幫助組織辨識、分析網路威脅。但樣本與訓練結果高度相關，講者建議要累積一定量之資料(至少 3 年以上)，累積資料轉為資料湖(data lake)，透過機器學習演算法，建立適合組織的威脅辨識假設，依不同組織間的響應計畫(Play Book)，透過資料迭代訓練，組織可透過訓練結果，擇選合適的模式，雖 AI 可以協助快速且客製化提供

網路威脅辨識、分析及響應之建議，但訓練結果仍須經由機關確認是否適用，因此具有經驗的審查是 AI 支援 SIEM 相當重要的一環，當訓練完成後，SIEM 即可提供縱深防禦之建議及分析，並可透過圖形化儀表板設計，讓相關人員更易理解當下情形。

圖 5 講者 Andrea Pompili

圖 6 會議過程

(四) 外訪塔林理工大學教授(Side Meeting)

1.講者：Birgy Lorenz 教授

2.重點摘要：

考量愛沙尼亞為高度數位化國家，建立世界銀行稱為全球最成功的數位身分證系統，並在聯合國評比為最高的公民數位參與率，包括報稅、投票與新生兒出生登記等事務皆採線上辦理，人民能享受安全、便利的網路服務，惟愛沙尼亞獨立建國後頻受鄰國俄羅斯網攻擊，並在科技方面除採積極主動創新並重視資訊安全。愛沙尼亞數位化程度高於其他國家，為進一步了解該國線上教學與資安教育，安排洽訪 Birgy Lorenz 教授，Birgy Lorenz 擔任國民中小學及塔林理工大學教師，開發多項資安教材被廣泛使用在國小至大學課程，多次獲得歐盟和愛沙尼亞教師獎，該教授也與愛沙尼亞國防部合作推動全民資安提升、辦理資安競賽。

Birgy Lorenz 教授說明愛沙尼亞學生自一年級開始學習資安、國防、游泳、烹飪、針織、(社群) 手機、化學等課程，培養孩子生活、思考及獨

立能力。教學方式係由老師主導，學校並為學生訂定學習地圖，協助學生依興趣擇選課程，課堂並非填鴨式教育，鼓勵學生自行摸索，課程部分情境思考，如假訊息識別，老師將在學習環境中，設計多項假新聞讓學生查驗發掘，課堂的功能是集結學生，讓學生共同討論，也學習團隊合作、分工及決策。當學生有基本知識後（如保護資料之意識、電腦繪圖、手機/電腦基礎操作等），進一步再教導程式編碼、機器人、無人飛機等設備，學生探索自己的興趣及專長後，老師將志同道合學員集結進行實作及討論，透過學生間經驗分享，有助於整體共同提升，也是透過這種方式，各老師帶領一群學生學習，依愛沙尼亞國家規模，可培植國內約 4,000 名同學，老師再建議合適學員參與各類 CTF 資安競賽(約 500 名)，競賽獲獎同學約 50 名，再遴選獲獎學員參與歐盟等級規模之競賽（約 10 名）。

另在全民資安意識提升方面，由國內提案各項推廣全民意識計劃（如 Insafe Program）至歐盟，申請核定後獲得預算，依推廣目標制定內容，例如電視推播、TV Show、小手冊、校園環境等方式推廣。主題如向老人宣傳防駭觀念、提供幼兒「編碼」教學課程，甚至讓青少年學習駭客技能。又如校園環境，學員習得資安知識後，會將所學帶回傳授家庭成員，教導家人如何提升密碼難度與檢查裝置安全性，最終達到全民守護資安的效果。

圖 7 無人機教材

圖 8 學習教材

(五) Train As You Fight

1.講者：Lingming Tu, Network Security Research Lab, Qihoo 360 Technology Co. Ltd.

2.重點摘要：

本項議程集結多位專家學者 YoungJae Maeng, Conner Bender, Martin Strohmeier, Prajwol Kumar Nakarmi 及 Jason Staggs，講者就資安演練主題進行分享，如韓國演練觀察發現、AI 支援演練規劃及巴西演練經驗等。韓國駐 CCDCOE 學者 YoungJae Maeng 分享國內演練之發現，演練目的是模擬組織面臨駭客攻擊時因對作為，演練團隊發現在過程中，藍隊為了獲取對應分數而做出與現實不符的作為，例如規劃組有製造正常使用者流量，藍隊就會透過正常流量的特徵，直接將非正常流量進行阻斷，導致紅隊根本就進不去。或是藍隊動態網頁的服務替換成靜態網頁，導致綠隊在確認時，以為藍隊仍有持續提供服務，但在此操作雖造成紅隊更難進攻，相對不符合現實網路世界。又如綠隊設計紅隊須至藍隊環境取得情資後回傳，但藍隊卻透過防火牆設定，讓紅隊只進不出，造成紅隊即使已攻進藍隊環境並識別出情資，而防火牆設定也無法將情資回報至演練平台，呈現藍隊並無遭入侵之假象，並指出裁判組將針對部分服務檢驗其可用性，部分服務已中斷卻未被查驗之情形。因此講者建議，攻防演練的評分及規則，應將前述藍隊規避行為納入，在有限資源下應仿真實網路環境，設計演練情境及規則，以合適檢驗方式評斷藍隊服務水準。

巴西國防部則是分享演練推動情形，2022 年演練共計 5 天，演練前會以說明會、研討會方式讓參與者知道演練進行方式，再採雙軌方式辦理搶旗技術型演練及兵推情境演練，最後一天再就演練結果進行分析，演練共納入 7 個關鍵基礎設施(交通、水、能源、通訊等)，超過 120 組織(450 名)參與該國之演練，最後講者亦表示歡迎各界參與該項演練，共同提升就資

安事件應變之能力。

圖 9 韓國講者

圖 10 巴西講者簡報過程

(六) Threat Is in the Air

1.講者：Conner Bender, Martin Strohmeier, Prajwol Kumar Nakarmi, Jason Staggs

2.重點摘要：

講者 Conner Bender 及 Martin Strohmeier 分享物聯網相關資安議題，兩位講者以無人機(Unmanned Aerial Vehicle, UAV)為研究對象， 分析 UAV 其飛行檔案，飛行檔案逆向工程後可解譯操作員地理位置，並分享陸資大廠所製造的無人機，以大疆廠牌無人機為例，提供盟友俄羅斯戰時情資，俄羅斯使用專用版本後，可定位出烏克蘭操作 UAV 士兵的位置，並非如大疆所聲稱無人機相關資料都有加密保護，透過研究可藉由中間人攔截，找出遠程 ID，加入已知的基地台參數，即可解譯出操作人員地理位置，兩人即是在此概念下，透過開源工具開發名為 DJI GO 軟體，期透過低成本方式，協助烏克蘭提升戰力，對抗俄羅斯。

另一位瑞士學者 Prajwol Kumar Nakarmi ，研究領域為 5G 資安，首先表明某些 5G 晶片製造商（如華為）是具有資安疑慮的，許多先進國家（英國、美國及加拿大）都已公告禁止使用，考量 5G 廣泛應用在許多重要系統，如導航系統、關鍵基礎設施、緊急系統及物聯網設備，講者表示 5G 確

實也繼承了過去 4G、3G、2G、wifi 等無線網路的不安全性，如未加密等，目前已可直接下載攻擊腳本進行攻擊，因此不是專業技術人員，也可以做到監聽、干擾等駭侵行為，雖然 5G 比過去幾代的通訊協定更安全，具有有加密功能，駭客較難實現監聽及追蹤，但也指出 5G 安全相關研究還不夠多，仍是建議組織應訂定網路邊界並搭配緩解措施，也呼籲 5G 應投入更多研究，才能讓 5G 更為安全。

圖 11 講者群

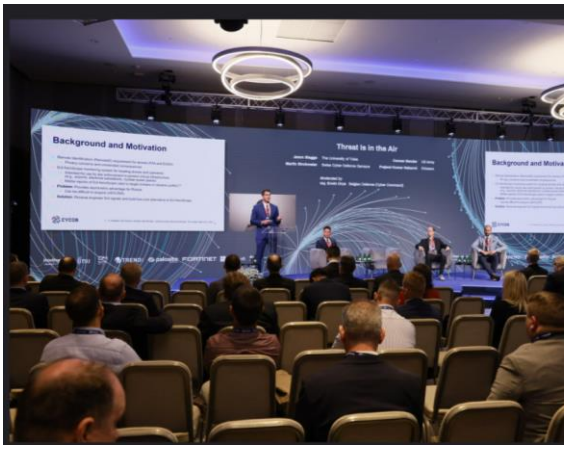

圖 12 會議過程

(七) Technical Novelties on the Battlefield

1.講者：Johannes Klick Mario Beccia Vitalii Zubok Andrii Davydiuk

2.重點摘要：

講者 Johannes Klick 指出烏克蘭網路特性，大型網際網路連線服務公司(Internet Service Provider, ISP)業者服務佔比僅 45%，其餘 55%皆來自小型 ISP 提供者，這與德國截然不同，因此烏克蘭網路並不會因單一線路故障而失效，講者分享該公司藉訪問各地區物聯網設備，作為烏俄戰爭受損偵測雷達，該研究每四小時掃描一次，並以社群媒體探測哪個地區遭受攻擊來輔助分析，來支持說明俄羅斯攻擊頻率有多高，講者展示觀察的網路可用性折線圖，並與現實電力基礎設施比對，指出網路可用性與電力的關鍵基礎設施有高度相關，可藉由此相關性來分析戰爭影響範圍，各

地區網路服務的相依性，如 Sumy 地區停電時網路可用性明顯下降、Chernihiv 地區停電時因部分網路由其他地區提供服務，網路掃描能夠為戰爭提供情報，也能了解烏克蘭之電力恢復情況。

另一位講者 Andrii Davydiuk 即來自烏克蘭，分析烏克蘭因應戰爭其關鍵基礎設施之網路韌性，戰爭期間關鍵基礎設施的確成為俄羅斯的攻擊目標，講者分享電力資安事件統計資訊，並指出電力亦影響其他服務的提供，如通訊、金融等服務，因此烏克蘭接續分析其依賴關係，試著找出單一失效的脆弱點予以保護，來提升電力關鍵基礎設施的可用性，講者也表示，戰爭時資源是有限，烏克蘭必須對高風險、高依賴的設施進行改善，並且提高關鍵基礎設施的機密性，避免讓俄羅斯獲得此類情報。烏克蘭境內國際公司也因為烏俄戰爭的影響，許多國際公司遷出烏克蘭，部分公司則是選擇向俄羅斯屈服，轉而提供俄羅斯情報，當然也有一些公司是協助烏克蘭，如愛立信即是提供烏克蘭所需的支援。

講者以電力工業控制系統 SCADA 為例，烏克蘭找出其邊界範圍，修改作業流程，針對邊界內漏洞加以管理及施作緩解措施，讓關鍵基礎設施更為安全，同時分享因俄羅斯集中攻擊電力設施，恫嚇相關操作員不敢去工作，因此人員也是很重要的資產，缺乏操作員也會造成電力中斷。同時也感謝各國支援，如分析收容資料及數據，預測相關網路威脅及攻擊，讓烏克蘭能夠針對威脅修訂相關法律及作業流程，並再次呼籲各組織應導入零信任，確實清查組織資產，禁止使用具有資安疑慮軟體(如俄羅斯軟體)，烏克蘭除感謝各方支援，其不是第一個被俄羅斯威脅的國家，但烏克蘭想成為第一個分享的人，讓後續遭相似威脅的國家都能夠有所因應。

圖 13 講者群

圖 14 會議過程

(八) Tech Finale -The Evolution of OT Targeting Malware: From CrashOverride to Pipedream

1.講者：Phill Tonkin

2.重點摘要：

講者 Phill Tonkin 服務的公司係專注於工業控制系統惡意組織之研究，鑑於威脅日漸提升，駭客規模也從個別提升為組織性、國家資助及以營利導為向，而工業控制系統過去強調其可用性，造成危害機密性的威脅，反而沒有受到重視，另工業控制系統設備也陸續採用國際標準通用格式，透過中間攔截，網路下載工具解譯封包也已具有可行性，講者分享近一年 APT 組織的行為，如 XENOTIME，該組織針對電網的攻擊，在察覺該領域工業控制系統系統經常未確實作好網路區隔，另一個組織如 CHERNOVITE 擅用新的 TTPS 撰寫腳本攻擊，相關漏洞會針對 WEB 底層及網路橋接處進行危害。

講者進一步分享，勒索軟體已出現 6 年，相關工具不斷地重新打包再利用，觀察到現今的惡意軟件都會置放軌跡清除工具或刪除特定文件功能，避免在後續鑑識上留下跡證，作為延遲關鍵基礎設施中斷的恢復時間，攻擊者會將相關惡意程式包裝為 IT 管理工具，功能越複雜越不容易被察覺，

並發現開始有 APT 組織間相互合作，造成工業控制系統威脅規模及數量都日漸提升。呼籲各國要針對舊有的漏洞進行防範及管理，研究顯示攻擊腳本會不斷更新再重新使使用，透過跨不同領域，直到相關 APT 組織再也無法透過該腳本實現攻擊，該腳本才有可能會停止。

圖 15 講者

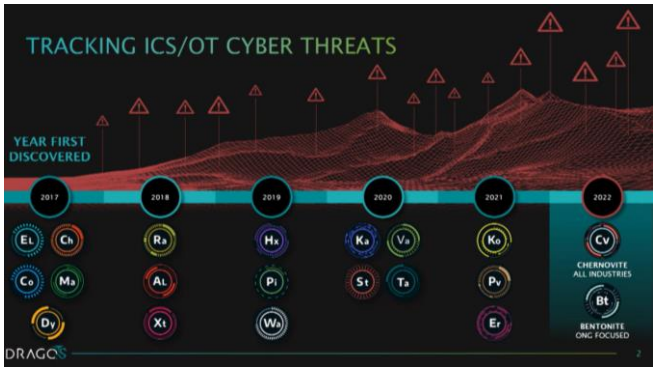

圖 16 OT 威脅概況

(九) Tech Finale -Asset and Configuration Management to Support Cyber Security Strategic Goals

1.講者：Sarah Brown

2.重點摘要：

講者 Sarah Brown 表示 NCI Agency 小組旨在維護北約網路安全，制定北約組織內的網路安全戰略，提供北約成員國家在政治、軍事等面向的協調框架，著重在整體的網路治理，接續關注網路基礎知識及網路議題，推動方式為提倡去中心化，所以成員間能界定出邊界。針對資安長(CISO)及企業挑戰，在於無法掌握實際的資產清單，包含資產識別、關鍵業務，資安不僅是漏洞安全管理，涉及系統架構、工程解決方案、防護基準及合規性，如此一來當漏洞來臨時，能快速發覺並作出因應決策。

當資安漏洞出現後，組織需鑑別資通系統是否會受到該特定漏洞的影響，組織應決定修補弱點的優先性、不處置時造成的衝擊性、整體漏洞的管理、修復或緩解措施、重新配置系統、驗證及追蹤，可回溯到決策歷程，都

需要相當多的基礎知識。

因此講者呼籲針對現在北約的網路安全，基礎知識比一些新興科技(如量子技術、AI 技術)還重要的，基礎知識較能協助組織快速回應，藉由 Asset, Configuration, Patching and Vulnerability (ACPV)框架的推動，實現資訊資產的高度可視性，識別出關鍵資產、資產相依性及資產的漏洞管理，在此框架推動的資產管理除高度可視化，還能達到單一正確來源。

該框架參考 NIST 三層資產管理概念，將資產統一管理，而不是將分散各處資產清單連接在一起。框架內的成員間，支援安全功能訪問、動態查詢、可視化功能，最底層則是地端系統和資產。操作概念是成員間使用相同的方式管理，過去資產盤點並非為安全而盤點，而基於財務考量而盤點，在此前提下，造成各成員依各自需求有不同的盤點方式及資源配置，造成識別總體關鍵資產及整體資產風險，其相關結果的正確性造成落差。

因此，為實現企業間一致性，成員間不需改變現有技術，而是改變流程、架構、採用標準格式，NCI 負責資料格式一致及自動化收容數據，各成員可自定義適當頻率回傳，組織遵循各政策命令及相關安全控制，便可串接不同重要級別、地區的網路，達到前述的成果，以最高可視化、資料正確性及即時漏洞因應措施。

圖 17 講者

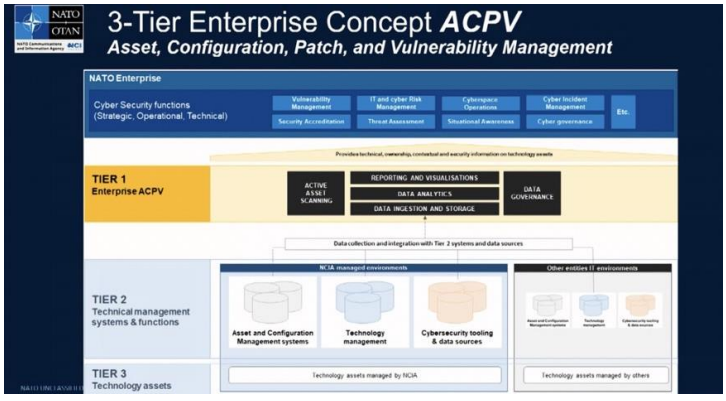

圖 18 會議過程

參、心得與建議事項

本屆 CyCon 會議主題為「Meeting Reality」，各成員針對全球議題(如關鍵基礎設施安全、物聯網、5G、AI 等)進行討論，並以烏俄戰爭為例，和平時期仍可能面臨的危機衝突，如地緣政治衝突，也帶來各成員間結盟聯防之議題，在法律遵循下(國際中立法適用範圍)協助烏克蘭聯防。而北約各成員數位化發展不一，因規模相異的網路環境，如何盤點一致及資訊整合，亦是後續北約將努力方向之一，觀察重點及建議如下：

1．技術面：資安演練、新興科技資安(人工智慧、物聯網、5G)、關鍵基處設施威脅

資安演練仍係各國應定期辦理的項目，藉由演練以檢視整體資安防護及資安意識，並檢驗組織在面臨資安事件時之網路韌性，過往面臨僅單一駭客或組織，影響為單一資訊系統，惟威脅趨向組織化、營利化及跨領域合作，提升駭客規模及資安事件影響範圍，也擴及關鍵基礎設施，爰演練重點除資訊系統外，建議應納入跨領域或關鍵基礎設施，演練對象亦應將相關利害者(聯盟成員)納入，透過執行成果精進後續資安防護。

另針對針對新興技術如物聯網，物聯網開發目的係協助民眾便利生活，為智慧居家、智慧製造、智慧城市帶來了各種便利，但卻也因為裝置採用標準協定不一，各裝置採用特定零件，因此設備僅具備有限運算能力，無法內建嚴格的安全機制和資料防護，爰造成物聯網漏洞不易通盤檢討，呼應到講者所指，戰爭採用 UAV 亦是相同道理，即便廠商聲稱有加密機制，但廠商自身亦有可能將客戶資訊提供予第三者(如俄羅斯)，因此組織在使用物聯網前，應針對其安全性進行評估，物聯網細部從晶片、硬體設計、韌體、軟體開發、通訊等，只要有一個環節出現漏洞，就可能造成組織環境被入侵，爰可建議物聯網主管機關可適當規劃

漏洞修補計畫或納入資安演練，藉由演練適時納入物聯網設備，除可協助應用產品開發者發掘未發現的漏洞，或是開發出新的攻擊手法。

而關鍵基礎設施安全，目前主要威脅仍為勒索軟體，現在駭客組織間已趨向專業化及企業化，針對特定領域駭客組織願意投入更多時間及人力，且不同領域駭客組織也會進行合作，以獲得更大報酬，相關惡意腳本在消失前會不斷被重複更新再利用，直至漏洞無法再利用，爰中央事業目的主管機關訂定防護基準後，由納管對象落實，如漏洞管理、網路區隔、定義邊界，後續由中央事業目的主管機關透過稽核或演練方式，檢視關鍵基礎設施防護基準等合規性。

2. 政策面：非政府部門參與、供應鏈安全、國際結盟

因應烏俄戰爭及疫情影響，各成員國也意識到供應鏈安全的重要性，本次會議美國白宮即指出，美國政府在 2021 年進行一年的供應鏈檢討評估後，為加強供應鏈之韌性，新的網路戰略，將風險責任分配到最有能力承擔的人(如供應商)，明定對供應商要求事項。後續將與私部門緊密合作並朝向立法方式賦予供應商如未採取合理預防措施保護產品及服務應承擔之責任。並針對關鍵基礎設施，如面臨重大資安事件或網路攻擊時，國家如何支持，及規範防護基準及法規保護關鍵基礎設施，並將勒索軟體自犯罪行為提升至國家安全問題。亦將持續深耕國際戰略夥伴之關係，與理念相近之國家合作以應對相似的威脅，為科技及資訊創建安全的供應鏈，如美國 FBI 和 CISA 以及英國私部門合作，記錄了俄羅斯政府支持的對 Cisco Systems Inc. 路由器的攻擊手法。而 NIST 負責制定各種網路安全標準，也將進行重大改革，如物聯網安全性、保護隱私、加強身份管理和提高軟體供應鏈安全性。

3．法規面：網路戰爭中立法、塔林手冊

CCDCOE 國際專家小組著手於塔林手冊(Tallinn Manual)改版，其中第七章規定了基於武裝衝突法的網路戰爭中立法，本次會議美國學者以烏克蘭戰爭為例，以網路中立性進行解析，在烏俄戰爭中，美國及歐盟在網路聯防已直接參戰，但仍維持中立觀點(直接參與如何符合中立和共同交戰的國際法律規則)。瑞士學者也指出提供數據資料與提供武器一樣，中立國如何在合規下與合作伙伴分享數據。丹麥學者另指出，單一駭客參與烏俄網路戰爭，管轄國家應在法律上義務進行審查。英國學者探討了私部門(資訊服務提供商)，在武裝衝突中的法律影響，表示私部門參戰性質類似個人直接參與軍事行動，可能使科技公司的人員和資產面臨損害風險，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。

4．深化國際合作

CyCon 會議參與採申請制，經主辦方審核後參與者應與北約相同理念者，出席人員多屬軍事機關、政府單位、國家學術機構，聯防概念也會更為強烈，並隨著烏俄戰爭興起，國際上開始出現指責專權主義國家網路攻擊(中國、俄羅斯等)的聲浪，在此國際情勢下，我方亦可就地緣政治或對外來網路攻擊之研究發現參與並推動跨國資安聯防。

本屆採實體參與，本次本署出席人員與國內相關組織，得於會議期間與主辦方進行空檔的雙邊合作交流，雙方並藉此討論未來合作領域及可行性並有利於後續進行的深度交流，我方亦介紹我國的跨國攻防演練(CODE)，將於本年十月於臺北舉辦，期間將並行舉辦政策會議，我方誠摯邀請各夥伴派員參加，或可邀請參加主題演說發表，各友方表會將進行評估、考慮指派適當人員出席等。

會議期間，本署亦尋適當時機參與演練相關議程，並與講者建立聯

繫，邀請參與我國跨國攻防演練，則與友好國家等加強聯繫，以推廣我國辦理之攻防演練，邀請對方實地參與我國演練，俾推動後續資安合作(如攻防演練、人才培育及政策交流)。