出國報告（出國類別：開會）

參加2024年第16屆 MERIDIAN 關鍵基礎設施防護會議 出國報告書

服務機關：數位發展部資通安全署
姓名職稱：林春吟副署長
陳彩玲科長
派赴國家：印度
出國期間：113年7月2日至113年7月7日
報告日期：113年9月

摘 要

Meridian 2024年會於本(2024)年7月3至6日在印度新德里舉辦，並由印度國家關鍵資訊基礎設施保護中心（National Critical Information Infrastructure Protection Centre, NCIIPC）負責籌辦，由Meridian各會員國負責關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)之政府高階主管及專業人員參加。

Meridian 會議係由英國於2005年發起倡議後，原則每年辦理，惟2019年瑞士辦理第15屆會議後即因疫情停辦，直至本年印度重啟本項會議，本次年會的主題訂為「合作是CII保護的關鍵(Collaboration is Key to CII Protection)」，重點在於各國CIIP政策之學習交流及經驗分享，並將重點放在強化公私夥伴關係、網路安全社群國際合作、情資分享平台、風險管理、網路安全成熟度評估、供應鏈相互依存性、CII 韌性及新興網路威脅防護等。

我國為Meridian 指導委員會成員國之一，每次年會皆派員參與會議，與各會員國在CIIP 議題交換意見與交流合作，並瞭解各國CIIP 最佳實務經驗及法規制定，供我國關鍵資訊基礎設施防護作業參考，並提高我國國際能見度。

目　錄

圖目錄

表目錄

壹、出國基本資料

一、 活動名稱：2024年關鍵基礎設施防護會議

二、 會議時間：113年7月3日至7月6日

三、 活動地點：印度新德里巴拉特曼達帕姆大廈會議中心（Bharat Mandapam）

四、 參訪人員：數位發展部資通安全署林副署長春吟及陳科長彩玲（以下稱我參訪團隊）

貳、背景與目的

關鍵資訊基礎設施(Critical Information Infrastructure, CII)為支持關鍵基礎設施運作之重要資通系統，隨著資通訊科技發展及工業系統智慧化的發展趨勢下，網路攻擊被利用機率亦隨之提升，全球協作保護和保障 CII 的安全也變得更加重要。

CII 的保護非全球合作無法達成，沒有哪個國家可以獨善其身，也無法僅憑自己保護其 CII。因此，各國必須相互了解不同國家的情況和機制，以便在面對保護 CII 的各種新型態挑戰能共同協調應對。

Meridian 會議係由英國政府於2005年倡議創立，它將來自世界各地的國家政府高階主管與專業人士聚集在一起，每年分別由不同的會員國輪流主辦，希望藉由每年於不同地區舉辦，提升各國對 Meridian 的參與程度，並作為各國關鍵資訊基礎設施防護（Critical Information Infrastructure Protection, CIIP）政策制訂者之經驗分享與交流平臺。

Meridian 會議在2019年瑞士舉行後，因新冠疫情停辦4年，印度受 Meridian 委員會委託，於本年重新啟動了 Merdian 2024，故本年的 Meridian 會議具有復興與延續的意義，在面對 CII 保護的廣泛挑戰中，重申全球合作的重要性。

本次主辦單位為印度國家關鍵資訊基礎設施保護中心（National Critical Information Infrastructure Protection Centre,

NCIIPC)，隸屬於印度國家技術研究組織（NTRO)。該中心是根據《2000年信息技術法》第70A 條（2008年修訂）於2014年1月16日通過憲報公告成立，為印度保護關鍵資訊基礎設施的重要政府機構，負責促進國家關鍵部門的資訊基礎設施安全、可靠和韌性。

第16屆 Meridian 會議的主題是「合作是 CII 保護的關鍵」，包括領域知識分享和全體會議、工作坊及圓桌會議等，希望為所有與會者儘量提供互動交流機會，以分享各與會者在 CIIP 相關主題上的倡議、挑戰和觀點。

參、會議資訊及議程

NCIIPC 於本年7月3日至6日在印度新德里辦理 Meridian 2024，共35個國家、110位代表及約80名印度關鍵資訊基礎設施運營商的代表參與。會議的安排包括1個專題小組討論、2場圓桌會議、4場領域分享會議及9場關鍵資訊基礎設施（CII）保護議題的相關工作坊，如 CII 韌性、ICS/OT 、SCADA 安全，以及人工智能和機器學習在 CII 安全中的應用。議程如附件1(資料來源：會議網站，https://meridian2024.gov.in/)，並要求與會者不得於網路上發布本次會議的照片和影片。

肆、會議重點摘要

在議程正式開始之前1天，安排報到行程及非正式的餐會，讓會議參與人員能提前熟悉會場位置，並進行軟性交流活動，為正式議程暖身。第1天的議程包含：開場及歡迎致詞儀式、破冰會議、小組討論、圓桌會議及工作坊等。

為促進來自全球各國與會者的熟悉，大會設計破冰活動，在會議室設置25張桌子，每張桌子容納8位參與者，事先安排每1個與會者的座位，確保來自同一國家的代表不會坐在同一張桌子上，同一桌的成員於破冰時間裡，互相介紹並討論各自國家的做法及分享見解；這樣的流程共進行2個階段，有助於後續各工作坊的進行及討論。

7月4日小組討論會議，專家小組代表包含來自美國網路安全暨基礎設施安全局(CISA)、英國國家網路安全中心（NCSC）和日本「網路安全戰略本部」下設內閣網路安全中心（NISC）的代表，皆是負責各該國關鍵資訊基礎設施保護的機關。討論會議係以提問有關策略發展、平衡安全與創新、公私合作夥伴關係與激勵措施以及未來展望等議題面向，由與會代表說明該國處理作法，達到互相交流的目的。

針對「如何將供應鏈安全和網路安全韌性納入關鍵基礎設施保護策略，以應對來自第三方供應商或管理服務提供商的潛在漏洞」之提問：

日本代表說明該國自2018年開始，即對政府 IT 系統採購進行監管，要求政府機構在採購關鍵 IT 系統時，尋求 NISC 組織的建議，看看是否存在供應鏈風險。日本在2022年制定的《經濟安全保障推進法》也將對關鍵設施運營進行篩選，以防止這些設施被外部利用。透由政府採購和篩選關鍵設施的規範化，應對來自第三方供應商的潛在弱點威脅。

針對「最有效的公共私營夥伴關係模型是什麼，這些模型如何在開發和實施關鍵信息基礎設施（CII）保護策略中發揮作用」之提問：

代表說明在該國大多數關鍵基礎設施是由私營部門擁有的，而 CISA 在過去六年來，建立很多論壇，私營部門可自主參與，以便在公共和私營部門之間共享資訊，了解威脅、共享漏洞和尋找解決方案。例如：CPAC（關鍵基礎設施保護合作委員會）召集私營部門夥伴參加這樣的論壇，論壇成員組成包含美國的16個關鍵基礎設施領域，允許公共和私營部門之間安全地共享資訊，討論共同的威脅和脆弱性。另美國制定《關鍵基礎設施資訊法案》，允許私營部門夥伴向 CISA 提交有關漏洞的資訊，以便能夠了解基礎設施領域中的共同性與認知差距，俾能建立信任，促進資訊共享。

針對「行業自我監管與政府法規在關鍵基礎設施保護中的作用有

什麼看法？」之提問：

英國代表說明該國查看行業迴避規範時，需要考量該行業的激勵及推動其業務的動力，建議需要一定程度的監管和立法，以平衡私營部門固有的激勵機制，否則私營部門會專注於行業收入和利潤。完全依賴規範無法實現網路安全韌性，為解決基本的激勵模型，英國對策為考慮讓企業董事會和商業組織在網路安全的過失中承擔個人責任。

一、7月4日圓桌會議主題：CII 保護國際合作機制

（一）印度關鍵資訊基礎設施防護重點

隨著數位時代模糊了地理邊界，網路威脅可以來自世界任何地方，而全球各國皆可感受到網路威脅的影響。建立這種國際反應框架至關重要，印度國家安全顧問 Shri Rajinder Khanna 提出了5個合作領域，並且根據優先等級，並將這些領域列出如下：

1. 資訊共享：共享威脅情報、最佳作法及事件報告，允許各國從彼此的經驗中學習，主動應對新興威脅。這可以通過雙邊國際組織、非正式論壇，甚至工業合作夥伴之間的雙邊論壇進行。

2. 制定和採用通用的網路安全標準及最佳作法：確保跨國界的安全基準。此部分涉及安全網路、漏洞揭露實踐和事件回應協定之合作。

3. 建立值得信賴和有彈性的公私合作夥伴關係：這些合作夥伴關係會將專業知識、資源和資訊共享能力結合在一起，以應對網路威脅。

4. 執法合作：網路犯罪通常超越國界，使得國際執法合作至關重要。這亦涉及資訊共享、聯合調查及在中立法律援助程序下加快處理過程。

5. 能力建構和聯合網路安全演習：發展中國家可能缺乏資源和專業知識來有效保護其 CII，聯合網路安全演習的國際合作可能涉及能力建構計劃，以幫助他們改善網路安全態勢。

（二）美國關鍵資訊基礎設施防護重點

CISA 聯合網路防禦協作部門未來計劃主管 Seth McKinnis 分享3個指導戰略及參與的關鍵領域如下說明：

1. 推進與美國國際夥伴的協作：從美國的網路資安事件應變團隊與其他國家網路資安事件應變團隊分享相關情資，以便可以快速共享 TTP（技術、戰術和程序）和 IOC（威脅指標），這些指標提供背景資訊，可瞭解威脅發生根因及如何緩解?

2. 加強戰略協作的能力：CISA 提供一個網頁，收容來自私營部門實體的免費服務和工具，這些工具可供全球的關鍵基礎設施實體使用，以更好地保護其系統。另建立已知遭利用漏洞(Known Exploited Vulnerabilities, KEV) 目錄清單，該目錄基本上優先處理實際已被威脅行為者在外利用的漏洞，並幫助關鍵基礎設施實體優先處理這些漏洞。

3. 針對保護關鍵基礎設施之全球政策演變，CISA 適時提出策略：從 CISA 的角度來看，將保護關鍵基礎設施與共同目標聯繫起來是非常重要的，如何識別那些共享的依賴關係，例如：對多國和跨國界多部門使用的雲服務提供商的攻擊，共同協議和處理協定的漏洞，國際間合作支持 ICS 系統朝向設計安全的產品。CISA 發布網路安全績效目標，這基本上是將 NIST 網路安全框架優化，以便更容易被關鍵基礎設施實體使用。網路安全審查委員會在發生重大事件時會公開發布一個全面的技術審查報告，說明該事件的樣貌及應變方式為何？

（三）西班牙關鍵資訊基礎設施防護重點

西班牙國家關鍵基礎設施保護中心隸屬於內政部，成立於2007年，負責國家基礎設施系統保護，任務是協調並確保系統接收端之資料完整性及安全性，協助關鍵基礎設施適應及應變面臨的新威脅。

西班牙分享與歐盟國際合作方式，主要是與來自不同國家的專家小組協作，這個專家小組為歐盟委員會的關鍵實體韌性小組，於2022年開始運作，近期關注重點為關鍵實體的韌性。2023年西班牙作為歐盟理事會的輪值主席國，協調西班牙在聯盟中對具有重要跨境相關之關鍵基礎設施中斷的應變措施，並確保資安事件的協調和通訊。

西班牙與其他國家間亦有在法令方面的合作，包括與黎巴嫩和烏克蘭的合作。目前係以西班牙的經驗，協助烏克蘭為法律框架做好準備，使其與歐洲相關的基礎設施保護和韌性保持一致。

二、7月5日圓桌會議主題：對關鍵資訊基礎設施保護之產學研合作

（一）干擾關鍵資訊基礎設施運作，比實際物理傷害造成更多的經濟和財務損害。在這種情況下，印度認為需要所有可能的利益相關者來共同解決與網路安全相關的所有問題。且許多關鍵資訊基礎設施本身並不一定是公共或由政府管理，可能是由私營機構(私營公司、私營銀行及金融機構)與大公司(運輸公司或航空公司)所負責，因此它們身為網路安全的基本利益相關者，其參與任何國家具相同的重要地位。

（二）隨著新興技術發展，私營部門、學術領域或新創企業都扮演著重要的角色，特別是網路安全領域的新創企業。因此，無論是私營部門、學術界還是創新者，它們都是這個過程中重要的合作夥伴。印度透過關鍵基礎設施合作夥伴諮詢委員會的多個論壇，把私營部門

合作、學者和群體成員聚集在一起討論問題。在法規上，有關網路漏洞評估能力及物理安全評估能力方面，則透過地方 ISAC（資訊共享與分析中心）緊密地合作，並能真正與執法機構建立合作關係，因為網路演習或實際上的網路攻擊並沒有區分私營或公共部門，促進公私合作，這對推動資安事件應處至關重要。在資安治理方面，例如：私營部門與印度政府機關共同參與許多資安治理的過程，甚至是立法草案，提出相關見解和協調政策回饋，強化公共私營合作夥伴關係。

（三）印度分享由於網路安全問題很多是因終端使用行為造成的，所以群體成員的參與也非常重要。終端使用行為通常涉及人們洩露登入憑證、用戶帳號和密碼，在不知情狀況下與未知人員共享大量資訊等。而與關鍵資訊基礎設施互動的群體成員行為方面的風險，是印度在處理整個資訊安全時需要考慮的問題，這也是印度與群體成員的重要議題，需不斷努力提高資訊安全的意識。

（四）英國分享公私協力合作，首先，引導來自各領域的人能互相交流學習；其次，盡可能提供一個夥伴架構，且必須有團隊參與協助，他們擁有必要的技能和經驗，能夠與各行各業對話，並能夠用他們的語言交流。英國認知到可能能源行業提供的安全建議不夠具體，所以擁有理解金融行業如何運作的人，或者理解交通行業如何運作的人，能夠以一種理解業務流程的方式共同進行交流，這樣更為有效。第三個要點是盡可能地擴大真實資訊的共享，因為逐步邁向高程度的自動化，促進資訊在各行業中移動，可提供最大程度的保護和覆蓋。

三、7月4日參加工作坊(Workshop)重點

本日參與由各國專家所主持的工作坊(Workshop)，對各項 CIIP 安全議題進行較深入的討論，議題包含資訊安全 ICS/OT/SCADA：挑戰和前進的道路(Topic: Cyber Security in ICS/ OT / SCADA: Challenges

and Way ahead)與威脅獵捕與網路威脅情資(Topic: Threat Hunting and Cyber Threat Intelligence)。

（一）資訊安全 ICS/OT/SCADA：挑戰和前進的道路

1. 早期網路攻擊事件和應對挑戰：在 Stuxnet 事件之前，OT 領域已經發生過網路攻擊，但人們通常將其歸因於系統故障，而不是網路攻擊。OT 資安事件應處存在盲點，尤其在判斷事件根因是網路攻擊或系統故障造成。

2. 重大網路攻擊事件：Stuxnet 發生首次有具體證據的網路攻擊事件，打破了實體隔離網路的理論。俄羅斯使用 BlackEnergy 3對烏克蘭電網發動資安攻擊事件，突顯了監視控制與資料採集系統(Supervisory Control And Data Acquisition , SCADA)的脆弱性。

3. 針對 OT 系統的攻擊趨勢： SCADA 系統受到越來越多針對關鍵基礎設施的網路攻擊，包括電網、水處理廠、油氣領域、交通運輸和煉油廠等。駭客具備對 OT 設備、OT 協議和安全儀表系統本身的配置方式之知識，甚至能攻擊用於備用目的的安全儀表系統(Safety Instrumented System，SIS) 。

4. IT 和 OT 安全上的差異：OT 領域的威脅行為者通常是國家級行為者，而非在 IT 領域攻擊之駭客，應考慮到人員、過程、技術的影響，並且視需要增加監管措施，亦須考慮 OT 系統更新和修補漏洞的時間可能是在3-5年後的停機期。OT 資安事件的根因和取證較 IT 更加困難，因為 OT 設備通常缺乏提取日誌的功能。

5. 勒索軟體攻擊：勒索軟體攻擊不僅僅是為了竊取數據或獲取財務報告資訊，亦逐漸針對使用 SCADA 系統的金融技術公司作為攻擊目標。

6. 日本提出 OT 和 IT-OT 的融合增加了整個供應鏈的資訊安全風險

及缺乏針對 OT 和 ICS 資訊安全的完整指南，特別是對於中小企業而言，因其缺乏資源來減輕風險。日本通過合作和政策制定，加強整個供應鏈的資訊安全保護，例如：日本政府制定《物聯網產品安全合格評估方案政策草案》，以確保 OT 和 ICS 的資訊安全，並與國際標準接軌，並透過人力發展資源計畫，擴大資訊安全市場生態系統，包括人才培養和政策推動，擴展資訊安全能力到中小企業，以加強整個供應鏈的保護。

（二）威脅獵捕與網路威脅情資

1. 日本的威脅態勢

日本國家網路安全中心(NISC)擔任國家政策協調員、政府基準設置者和國家級安全緊急應變小組，介紹日本受到的網路攻擊數量正在增加，如圖1所示，來自海外的可疑連線和網路攻擊相關通訊的數量，在過去四年中增加兩到三倍。2022年報告指出國家警察廳的勒索軟體之資安事件數量為230件，相較於2021年的146件大幅增加。這些數字顯示網路攻擊次數增加和威脅手段的多樣化，從 DDoS 攻擊、網站篡改、虛假資訊傳播、劫持物聯網設備和網通設備與金融利益相關動機造成攻擊，如勒索軟體攻擊及針對機密資料竊取和智慧財產權的間諜活動，以及利用 Wi-Fi 惡意軟體進行的破壞性攻擊。

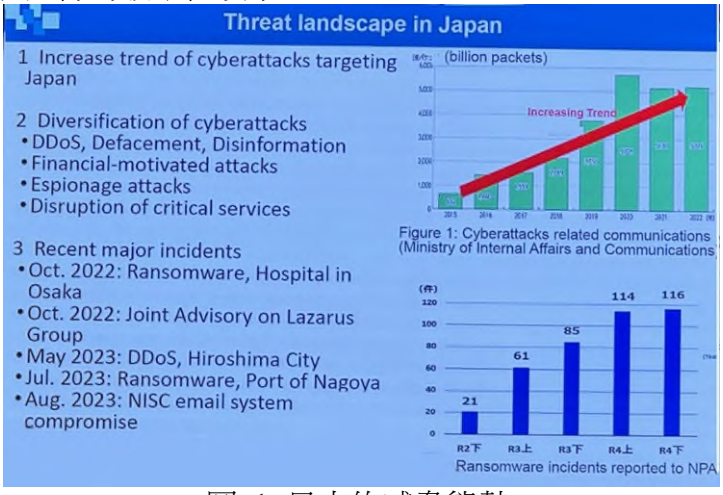

圖 1 日本的威脅態勢

2. 印度的威脅態勢

C3 Hub，這是一家由印度科學與技術部依保護關鍵基礎設施的使命所建立的第8類公司，從事進階持續性威脅(Advanced Persistent Threat, APT)的監控、偵測和分佈工作，以及早期偵測和確定加密勒索軟體。傳統的蜜罐因為2個原因導致無法有效地與這些高級威脅行為者互動，第1個原因是生命週期編排有限，典型的蜜罐無法與威脅行為者在整個生命週期階段（從初步妥協到資料導出階段）進行互動；第2個原因是模仿現實環境的能力不足，這些高級威脅行為者可以輕易偵測到蜜罐設置，並避免在這樣的受控環境中展示入侵的行為。

所以，提出3個關鍵點：

(1) 瞭解攻擊者行為是現代網路戰的關鍵：僅依靠傳統蜜罐系統是遠遠不夠的，需要進一步發展到編排擬真的蜜罐網路，並戰略性地設置陷阱，以創建具有挑戰性的環境來與高級威脅行為者互動，從而監控他們的行為。

(2) 現成二進制文件(binary file)在APT中的重要性日益增加：我們需要認真考慮建構能力來理解這些二進制文件的執行上下文。(二進制文件係指ASCII及擴充ASCII字元中編寫的資料或程式指令的檔案)。

(3) 建立有效的根因機制：這對於理解惡意軟體樣本的能力以及更好地偵測和找出根因至關重要。

3. 瑞士的威脅態勢

討論威脅獵捕和網路威脅情資（CTI）的實際應用及其在不同層面的重要性。威脅情報處理涉及從技術（如IP、攻擊指標）到來自專家和國際同行的報告，這些資訊經過結構化處理，形成威脅情資圖示，用來展示當前的網路安全狀況。

威脅情資的可操作性： 強調如何將威脅情資打包成可操作的資訊，使其在不同層面上有實際用途，並通過與關鍵基礎設施提供商的長期合作，針對不同的威脅和行為者進行分類和分析。

威脅情資在不同層級的應用：包含提供資安長層級之威脅圖示如圖2，可協助他們識別針對性的攻擊行為及其活動範圍。另提供部長層級之圖資，主要是評估整體威脅態勢對國家安全的影響，而非具體的攻擊行為。

瑞士強調威脅情資在不同層級上的應用和重要性，並展示了如何根據具體需求生成有用的威脅情資圖示。

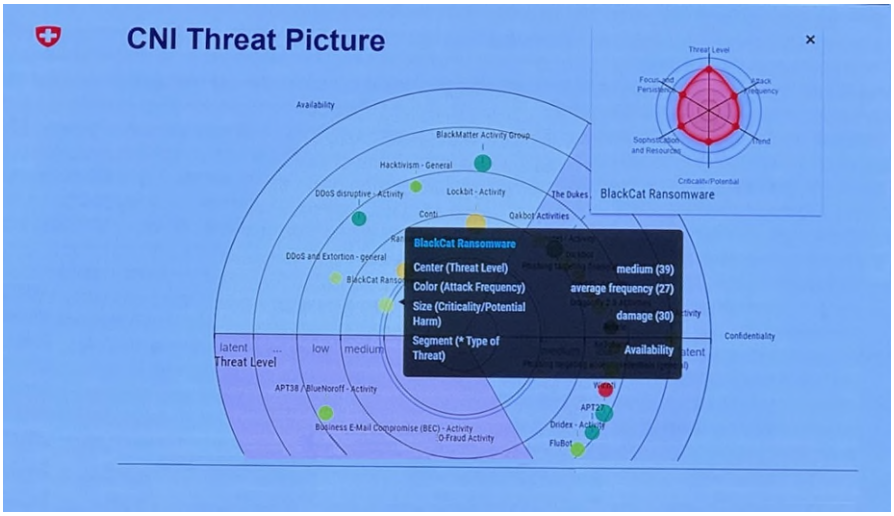

圖 2 威脅圖示

四、7月5日參加工作坊(Workshop)重點

（一）澳大利亞介紹 CIIP 供應鏈安全挑戰

澳大利亞在《關鍵基礎設施安全法》立法框架下，確認11個關鍵基礎設施行業。這些行業中的組織都有對它們至關重要的供應鏈，這些供應商往往也是其他關鍵基礎設施行業的供應商。所以總體風險評估點在於澳大利亞的關鍵基礎設施行業部門和組織是否擁有共享的關鍵供應商，如果這些供應商無法運作，會造成大部分的關鍵基礎設施無法正常運作。

在澳大利亞的立法下，要求關鍵基礎設施須有實體達到全方位風險管理計畫，網路風險也包括實體風險、破壞風險及內部威脅風險等。考量供應鏈風險，澳大利亞要求其部門設立和管理風險計畫，以風險管理計畫來應對這些全方位的風險，識別跨關鍵基礎設施生態系統及跨部門的供應鏈風險，及結合在一起可能存在的漏洞，及如何有效管理這些合約，並考慮風險管理或供應鏈安全。

（二）英國介紹 CII 網路安全成熟度模型

由來自日本、英國及印度的專家小組，講解關於關鍵資訊基礎設施的網路安全成熟度模型。英國牛津大學國際網路安全能力建設研究中心分享國家網路安全能力成熟度模型（Cybersecurity Capability Maturity Model，CMM），這個模型已經有10年，CMM 不僅關注關鍵基礎設施，也涵蓋整個國家網路安全生態系統。探討模型的5個維度，包括網路安全政策和策略、網路安全文化和社會、網路安全知識和能力建設、法律和監管框架、標準和技術，經過全球多方利害相關者的審查和討論，目前使用的是2021年的第三版如圖3，這個模型適用於自我評估。

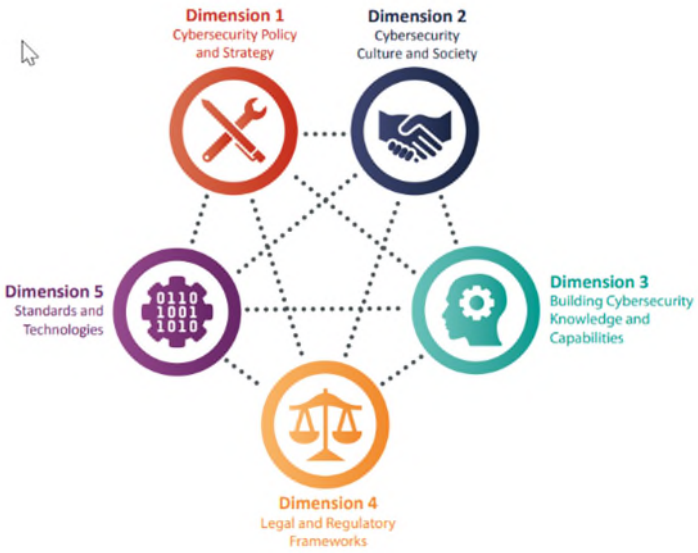

圖 3 CMM(Cybersecurity Capability Maturity Model)

英國的研究團隊每年會進行多次國家評估，這些評估包括與各方利害相關者進行深入討論，以確定國家的成熟度階段並制定改進建議。這個模型幫助了解不同維度之間的關聯，例如網路安全文化的缺乏會影響到基礎設施保護的成熟度。

（三）日本介紹 IoT 網路攻擊

日本介紹 Mirai IoT 攻擊，如圖4及圖5，強調這些攻擊的複雜性和持續性，不僅僅是普通的物聯網感染，在物聯網的環境下，設計利用蜜罐蒐集勒索軟體通知的實例如圖6，還能識別物聯網贖金攻擊，並描述了勒索支付的暗網情況，例如「你的所有資料已被鎖住。」支付指令被引導到黑暗網路上的支付指令網站。

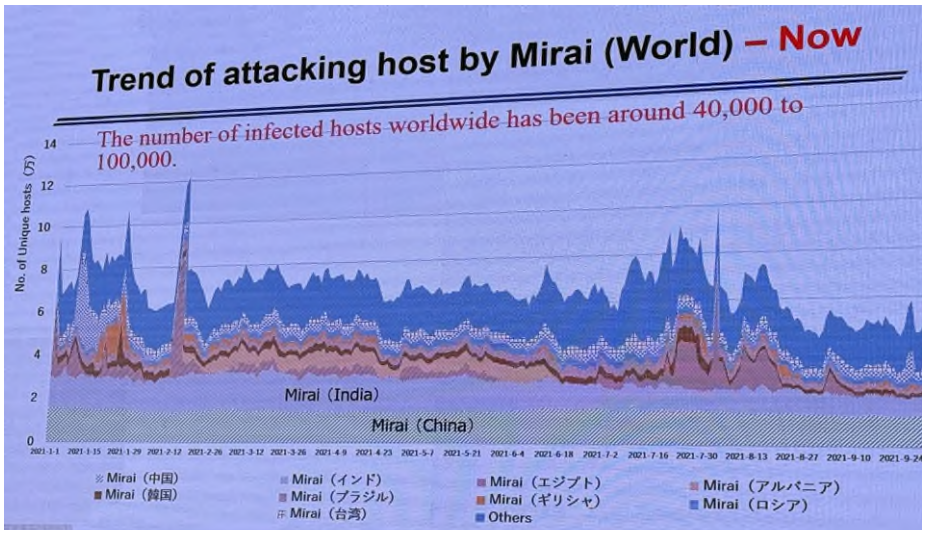

圖 4 Mirai 攻擊各國主機趨勢

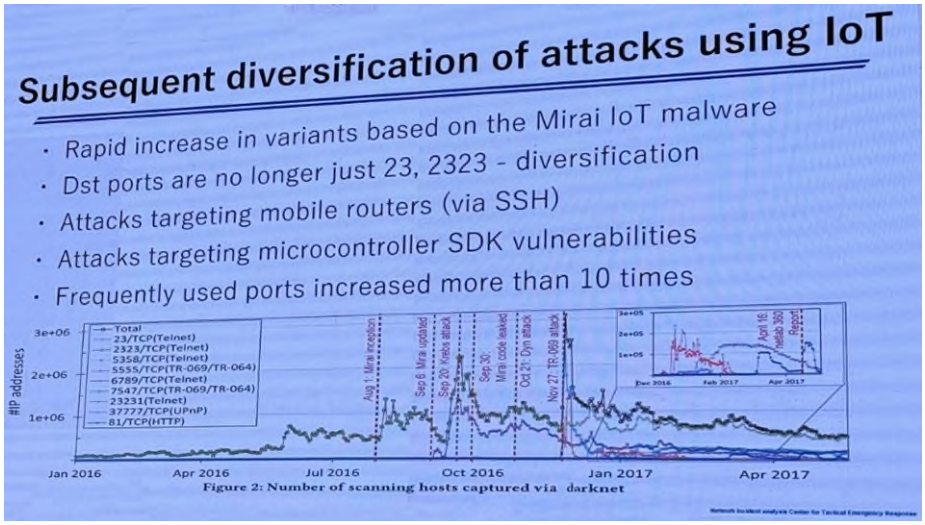

圖 5 使用物聯網的後續攻擊多樣化

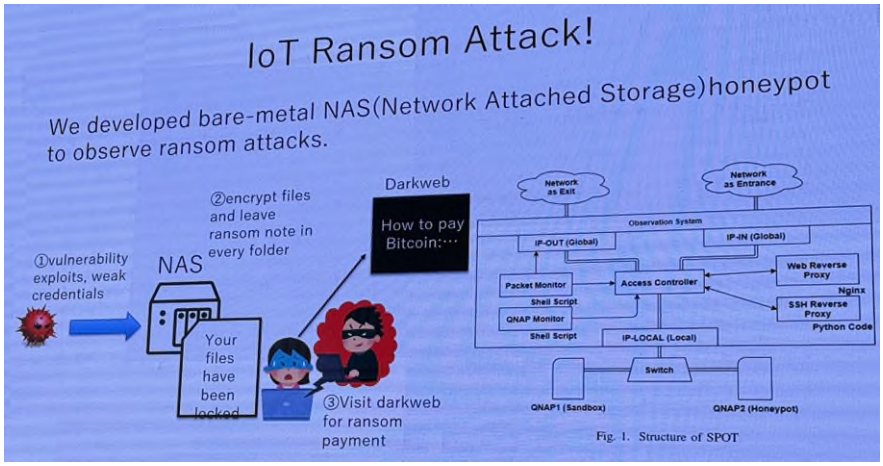

圖 6 IoT 勒索攻擊

在遭遇被利用的威脅階段，ISAC（資訊共享與分析中心）運作是關鍵，根據不同領域有不同的 ISAC，各自識別易受攻擊的物聯網設備。嘗試掃描物聯網設備，識別具體的設備資訊，並發送 ID 和密碼，這些情資已經在電信 ISAC 上分享，並與 ISP 共享，以通知終端用戶。ICT NICTAR 還提供了針對物聯網設備的蜜罐，結合了主動和被動對策的統計數據，但已經觀察到和識別了受感染的物聯網設備。這是 ICT ISAC 推動的另一項嘗試，旨在找出關鍵的物聯網設備，這與關鍵資訊基礎設施（CII）相關。為了識別這些與關鍵 CII 連接的網站，我們通知這些組織修改預設帳號和密碼，並進行教育或提高安全意識，以改善 CII 方面的安全性。

國際合作有很多需要考慮的方面，基於信任關係、資訊共享、及技術開發研究等。因此，持續關注重點威脅趨勢或監控分析、ISAC 合作或標準遵循，以及與專家和學術界的合作，以獲取更具體的資訊。

（四）澳洲分享增強關鍵資訊基礎設施的防禦能力

澳洲分享韌性議題為如何抵禦網路攻擊的能力，討論如何在遭受網路攻擊後能迅速恢復韌性。組織在遭受重大資安事件或其他對資產的攻擊後，在恢復過程中往往會面臨重重困難，這種恢復期的功能缺失不僅對組織本身有害，對澳洲經濟和安全也會產生很大的影響。10年前，澳洲有24個關鍵基礎設施供應商，分布在6個部門，每個部門有數個供應商，但現在有約450個供應商。ISAC 的概念起源於美國，是部門內的資訊共享和分析中心，旨在促進相同部門成員之間的資訊共享。所以澳洲採用 ISAC 模式，並將其與部門 CERT 的功能融合，創建了網路安全合作中心（CSCs），這些合作中心主要有戰略、操作性網路安全和部門服務等3個功能。

五、Meridian 2024會議之結束會議

Meridian 2024會議由印度主辦，在最後結束會議已整理3天活動照片製成短片，並於結束會議時播放，進行本次會議的整體回顧。

第16屆 Meridian 2024會議第1次圓桌會議主題為「CII 保護國際合作機制」，交流了 CII 保護中的當前策略和未來目標。印度政府強調增加國際合作，採取多方面的方法保護 CII，包括但不限於促進資訊共享平台、制定國際標準和加強集體網路防禦。會議的第2天的研討會包括大規模保護交通行業 CII、醫療行業的勒索病毒和個人資料保護，以及 CIIP 供應鏈安全挑戰等主題，由各國代表提供見解並促進各種網路安全問題的討論。圓桌會議有9位主持人分享了他們國家的關鍵機構和計畫，包括來自澳大利亞、美國、阿聯酋、瑞士、瑞典、孟加拉國、柬埔寨、英國和埃及的各國代表，分享確保公私合作夥伴關係保護 CII 的作法。

在本次會議中，討論 CII 機構面臨的一些共同關注領域，如新興威脅、提升 CII 的韌性、威脅狩獵和網路威脅情報。另一個共同挑戰

是如何評估 CII 運營者面對新興網路威脅的視界及準備程度，或者評估 CII 在一段時間內的改善程度，以及如何評估各個 CII 面對網路攻擊的相對準備程度，並相應地提出改進建議，發展符合特定國家或行業背景的網路安全成熟度模型，是解答這些問題的關鍵。

供應鏈的互連性意味著其中一部分的漏洞可能會危害整個系統。組織必須與供應商、製造商和終端用戶合作，以建立更安全的供應鏈。通過採取主動協作的方式，可以確保所有利益相關者在安全工作理念保持一致，保護關鍵供應鏈之完整性和可靠性；但由於供應鏈超越國界，國際政策需要以協作的方式制定，以解決安全方面的問題。

印度表示從討論中了解須為 IT 和 IoT 技術制定網路安全基準，加強對電信基礎設施的立法和監管。因此，重點是與監管機構緊密合作，將網路安全指導方針嵌入現有的監管過程，而不是制定獨立的、特定行業的指導方針；另應考慮到量子技術對數位交易和資料交換安全的影響，及利用人工智慧和機器學習技術來識別、定位、探測和應對威脅。其中最重要的第一步是建立一個共同平台，每個成員國可以通過分享他們在 CIIP 過程中的重要經驗及見解，共同提升資通安全。這個平台不僅能提供一個動態和協作的環境，還能作為我們對本次會議主題的承諾，即合作是 CII 保護的關鍵。

伍、心得與建議事項

本次我參訪團對參加2024年 Meridian 會議，與會者除 Meridian 各會員國主責關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)之官方機關代表外，也有各國政府機關代表及 CERT 組織專業人員，會議主要目的期望藉由聚焦議題的討論與互動，產出可供會員參考的資料。所以大會設計破冰會議，旨在鼓勵參與者分享見解、討論創新解決方案，並交流關於會議主題「合作是保護關鍵信息基礎設施的關鍵」的看法。以下摘要參加此次會議有幾項觀察重點值得我國思考及學習之作法，簡述如下：

一、關鍵資訊基礎設施（CII）韌性

本次會議印度、西班牙及澳洲等多國代表強調公私合作夥伴關係對增強網路安全韌性至關重要，並透過情資分享增強 CII 韌性方面的擴展性和行業專業知識，英國透過 CPAC（關鍵基礎設施保護合作委員會）召集私營部門夥伴參加論壇，允許公共和私營部門之間安全地共享資訊，討論共同的威脅和脆弱性，如同我國「國家資安資訊分享與分析中心」(National Information Sharing and Analysis Center, N-ISAC)每年舉辦年會，邀請相關會員分享資安威脅分析與情勢及實務案例，交流分享各領域間掌握情資，促進產業與政府的資安合作夥伴關係，進而提高國家整體資安防護能量。

二、關鍵資訊基礎設施保護（CIIP）之供應鏈安全

供應鏈的互連性意味著其中一部分的漏洞可能會危害整個系統，由於供應鏈延伸至國界之外，所以影響是全球性的，國際政策需要以協作方式制定。網路風險管理政策應納入供應鏈風險，並從國際供應鏈風險管理的角度考量，透由共同合作以緩解因為供應鏈威脅的連鎖反應。我國資通安全管理法已納入對供應商的資安管理要求，為協助機關落實並妥適辦理資訊服務相關採購，行政院公共工程委員會與數位發展部、資訊服務、資通安全產業界及相關公協會合作研訂「各類資訊(服務)採購之共通性資通安全基本要求參考一覽表」及「資訊服務採購作業指引」，引導機關將資安事項納入契約辦理。

政府採購契約已將供應鏈安全納入關鍵基礎設施保護策略，包含關鍵基礎設施提供者須符合國家關鍵基礎設施安全防護指導綱要、關鍵資訊基礎設施資安防護建議，以及機關提供 IEC 62443規範要求，廠商須符合 IEC 62443等國際標準規範，以因應來自第三方供應商的潛在漏洞。

三、網路安全成熟度評估

英國關鍵資訊基礎設施（CII）網路安全成熟度模型的維度包括：網路安全政策與策略、網路安全文化與社會、建立網路安全知識與能力、法律與監管框架、標準與技術。對網路風險進行評估，採用綜合且校準的方式來識別和評估對關鍵資訊基礎設施的風險。我國工控領域(OT)資安治理成熟度評估作業，係依據第六期國家資通安全發展方

案推動，評估內容以政府資安治理成熟度評估為基礎，並參考「關鍵資訊基礎設施資安防護建議」與美國能源部(DOE)與國土安全部(DHS)合作發展之C2M2(Cybersecurity Capability Maturity Model)制定，每年由本署辦理成熟度評估說明，續由CI提供者依自身防護情形完成評估作業，並推動113年成熟度目標達成第3級以上。

本署將參考上開辦理作法據以精進本部後續關鍵資訊基礎設施資安防護之相關作業建議如下：

一、持續參與Meridian指導委員會及年度會議

我國目前為Meridian指導委員會的成員國，為參與及交流國際針對CI所面臨之資安風險及防護建議措施，應持續參與Meridian指導委員會及年度會議，並強化與各國代表成員的熟悉度及了解，提升成員間的信任度及CI聯防作業。

二、推廣我方資安國際活動

善用此類國際資安活動與各方交流機會，推廣我國資安政策及推動措施，並介紹及邀請參與我國辦理之「前瞻資安探索會議」（Advanced Cybersecurity Exploration Conference, 簡稱ACE政策會議）及每2年舉辦跨國網路攻防演練（Cyber Offensive and Defensive Exercise, CODE），進一步促進國際資安交流。

三、持續精進資安防護作業

會議中各國分享資安威脅趨勢及防護作法之建議，如精進蜜罐的擬真性、加強事件根因的了解掌握及強化供應商資安作為，以更妥適的應對網路攻擊行為及降低資安風險，皆可作為我國後續提升網路威脅偵測及主動式防禦參考。

四、精進資安治理成熟度

我國資安治理成熟度係參考美國相關組織，針對本次會議英國分享之成熟度評估模型及項目，建議可併同我國實務作業需求納入評估構面、評估項目等精進參考。

陸、參考資料

一、附件1:Meridian 2024會議議程(https://meridian2024.gov.in/)

表 1 Meridian 2024年會 Primer Day (7月3日)議程

03 July 2024	
Time	**Session**
14:30 – 15:30	Registration & Kit Distribution **Room: MR18**
15:30 – 16:30	Program Committee Meeting **Room: MR19**
19:00 – 22:00	Welcome Reception (Informal) *Venue: Officers Institute, Ayanagar, New Delhi*

表 2 Meridian 2024年會 Day 1(7月4日)議程

04 July 2024			
Time	**Session**		
09:00 – 09:45	Opening (India) Last Meridian Report (Switzerland) **Room: Summit Room**		
09:45 – 10:00	Break		
10:00 – 10:45	Keynote Address (India) **Shri Amit Shah, Hon'ble Union Home Minister & Minister of Cooperation, Government of India** **Room: Audi 1**		
10:45 – 11:15	Break		
11:15 – 11:55	Ice Breaking Session– Engagement Sessions **Room: Leader's Lounge**		
11:55 – 12:00	Break		
12:00 - 13:00	Panel Discussion – I **Topic:** Strategy for CII Protection *Facilitators: USA, UK, Japan* **Room: Summit Room**		
14:00 – 15:00	Workshop– I (A) **Topic:** Cyber Security Challenges in context of 5G and IoT *Facilitators: Sweden, UK, India* **Room: Leader's Lounge**	Workshop– I (B) **Topic:** Cyber Security in ICS/ OT / SCADA: Challenges and Way ahead *Facilitators: India, Japan* **Room: MR18**	Workshop– I (C) **Topic:** Securing BFSI in the age of Quantum Computing *Facilitators: India, Switzerland* **Room: MR19**
15:00 - 15:10	Break		
15:10 - 15:30	Sharing of learnings from the workshops **Room: Summit Room**		
15:30 - 16:30	Round Table I **Topic:** Mechanisms of International collaboration in CII Protection *Facilitators: India, Egypt, USA, Srilanka, Sweden, Spain, Singapore* **Room: Summit Room**		
16:30– 16:45	Break		
16:45 – 17:30	Domain Knowledge Sharing I (A) **Topic:** Role of AI/ML in CII Protection *Facilitators: India, USA* **Room: Leader's Lounge**	Domain Knowledge Sharing I (B) **Topic:** Threat Hunting and Cyber Threat Intelligence *Facilitators: Switzerland, India, Japan* **Room: MR19**	
19:00 – 22:00	Social Dinner *Venue: Ashok Convention Hall, The Ashok, Chanakyapuri, New Delhi*		

表 3 Meridian 2024年會 Day 2 (7月5日)議程

05 July 2024			
Time	**Session**		
09:00 – 10:00	**Workshop – II (A)** **Topic:** Securing Transport Sector Critical Information Infrastructure at Scale *Facilitators: Japan, Singapore* **Room: MR19**	**Workshop – II (B)** **Topic:** Ransomware and Personal Data Protection in Health Sector *Facilitators: Cambodia, India, Spain* **Room: MR18**	**Workshop – II (C)** **Topic:** Challenges in Supply Chain Security for CIIP *Facilitators: Australia, UK, Switzerland* **Room: Leader's Lounge**
10:00 – 10:10	Break		
10:10 – 10:25	Sharing of learnings from the workshops **Room: Summit Room**		
10:25 – 10:50	Break		
10:50 – 11:50	**Round Table II** **Topic:** PPP (Industry, academia, and community) collaboration for CII protection. *Facilitators: USA, Australia, Sweden, Bangladesh, Cambodia, UK, Switzerland, UAE, Egypt* **Room: Summit Room**		
11:50 – 12:00	Break		
12:00 – 13:00	**Domain Knowledge Sharing II (A)** **Topic:** Cyber Security Maturity Models for CII *Facilitators: Japan, India, UK* **Room: Leader's Lounge**	**Domain Knowledge Sharing II (B)** **Topic:** Effectiveness of dedicated Legislation for CIIP *Facilitators: Singapore, Estonia, Switzerland, UAE* **Room: MR19**	
13:00 – 14:00	Break		
14:00 – 14:50	**Workshop– III (A)** **Topic:** Emerging threats to CII *Facilitators: India, USA* **Room: Leader's Lounge**	**Workshop– III (B)** **Topic:** Future of Cybersecurity Workforce: Skilling, Certification and Talent management *Facilitators: Sweden, UK, India* **Room: MR18**	**Workshop– III (C)** **Topic:** Enhancing Resilience of CIIs *Facilitators: Australia, Switzerland* **Room: MR19**
14:50 – 14:55	Break		
14:55 - 15:10	Sharing of learnings from the workshops **Room: Summit Room**		
15:10 – 15:50	Securing the Public Digital Infrastructure (India) **Room: Summit Room**		
15:50 – 16:00	Break		
16:00 - 17:00	Plenary Session (India) **Room: Summit Room**		
19:00 – 22:00	Dinner and Cultural Program *Venue: Manekshaw Centre, Delhi Cantt, New Delhi*		

表 4 Meridian 2024年會 Day 3 (7月6日)議程

06 July 2024	
Time	**Session**
09:00 – 12:30	Field Trip to Red Fort (also known as Lal Qila), Old Delhi
12:30 – 14:00	Lunch at OKO, The Lalit Hotel
14:00 – 15:00	Steering Committee Meeting **Room: MR19**
15:00 – 15:15	Break
15:15 onwards	Departure

二、會議照片

圖 7 會議地點

圖 8 開幕致詞