出國報告（出國類別：開會）

出席泰國曼谷
全球網路安全機會與挑戰研討會
出國報告

服務機關：國家通訊傳播委員會
姓名職稱：王智遠　(北區監理處簡任技正)
張采玉　(綜合規劃處分析師)
許元耀　(基礎設施事務處技正)
高信雄　(電信偵查大隊偵查正)
派赴國家：泰國　（曼谷）
出國期間：107 年 12 月 6 日至 7 日
報告日期：108 年 1 月 15 日

摘 要

本次參加的全球網路安全機會與挑戰研討會(Global Cyber Security Opportunities and Challenges Conference)，為國際電訊傳播學會(ITS)與泰國國家廣播電視通信管理委員會（NBTC）首次合辦以資安為主軸之年會。

著眼於消費者的信任是推展電子商務中最重要的關鍵因素，除了需要有值得信任的軟硬體之外，更需要商業組織內部良好的資訊安全管理。為達成此目標，亦需要外部由政府機關訂定資訊安全與個資保護等相關監理制度，並建立資安聯防體系。

上開議題已成為全世界關注的焦點。本次會議邀集學者、公民團體、技術社群、政府部門等共同討論，藉此交流平臺探討各國發展現況，為進一步跨國合作尋求解決方案與因應策略。

目　錄

壹、目的

本次會議由國際電訊傳播學會（ITS）、泰國國家廣播電視通信管理委員會（NBTC）首次舉辦之年會。我國通訊傳播委員會長年關注網路發展趨勢，電信監理規劃力求與國際接軌，故十分重視與其他通訊傳播國際及區域組織機構交流合作。會議開場暨引言學者 Erik Bohlin 為 ITS 前任主席，與會學者 Hitoshi Mitomo（三友仁志）為現任副主席，兩者與本會劉幼琍前委員皆為 ITS 董事會（Board of Directors）成員，而本會議主辦單位（NBTC）亦長年與本會（NCC）在頻譜與網路治理議題上保持密切雙邊交流。

本次會議之議題涉及資訊安全、個資保護、大型災害之個資與大數據處理、網路犯罪、個資與經濟，故由基礎設施事務處（資通安全）、綜合規劃處（個資安全）、北區監理處（災防與個資）及電信偵查大隊（犯罪偵防）派員與會。透過接觸國外的實際做法及參予國際的研討會，瞭解不同國家、不同背景的參與者所提出的看法，探討新型態的網路威脅與安全架構，確保我們政策方向與國際接軌，並期能蒐集上述相關寶貴資料，作為未來精進本會監理之參考。

貳、過程

時間： 107 年 12 月 6 日 至 7 日

地點： 泰國曼谷

表 1.議程簡表

	第 1 日議題	第 2 日議題
Session 1	網際網路安全現況	歐盟近期網路安全及資料保護政策及措施
Session 2	亞洲主要經濟體的網路安全政策	國家安全和國際關係中的網路安全議題
Session 3	民眾提供個資予災防告警服務之意願研究	人工智慧與 IT 科技之網路安全
Session 4	工業之網路資安	構建泰國的資料保護及網路安全架構

圖 1.本會出席人員與主辦單位（NBTC）合影

圖 2.本會出席人員與開場引言學者 Dr. Erik Bohlin 等合影

參、重點摘要

一、網際網路安全現況

（The Current State of Cyber Security）

主講人：美國北卡羅萊納州立大學教授 -Dr. Nir Kshetri

圖 3.美國北卡羅萊納州立大學教授 -Dr. Nir Kshetri

2017 年全球花費在網路安全的經費達 930 億美元，預計到 2022 年會成長到 1970 億美元。網絡攻擊所造成的各種損失達到 3 兆美元，遠遠超過了自然災害。如果目前這種趨勢持續下去，到 2021 年每年的損失可能高達 6 兆美元。為了因應以上的狀況，講者指出資訊安全保險（Cyber-insurance）或許是有效的解決方案。此資訊安全保險的主要作用是保障企業所蒐集及運用的資料外洩，包含企業疏失或網路入侵等狀況，此保險應可支付第三人的賠償責任。此一保險在歐美等先進國家已經十分普遍，以美國為例：2016 年的年度資訊安全保險金額達 25 億美元，預估到 2020 年會成長到 62 億美元。但顯然此一保險方案在國內並不普遍（依據我國產險公會，我國於民國 76 年時即推出類似資訊不法行為保險，但至今大多乏人問津），但其他先進國家的投保狀況或許是未來值得我國借鏡的解決方案。

另外講者指出區塊鏈（Blockchain Could）的運用或許也是未來網路安全的解決方案之一。區塊鏈技術是一個全新的領域，和傳統資訊安全防護機制相比有著全然不同特性，簡單而言，即將資料、交易紀錄或訊息放到一個由多個節點共同維護的資料鏈（Blockchain）上，每個節點中都擁有相同資料，利用相同的演算法確保資料不被竄改、偽造，進而達成資料

認證的目的。雖然相關運用前景尚未明朗，相關產業也在持續摸索中，但仍值得我國持續關注。

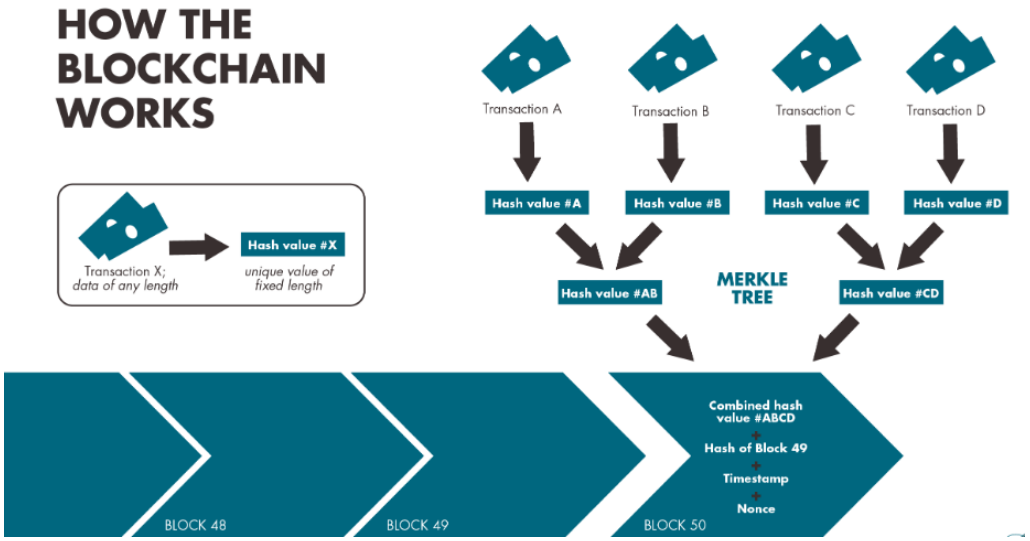

圖 4. 區塊鏈流程示意圖（圖片引自：華盛頓大學網站）

二、亞洲主要經濟體的網路安全政策

（The Cyber Security Policies in Major Asian Economies）

主講人：美國北卡羅萊納州立大學教授 -Dr. Nir Kshetri

圖 5.美國北卡羅萊納州立大學教授 -Dr. Nir Kshetri

本講次強調亞洲各國政府面臨著越來越複雜的網絡安全威脅，這些威脅有可能從經濟中榨取數百萬美元，破壞提供基本服務的關鍵基礎設施，甚至危及生命。政府有效應對這些威脅的能力取決於聰明的政策，強大的機構以及國際社會協力合作。

彙整講者對韓國、中國大陸、日本、印度網路安全政策有幾項共通點；各國政府都非常重視網路安全，將網路安全提升至國家安全等級，訂定專法，設置專責機構，並由最高層級首長直接管轄督導，譬如中國大陸直屬國家主席、日本由官房長官直接督導。網路安全政策大致上也有兩大趨勢，國內部分，立法要求關鍵資訊基礎設施營運者須主動提報及分享網路安全（攻擊）事件。國際間加強建立夥伴關係，共同防禦網路攻擊及犯罪事件，並分享網路安全事件等重要資訊。

講者也特別舉印度為例，印度是最先將網路犯罪定為刑事犯罪的國家，但因網路安全執法人力的短缺，造成 2006 年就成立的網路專責上訴法庭（Cyber Appellate Tribunal-CAT）至 2014 年止卻未判決任何一件案件，另依統計數據顯示網路犯罪的定罪率只有 2%，民眾嚴重懷疑政府的能力、專業性及誠信，造成有高達 70%以上網路犯罪受害者沒向警方報案。為此印度政府特別強調未來除了加強對關鍵基礎設施的保護外，也將在 5 年內培養出 50 萬網路安全專業人才，真正落實網路安全防禦能力。

表 2.各國網路安全政策概況

	中國	日本	歐盟	美國
特點	鼓勵純經濟性使用資通訊科技，保持嚴格網路控制	無專責機構規管	立法施行嚴格隱私權保護	傾向依賴業者自律，但敏感資料仍有特定部門監管
關鍵推動因素	藉政治控制以平衡其經濟現代化，維持統一穩定	針對政府機構與私部門之網路攻擊規模快速增加	二戰法西斯主義者與戰後共產黨員擔心因個資濫用而揭露記載其惡行之密檔	鼓勵行銷與創新
對 IT 業者影響	監管與執法部門、罰則不明，對於雇員自盜或設備故	某種程度依賴私部門自律	歐盟指令較美國嚴格，對各行業影響較廣	美國網路服務提供者被要求向美國政府揭露儲存雲端資

	障造成資料損失無力追查。			料卻未經資料所有者同意或告知，使外國消費者有疑慮
對 IT 用戶影響	外國公司選擇將伺服器放在中國以外鄰國，影響某些服務提供	個資蒐集、處理與傳遞免經個人同意，保護不足。企業於個資用畢亦未強制刪除。	用戶享有較高隱私，但較少雲端服務與品質可供選擇，消費者將較晚接受雲端服務。	政府監視及公司濫用公眾個資議題已吸引關注。

在這次研討會中特別值得留意的是，講者提及南韓如何處理來自北朝鮮的威脅:包括加強阻止來自北朝鮮特定網站和廣播（針對北朝鮮的宣傳戰、心理戰及其他相關的惡意網站）等防禦措施。更重要的主動研發特製的電腦病毒，類似知名病毒「Stuxnet」用以主動攻擊並癱瘓特定國家的核電廠和軍事導彈等重要設施。Stuxnet 又稱「震網」病毒，是第一個以關鍵工業基礎設施為目標的蠕蟲。該病毒的攻擊目標為伊朗使用西門子控制系統的核電基礎設施。據報導，該病毒已感染並破壞了伊朗納坦茲的核設施，並最終使伊朗的布什爾（Bushehr）核電站啟動進程延誤數年之久（Stuxnet 病毒感染流程如下圖）。

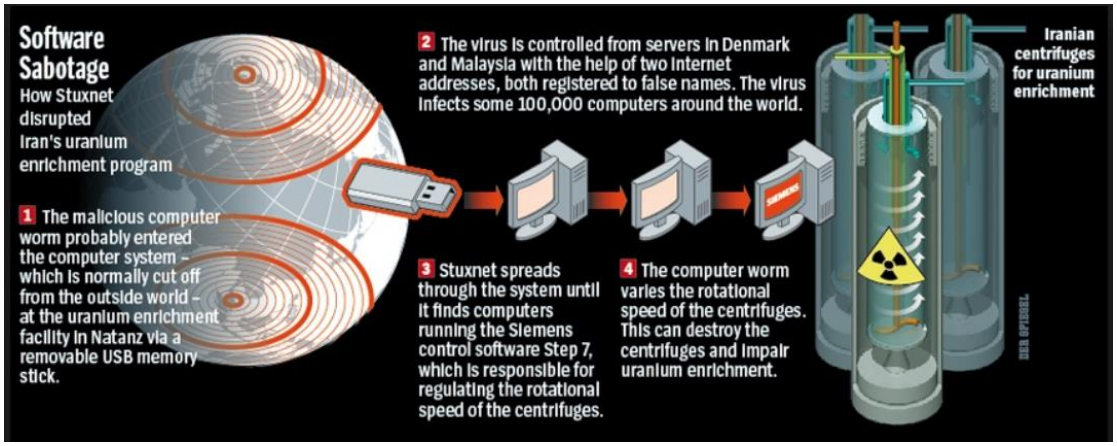

圖 6. Stuxnet 病毒感染流程示意圖（圖片引自：ExtremeTech 網站）

三、民眾提供個資予災防告警服務之意願研究

（Incentive for providing personal information for big-data services in time of large-scale disasters）

演講人：早稻田大學亞洲太平洋研究科教授-Dr. Hitoshi Mitomo

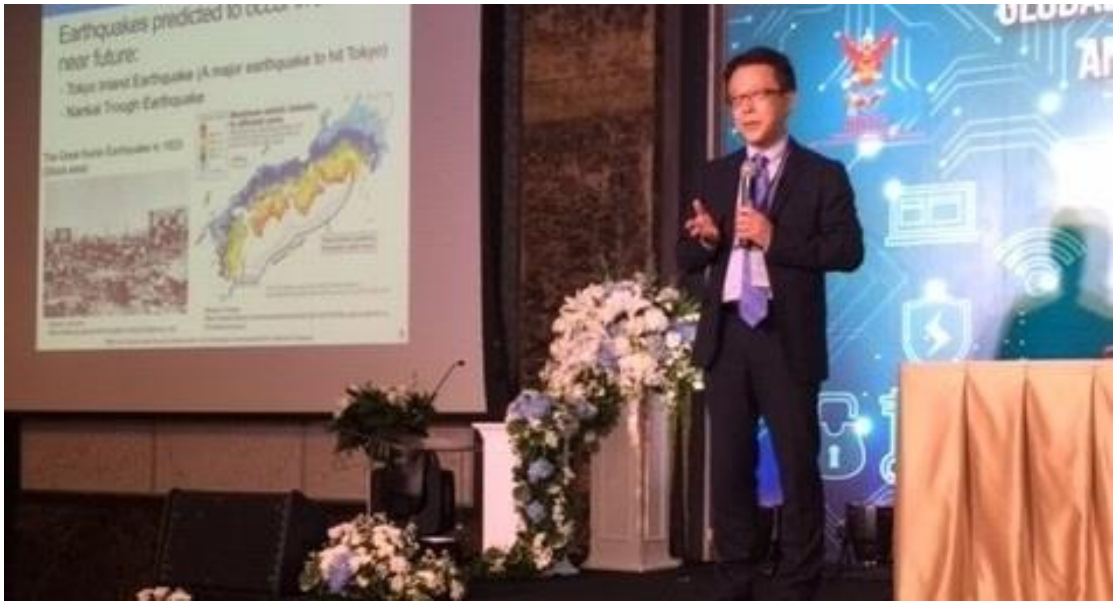

圖 7. 日本早稻田大學亞洲太平洋研究科教授-Dr. Hitoshi Mitomo

本講在現今網路資安威脅下，研究民眾對於發生大規模災難時，提供個人資料給可協助之大數據智慧型服務系統的意願，更進一步分析，民眾願意花費多少錢去買這樣的系統服務?其目的是為了探討私人公司提供及開發大數據智慧型服務系統的可行性。

在亞洲日本、泰國及臺灣等地震發生頻繁，資訊對於生存至關重要。但由於一連串個人資料洩露事件引起了社會的嚴重關注，也影響了民眾提供個資的意願。本次研究採用情境為在日本有大眾示警系統限制下，民眾無法取得更進階的資訊，而此時私人公司智慧型大數據服務可提供較多資訊，使民眾能快速避難或是存活，但加入民眾必須註冊並提供其個資，在考量網路安全下民眾是否有願意使用並且付費購買服務。

講者團隊應用假設市場評價法（Contingent Valuation Method，簡稱 CVM），以問卷調查收集 3,090 位東京網民回應後，得到大約 20%民眾有意願付費 （Willing-To-Pay，簡稱 WTP） 使用服務但可接受付費金額是介於 2,202 至 3,618 日元間 （其中有 27.4%認為有這種服務是好的，19.4%知道在大型災難發生時使用個資是必要的）。

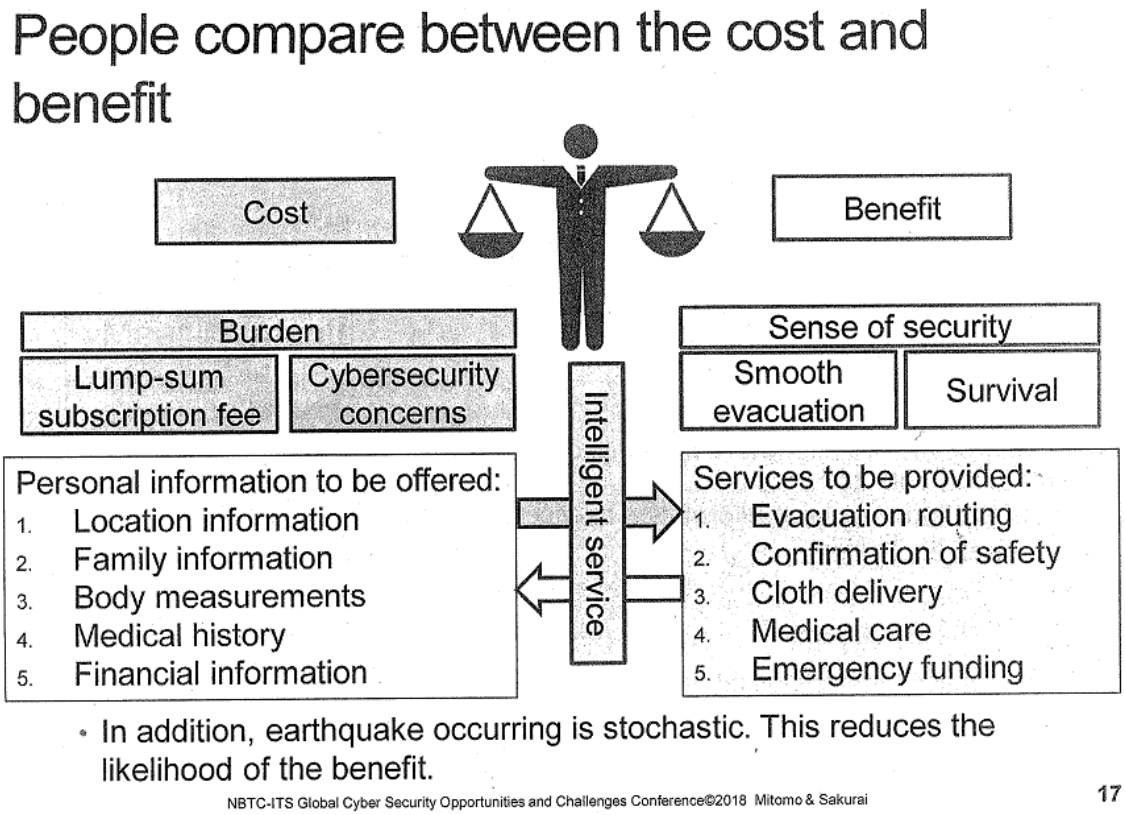

圖 8.消費者災防訊息付費決策考慮因素（圖片引自講者投影片）

表 3.調查問卷母體資料（圖片引自講者投影片）

Date of the Survey	August 5-6, 2016
Target	Internet users in the Tokyo Metropolitan area
Number of respondents	3,090 Male: 1,545(50.0%), Female: 1,545(50.0%)
Age	Between 20 and 69 years, average age: 44.6
Married or not	Married 1,806 (58.4%), Unmarried 1,284(41.6%)
Occupation	Employed 2,041(66.1%), Students 138(4.5%), Unemployed 911 (29.5%)
Members of household	Live with other(s) 2,542 (82.3%), Live with children 1,116 (36.1%)
Medical conditions	I have sickness: 821 (26.6%), Family members have sickness: 1,348 (31.5%)

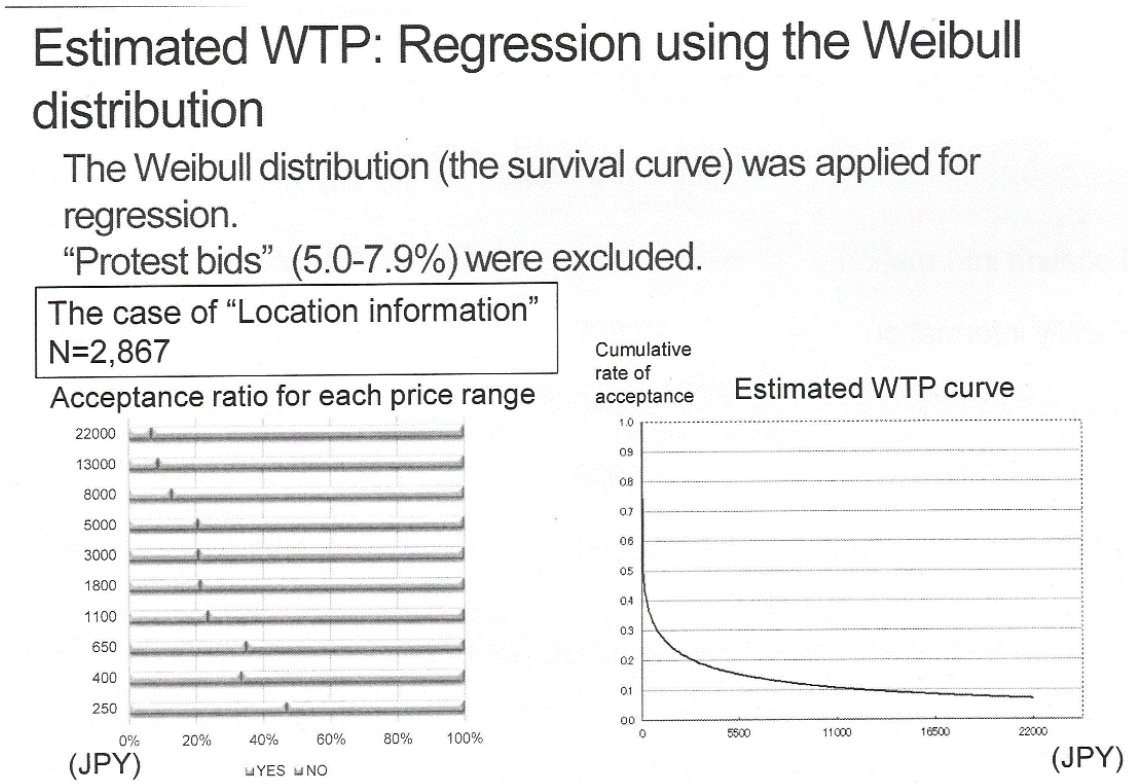

圖 9. 付費意願（WTP）分布（圖片引自講者投影片）

本講結論：依據此調查結果顯示在無法預期大型災難發生及無法確定智慧系統真的可提供最佳及精確的資訊情形下，一般民眾仍無法接受付費提供個資換取有效資訊。

四、工業之網路資安

（Cyber Security for Industry）

演講人：德國卡爾斯魯厄技術學院資深研究員 Dr. Arnd Weber

圖 10. 德國卡爾斯魯厄技術學院資深研究員 Dr. Arnd Weber

講者提出，面對盜取商業機密與入侵基礎設施之威脅，阿忍・韋伯博士將資訊產品製程依控制關係由上而下分成應用軟體、作業系統、硬體、晶片電路製造共 4 層。為防範在軟硬體設計中夾帶木馬程式,他的策略是要求設計本身以及輔助工具軟體皆須透明化。

然而，為達成全面透明化可能無承包商而需自製，成本過高未必是小業者可負擔。因此阿忍・韋伯博士的另一對策是增加電路分割單元或廠牌多元性。其網絡安全戰略已包含整個製造和供應鏈流程以及相關產業的完整配套，全面提升資通安全防護能力。

五、歐盟近期網路安全及資料保護政策及措施

（Recent Policy Initiatives in the EU for Cyber Security and Data Protection）

演講人：英國 SCF 聯營有限公司董事 - Dr. Simon Forge

圖 11. 英國 SCF 聯營有限公司董事 - Dr. Simon Forge

歐盟近期有關網路安全及資料保護政策為資料保護一般規則（General Data Protection Regulation，簡稱 GDPR），及於歐盟內關鍵基礎服務合作協調之網路與資訊系統安全指令（Directive on Security of Network and Information Systems, 簡稱 NIS Directive）。

GDPR 為歐洲議會及歐盟理事會於 2016 年 4 月 27 日通過歐盟規則，將自 2018 年 5 月 25 日開始施行，取代 1995 年制定之「資料保護指令（Data Protection Directive）」，藉以提升及確保對於歐盟境內資料當事人權利保護之一致性（特別是網路活動），並排除個人資料在歐盟境內流通之障礙。相比資料保護指令，GDPR 本身是針對所有歐盟居民設計適用規範，並非屬於在地執行法令，同時也無須由各國政府另外立法授權，而是可直接套用在所有歐盟居民身上，並且伴隨以公司全球市場營收 4%，或是以 2,000 萬歐元 （以金額較高者為基準）作為罰款的嚴格違法處置。

另外要求歐盟居民在任何存取個人用戶隱私運作的服務內容中，必須能獲得最高個人隱私資料控制權，同時也規範嚴謹的個人隱私被忘卻權利，亦即服務內容在取用任何用戶隱私資料時，必需要能讓使用者更容易明白會有什麼樣的影響，同時除非獲得使用者同意，否則不能將用隱私資料永久或長時間存放在網路伺服器，一旦使用者不希望個人隱私留存在網

路服務時，提供服務廠商必須提供全面清除用戶隱私的選項。

GDPR 有以下重點:

1. **以資料為主體：**除了適用在歐盟地區註冊的企業，或者是不是歐盟註冊的企業，但在歐盟營運，或者是有蒐集、處理或利用歐盟民眾個人資料的企業或組織等，都在 GDPR 的規範中。
2. **企業必須設置資料保護長，且需負起法律責任：**只要企業的核心業務涉及對歐盟民眾的個人資料的處理，為了確保企業組織可以有效因應 GDPR 的資料保護規範，歐盟就要求這些企業，都必須要設置一個資料保護長（Data Protection Officer，DPO）的重要角色。這個資料保護長必須要有效依法履行職責，一旦企業有違反 GDPR 的規範，這個資料保護長需要被追究相關的法律責任。
3. **個資的蒐集、處理和利用，必須先徵求當事人的同意：**不僅要求要提供簡明易懂的個資使用同意書，連撤銷個資使用的同意書，也必須一樣簡明易懂且容易撤銷；另也賦予歐洲民眾可以選擇「不共用資料」的權利，也就是說，歐洲民眾可以拒絕企業共同行銷。
4. **強化個人資料可攜權權利：**資料可攜權就是讓歐洲民眾在不同服務業者之間，具有自由搬動個資的權利，例如，歐洲民眾可以從某個 ISP 業者，輕易搬到另外一個 ISP 業者的服務上。不過，更具體細節的作法，仍要回歸到各國因應 GDPR 所做的法規調適的規定中。
5. **新增被遺忘權：**被遺忘權也被稱為「資料抹除」，就是要讓資料的當事人可以要求包括資料控制者以及資料處理者，必須協助抹除當事人個人資料、停止使用當事人個資，這包括供應商和其他的第三方業者在內。抹除資料的前提條件包括：資料利用與處理目的不同、非法處理個資，或者是資料當事人撤銷同意書等，都可以要求刪除。
6. **外洩個資必須在 72 小時內通報資料保護主管機關：**不論是資料控制者或者是資料處理者，一旦爆發個資外洩的資安事件時，必須要在 72 小時內，立即通報給資料保護主管機關（Data Protection Authority）；如果這個外洩資料對於當事人會造成重要危害時，

也應該要及時通知當事人。

7. **個資保護系統預設要納入隱私保護：**不論是 Privacy by Design（隱私保護設計）或者是 Privacy By Default（隱私保護預設），都是近年來歐盟在談論個資或隱私保護的重要觀點，因此在 GDPR 的規範中，也正式納入相關的規範制度，要求企業或組織在建置及設計新資訊系統時，應該要將資料保護設計納入考量。
8. **賦予當事人有權反對被自動化剖析（Profiling）權利**：當事人有權在特定情況下，可以反對資料控制者和資料處理者，對於他們如何處理當事人資料的方式，除非資料控制者或處理者可以證明，原先的資料處理方式有其不得不的正當性，例如有其他法律要求規範等。一旦當事人提出反對權，而資料控制者或處理者無其他正當理由反對時，就必須立即停止處理當事人個資。GDPR 賦予資料當事人有權了解某一項特定服務，是如何利用大數據分析、機器學習、人工智慧等技術，進行資料分析和研判的服務，當然也有權反對被如此剖析。
9. **要求企業必須落實資料保護影響評估：**資料保護影響評估（Data Protection Impact Assessments，DPIA）主要是要辨識業務流程中，有哪些涉及個人隱私權利的風險，並加以衡量、管理和因應；而且在進行評估前，也應該先確認相關的業務活動與帶來的隱私風險，是否具有其對稱性和必要性。
10. **提高罰則金額，甚至以全球營業額計算罰金金額：**為了讓企業更有警覺，GDPR 更大幅提高罰金金額。罰款分兩種情境做處罰，第一種是沒有合法理由，拒絕當事人刪除個人資料的請求，也沒有建立對企業或用戶資料保護的文件化管理系統時，最高可以處罰 1 千萬歐元（約新臺幣 3.6 億元），或者是全球營業總額的 2%作為罰款。如果是更嚴重的違規，不論是非法處理個資；沒有合法理由，拒絕用戶停止處理個資的請求；在資料外洩事故發生後，沒有及時通知個資監管機構；沒有執行隱私風險評估（DPIA）；沒有任命資料保護長；違法向第三國傳輸個資等違規行為，最高可以處罰 2,000 萬歐元（新臺幣 7.2 億元）或是全球營業總額 4%，取較高者。

NIS Directive 為歐洲議會於 2016 年 7 月 6 日通過公布，於當年 8 月生效，會員國須於指令生效後 21 個月內即 2018 年 5 月，將指令之內容適用至其本國法並公布之，並在之後的 6 個月（2018 年 11 月）確認各個基礎營運商的導入狀況。網路與資訊系統安全指令要求仰賴資訊與通訊技術的基礎服務重視資安問題，涵蓋能源、運輸、水力、金融、健康醫療與數位基礎建設等領域，業者必須採取適當的安全措施，並在發生重大資安事件時通報有關單位。除了上述的基礎服務營運商之外，NIS Directive 還適用於諸如搜尋引擎、雲端運算服務及線上市集等數位服務供應商。

為了促進會員國間之策略合作及資訊交換，歐盟設立合作小組，及建立電腦安全事件因應小組（Computer Security Incident Response Teams, CSIRTs），主要負責監測國家資安事件、並對資安風險預警、因應及分析等，另為確保各會員國彼此間在運作上之迅速與效率，並建立電腦安全事件因應小組網路（CSIRTs network），提供各會員國交換資安風險或事件相關資訊之平台。目的是希望歐盟內之關鍵基礎服務營運商及數位服務提供者就資訊交換、合作及共通安全要求上有建立及規劃之基本能力，以提高歐盟內部市場之功能。

六、國家安全和國際關係中的網路安全議題

（Cyber Security Issues in National Security and International Relations）

演講人：美國北卡羅萊納州立大學教授 -Dr. Nir Kshetri

圖 12. 美國北卡羅萊納州立大學教授 -Dr. Nir Kshetri

網絡安全在國家安全和國際關係，此講強調網路安全已成為前所未見的國際政治的重要變數。目前國際間主要的解決方案是基於歐盟各國所主導的 The Council of Europe Convention on Cybercrime 歐盟網絡犯罪公約（CoECoC），截至 2018 年 11 月 19 日為止，共有 65 個國家簽署了 CoECoC，但此公約的功能並非全面，原因如下：

1. **網路犯罪公約僅採用模糊的網絡犯罪定義及相關概念**（僅包含各國承認網路犯罪的最大公約數），例如：阻斷服務攻擊 DOS、網路兒少犯罪等，並非包含所有的網路犯罪型態。
2. **並非所有的重要經濟體都認同 CoECoC**，如著名的金磚四國（巴西、俄羅斯、印度和中國）目前都不是簽約國。
3. **即使是已簽約的各協約國，各國關注的網路犯罪議題不同**，導致跨國合作仍然不易，例如：日本境內並無網路恐怖主義問題。
4. **部分 CoECoC 協約國家網路執法能力不足**，無力取締不法網路活動，成為防堵國際網路犯罪的漏洞。

對此，講者所建議的解決方案/政策：

1. **強化及建立區域的執法機構**，幫助發開發中的經濟體（如南歐國家）處理新興的網路犯罪問題。
2. **建立非官方的合作協議**，減少全球化帶來的摩擦（如全球航空業或

金融業內的網路安全合作協議）。

3. **鼓勵並協助各國加入西方所主導的網路犯罪協防體系**。
4. **善用現有的國際/區域組織及其影響力**，補足 COECOC 的不足。
5. **針對特定的攻擊要有量身訂製的解決方案**，例如：南韓為了防禦北韓的 GPS 干擾攻擊（GPS 蓋臺），制訂專用的攻擊來源追蹤系統。

七、人工智慧與 IT 科技之網路安全

（Artificial Intelligence and Security & A Global Agenda for More Secure IT）

主講人：Dr. Patricia Longstaff、Dr. Arnd Weber

圖 13. 主講人：Dr. Patricia Longstaff

此講 Dr. Patricia Longstaff 探討了人工智能對受控與不受控對人類安全的風險，講述對人工智能發展應謹慎戒懼。

Dr. Arnd Weber 除講述 IT 產品製造之透明化，為顧及工業製造之產品性能要求，阿忍博士以空中巴士採購零件為例，說明零件符合資通安全標準有利於採購作業。

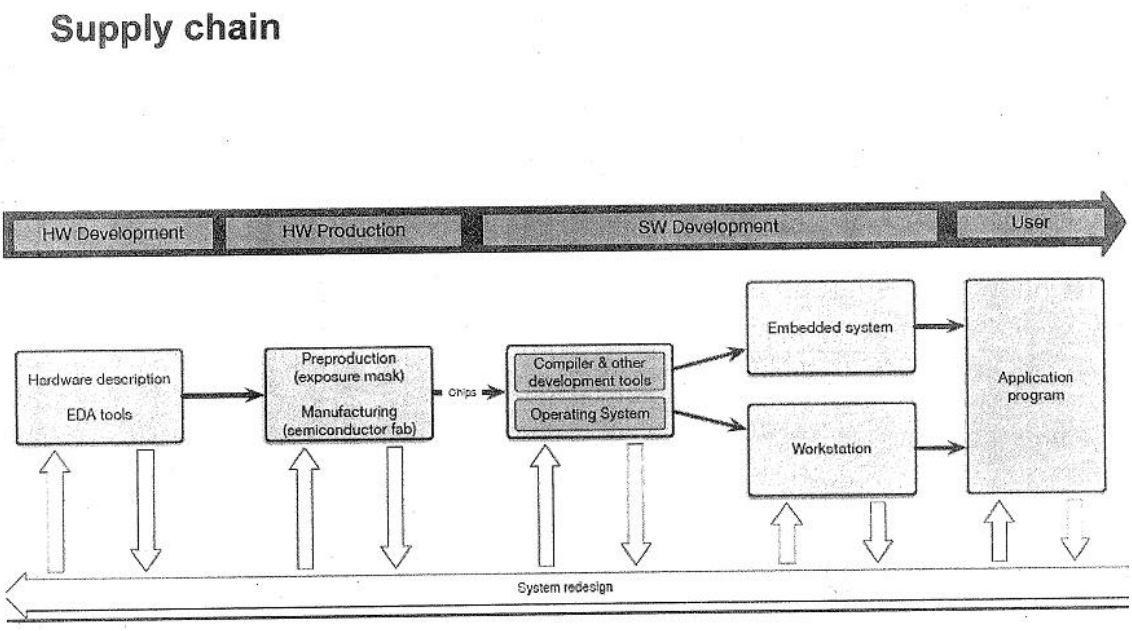

圖 14. 網路安全融入供應鏈示意圖（圖片引自講者投影片）

八、構建泰國的資料保護及網路安全架構

（Building a Comprehensive Data Protection and Cyber Security Framework for Thailand）

演講人：SCF 企業有限公司 -Dr. Simon Forge

圖 15. 英國 SCF 聯營有限公司董事 - Dr. Simon Forge

此講介紹泰國於數位時代下的威脅及對應的數據保護和網絡安全架

構，強調在這個快速發展的網路環境中建立全面安全結構，為網路資料提供足夠的保護。

介紹泰國所面對的主要網路安全威脅來源，包含：網路犯罪、網路恐怖主義、商業間諜、駭客、內部人員、腳本小子（特指利用現成駭客軟體犯罪的低階犯罪者）等。其中講者特別強調來自「內部」的威脅，在泰國有 55% 的威脅來自組織內部的人員濫用（含系統的錯誤操作）；32%的組織反應前述將內部威脅造成的損失大於外部威脅。主要的關鍵威脅目標包含政府機關、產業、基礎設施及一般民眾。

講者也特別強調泰國政府為呼應大眾對資料保護的需求，就在今年初剛剛通過資料保護法的修訂，將資料控制者（所有者）與處理者的概念納入，直接增加資料處理者的義務，包刮增加資料保護的安全措施和將違規（安全）事件主動通知資料控制者的義務，泰國也是為數不多直接引入資料控制人「合法利益」概念的國家之一。

針對以上威脅，泰國政府參考歐盟及部分已開發國家的經驗，成立國家層級的網路安全專責機關，直屬內閣部長督導，建立全國統一網路防禦架構包含：國家緊急應變中心（CERT）、資料共享及分析中心、政府 APT 攻擊反應機制、針對關鍵基礎建設的產業整合機制、民間及教育單位的支援。

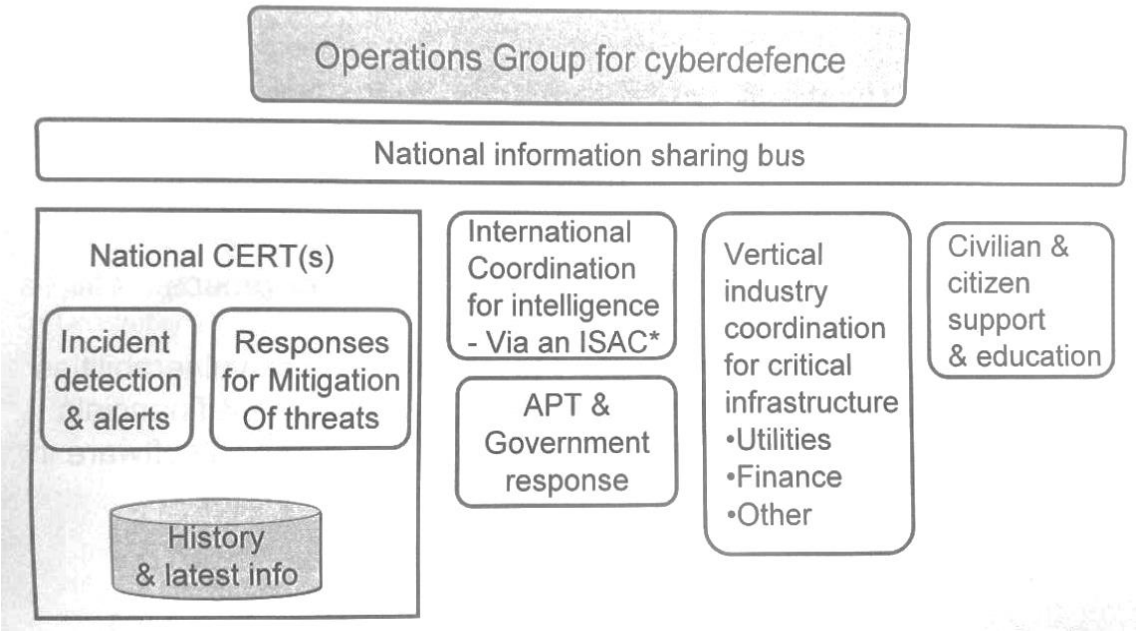

圖 16. 泰國政府的網路安全架構（圖片引自講者投影片）

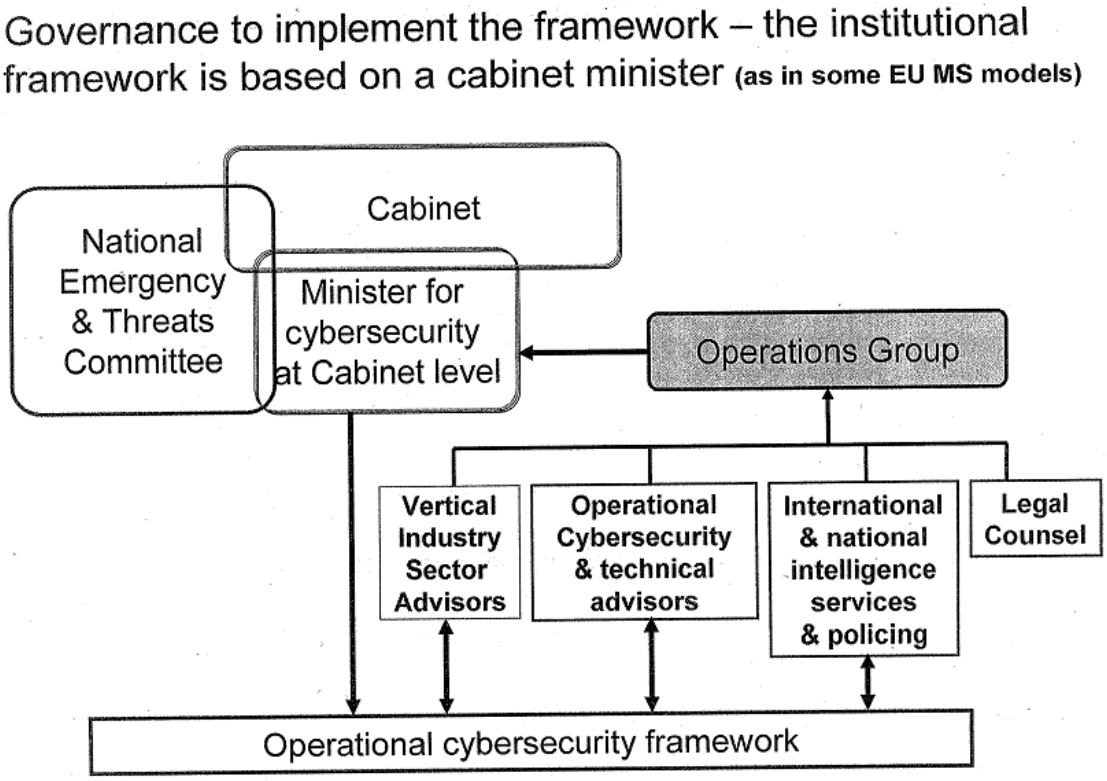

圖 17. 講者建議的泰國政府網路安全架構（圖片引自講者投影片）

圖 18. 本會王簡任技正智遠與主持人 Dr. Erik Bohlin 交流合影

肆、心得及建議

近年來，資安威脅型態之轉變已使全球各國均面臨嚴峻考驗，新型態的威脅也層出不窮。例如人工智慧（AI）所帶來的資安風險，即為近期衍生的安全挑戰。在「人工智慧與安全」（Artificial Intelligence and Security）一講中，本會與會人員與講者 Dr. Patricia Longstaff 探討政府面臨人工智慧所帶來的便利及挑戰，宜採取嚴謹的態度杜絕危害，亦或是採開放的態度擁抱新科技。泰國與會成員亦提問關於俄羅斯、中國等國都已致力於發展 AI 武器化帶來的風險應如何因應。Dr. Longstaff 表示：人工智慧帶來的風險，解決方案往往也在 AI 本身。例如在近期 AI 在自動化系統入侵的領域已經取得很大的進展，對駭客來講，AI 可以大幅提高攻擊效率（如透過機器學習分析社群媒體上的訊息，再依照這些個人化資訊發起針對性攻擊），另外也可以利用 AI 的學習能力躲避入侵偵測。但對於防禦方，AI 的地位同樣重要，目前 AI 已經被大量用於資安產品，包含病毒掃瞄、入侵偵測與防禦等等，都少不了人工智慧的運用。是以 Dr. Longstaff 建議，人工智慧雖然會對政府及社會帶來前所為有的風險，但科技的發展是不可阻擋的趨勢，政府宜採開放的態度接受新科技的運用，以符合時代潮流。

另本次會議以非常大的篇幅在探討各國的資料保護政策及措施。參諸國際近年對於資通安全保護之趨勢，各先進國家莫不將資安議題提升至國家安全層次，並訂立專法加以規範，例如：美國的聯邦資訊安全現代化法、網路安全法、日本的網路安全基本法等；在國際組織部分，歐盟近日亦通過網路與資訊系統安全指令，且要求會員國應加以規範之對象，除了公務機關、關鍵服務營運者外，更已擴張至數位服務提供者。我國亦訂定資通安全管理法，於 2019 年 1 月 1 日正式實施。

從目前各先進國家（歐盟為主）的措施我們可以學習到制定政策需要長期規劃外，還需努力整合及建立適當主要機構推動執行，關鍵基礎建設保護雖然是高成本，但若保護失效所付出代價更大。另因應未來新威脅，投資重要研發是必要的。民國 99 年我國訂定之個人資料保護法，其與 GDPR 差別，在當事人之權利部分，除以往之資料查詢、複製、更正及刪除權之外，GDPR 更進一步賦予當事人得請求資料管理者及處理者刪除連結

（被遺忘權）、要求以可共同操作之格式提供資料（資料可攜權）等權利。

歐盟近期有關網路安全及資料保護政策為資料保護一般規則（General Data Protection Regulation，簡稱 GDPR）在資料管理者部分，新增資料保護影響評估、資料保護長等制度，十分值得我國借鏡。惟 GDPR 諸多新穎性規範，實務上究應如何運作，仍待歐盟資料保護工作小組持續訂定規範加以補充，值得我國相關單位持續追蹤觀察。

附錄、大會議程

National Broadcasting and Telecommunications Commission
& International Telecommunications Society

Global Cyber Security Opportunities and Challenges Conference

6-7 December, 2018
Conference Venue:Sofitel Bangkok
189 Sukhumvit Road Soi 13-15, Klongtoey Nua, Wattana,Bangkok 10110

DAY 1: Thursday 6 December, 2018

Time		
8:30 – 9:00	**REGISTRATION**	Venue: Sofitel Bangkok, Ballroom 1-2, Floor 7
9:00 – 9:15	**WELCOME AND OPENING REMARKS**	**Dr. Erik Bohlin** International Telecommunications Society & Professor, Chalmers University of Technology, Sweden **Speaker TBC** Title National Broadcasting and Telecommunications Commission **Speaker TBC** Title National Broadcasting and Telecommunications Commission
9:15 – 10:45	***Session 1***	***The Current State of Cyber Security*** **Dr. Nir Kshetri** Professor, University of North Carolina at Greensboro, United States
10:45 – 11:00	**MORNING TEA BREAK**	Venue: Ballroom 1-2 Foyer, Floor 7
11:00 – 12:30	***Session 2***	***The Cyber Security Policies in Major Asian Economies*** **Dr. Nir Kshetri** Professor, University of North Carolina at Greensboro, United States
12:30 – 13:30	**LUNCH**	Venue: Voilà! Restaurant, Floor 2
13.30 – 15.00	***Session 3***	***Incentives for Providing Personal Information for Big-Data Services in Time of Large-Scale Disasters*** **Dr. Hitoshi Mitomo** Professor, Waseda University, Japan
15:00 – 15:15	**AFTERNOON TEA BREAK**	Venue: Ballroom 1-2 Foyer, Floor 7

15:15 – 16:45	***Session 4***	***Cyber Security for Industry*** **Dr. Arnd Weber** Senior Researcher, Karlsruhe Institute of Technology, Germany
16.45-17.00		***Discussion and Q&A*** **Dr. Erik Bohlin** International Telecommunications Society & Professor, Chalmers University of Technology, Sweden
17:00	**CLOSE OF DAY**	**Dr. Erik Bohlin** International Telecommunications Society & Professor, Chalmers University of Technology, Sweden (Transportation will be provided for Dinner Reception)
18:00	**Dinner Reception**	Venue: Baan Khanitha at Fifty Three, 31 Soi Sukhumvit 53, Sukhumvit Rd., Klongton Nua, Wattana, Bangkok 10110 BTS sky train at Thonglor Station (Exit 1)

DAY 2: Friday December 7, 2018

Time		
8:30 – 9:00	**REGISTRATION**	Venue: room TBC
9:00 – 9:15	**WELCOME AND INTRODUCTION DAY 2**	**Dr. Erik Bohlin** Professor, International Telecommunications Society & Chalmers University of Technology, Sweden
9:15 – 10:45	***Session 1***	***Recent Policy Initiatives in the EU for Cyber Security and Data Protection*** **Dr. Simon Forge** Director, SCF Associates, United Kingdom
10:45 – 11:00	**MORNING TEA BREAK**	Venue: Ballroom 1-2 Foyer, Floor 7
11:00 – 12:30	***Session 2***	***Cyber Security Issues in National Security and International Relations*** **Dr. Nir Kshetri** Professor, University of North Carolina at Greensboro, United States
12:30 – 13:30	**LUNCH**	Venue: Voilà! Restaurant, Floor 2
13.30 – 14.30	***Session 3***	***Building a Comprehensive Data Protection and Cyber Security Framework for Thailand*** **Dr. Simon Forge** Director, SCF Associates, United Kingdom
14:30 – 14:45	**AFTERNOON TEA BREAK**	Venue: Ballroom 1-2 Foyer, Floor 7
14:45 – 16:45	**Session 4**	***Artificial Intelligence and Security*** **Dr. Patricia Longstaff** Syracuse University, USA ***A Global Agenda for More Secure IT*** **Dr. Arnd Weber** Senior Researcher, Karlsruhe Institute of Technology, Germany
16:45 – 17:00		***Discussion and Q&A*** **Dr. Erik Bohlin** International Telecommunications Society & Professor, Chalmers University of Technology, Sweden
17:00	**CLOSE OF CONFERENCE**	**Dr. Erik Bohlin** Professor, Chalmers University of Technology, Sweden & **Speaker TBC** National Broadcasting and Telecommunications Commission