財團法人台灣網路資訊中心因公出國人員報告書

107 年11 月 16 日

報告人 姓　名	黃耀輝、江奕昉	服務單位及職稱	網資組 資深工程師、管理師
出國期間	107 年 10 月 20 日 至107 年 10 月 24 日	出國地點	上海
機密等級	□　機密　□ 密　■一般		
出國事由	報告書內容應包含： 一、出國目的 二、考察、訪問過程 三、考察、訪問心得 四、建議意見 五、其他相關事項或資料 （內容超出一頁時，可由下頁寫起）		
授　權 聲　明　欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人：　　（簽章）		

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

目錄

一、 出國目的

本次出國主要目的為代表台灣電腦網路危機處理暨協調中心（Taiwan Computer Emergency Response Team / Coordination Center, TWCERT/CC）（以下簡稱 TWCERT/CC）前往上海參與今（2018）年由中國國家互聯網應急中心（National Computer Network Emergency Response Technical Team/Coordination Center of China, CNCERT/CC）（以下簡稱 CNCERT/CC）主辦之 2018 年亞太地區電腦網路危機處理小組（Asia Pacific Computer Emergency Response Team, APCERT）（以下簡稱 APCERT）年會與研討會（Annual General Meeting & Conference）。

APCERT 為亞太地區著名的國際資通訊安全組織，主要由亞太地區各國政府及相關單位所成立的電腦網路危機處理小組（Computer Emergency Response Team, CERT）（以下簡稱 CERT）以及電腦網路安全事件應變小組（Computer Security Incident Response Team, CSIRT）（以下簡稱 CSIRT）所組成。

本次代表 TWCERT/CC 前往上海參與 2018 年 APCERT 年會，增進亞太地區各電腦網路危機處理（Computer Emergency Response Team, CERT）組織間之交流，並透過各國以及各工作小組（Working Group）的近況報告和未來發展計畫，互相學習以強化我國 CERT 營運模式和發展計畫。同時增加本單位於國際上之知名度，確立和他國之良好互動，以利未來資安情資的交流互利，以期達到更加全面完備的網路防護體系。

二、 考察、訪問過程

表 1 10 月 21 日大會議程安排

Sunday, 21st October 2018	Event	Venue: Westin Bund Center Shanghai
8:30	Registration Open	Diamond Ballroom Foyer （3F）

9:00-12:00	Working Group Meetings	Diamond Ballroom II （3F）
12:00 – 17:00	Lunch and APCERT Team Building	Diamond Ballroom III （3F）

表 2 10 月 22 日大會議程安排

Monday, 22nd October 2018	Event	Venue: Westin Bund Center Shanghai
8:30	Registration Open	Diamond Ballroom Foyer（3F）
9:00 – 12:00	Technical Training: Digital Forensics with a Focus on the Cloud	Diamond Ballroom I （3F）
12:00 – 13:30	Lunch	The Stage （1F）
14:00 – 17:00	Steering Committee Meeting	Turquoise （3F）

表 3 10 月 23 日大會議程安排

Tuesday, 23rd October 2018	Event	Venue: Westin Bund Center Shanghai
8:30	Registration Open	Diamond Ballroom I&II Foyer（3F）
9:00 – 12:00	Closed Conference	Diamond Ballroom I&II （3F）
12:00 – 13:30	Lunch	The Stage （1F）
14:00 – 17:30	Annual General Meeting	Diamond Ballroom I&II （3F）
18:00 – 20:00	Gala Dinner	The Crystal Garden （5F）

表 4 10 月 24 日大會議程安排

24 October 2018 Venue: Westin Bund Center Shanghai，Diamond Ballroom I&II （3F）		
Time	Session	Presenter
8:30-9:00	Registration Open	
9:00-9:25	Welcome Remarks	Chair/Host
9:25-9:30	Handover Ceremony	CERT-In, CNCERT
9:30-10:00	Keynote Speech	CNCERT
10:00-10:30	APNIC Community Honeynet Project	Adli Wahid, Senior Internet Security Specialist, APNIC
10:30-10:50	Tea Break	
10:50-11:20	Splunking Honeynet Data （LebahNET）	Muhammad Zuhair Abd Rahman, Analyst, MyCERT

11:20-11:50	TBD	Denzel Song, General Manager, Huawei
11:50-12:20	Recent Internet Incident Trends in S.Korea	JAE HYOUNG LEE, Manager, KISA
12:20-12:50	An Overview of International Cybersecurity Standardization for the IoT and Its Implication for China	Lingfei Kong, Cyber Security Director, China Unicom
12:50-14:00	Lunch Break	
14:00-14:30	National Information and Cyber Security Strategy of Sri Lanka	Rohana Palliyaguru, Director-Operations, Sri Lanka CERT|CC
14:30-14:50	OLD VULNERABILITIES ARE NEW	Eric Kaithula, Senior Program Manager, Microsoft
14:50-15:20	Safeguarding the Resource Public Key Infrastructure	Ma Di, Principal Research Fellow, ZDNS
15:20-15:40	RATs in ICS network	Evgeny Goncharov, Head of Kaspersky Lab ICS CERT, Kaspersky Lab
15:40-16:00	Tea Break	
16:00-16:30	Protecting Asian Games IT Infrastructure from Cyber Attacks	Andika Triwidada, Deputy Director, ID-CERT
16:30-16:50	Threat Intelligence Application for Fighting Against Black Industry Chain	MANTAI A, Head of Network Security Research Institute, Eversec
16:50-17:20	Exploration of Emergency Response in Various Network Environments	Yonggang Han, VP, 360 Enterprise Security Group
17:20-17:50	Panel Discussion（30min）	
17:50-17:55	Wrap Up & Closing	

三、 考察、訪問心得

1. 2018/10/21：Working Group Meeting

   由 APCERT 委員及各工作小組（Working Group），簡報各自於 2018 年度執行成效，以及預計未來在 2019 年度，可能進行的改變和優化。

   (1). Policy, Procedures and Governance Working Group （PPG-WG）

   此工作小組主要目標為通過制定和協調政策,促進 APCERT 的願景和使命。並在簡報時提出 OPFW 修正案，修改 APCERT 最低出席率、投票制度以及代理人之規範。

圖一：PPG-WG 報告

(2). Malware Mitigation WG

由馬來西亞（MyCERT）進行報告。建立分布式誘捕系統（Honeypot）– LebahNet，用以模擬網路服務之漏洞，向管理員提出攻擊警報。同時也建立了惡意程式資料庫 – CMERP，希望能有效減少被侵駭成功之機率，以及降低後續損害之風險。並且希望更多 APCERT 成員的參與，以達到全面防護之成效。

圖二：Malware Mitigation WG 報告

(3). MBS WG update：Changes in the Membership & partnership

定義新的 APCERT 成員等級，成員主要分為 Operational Member（OM）以及 Supporting Member （SM）；而合作夥伴則分為 Liaison Partner、Strategic partner 以及 Corporate partner。

圖三：KrCERT 報告

(4). Internet of Things （IoT） Security Working Group （IoT-Sec-WG）

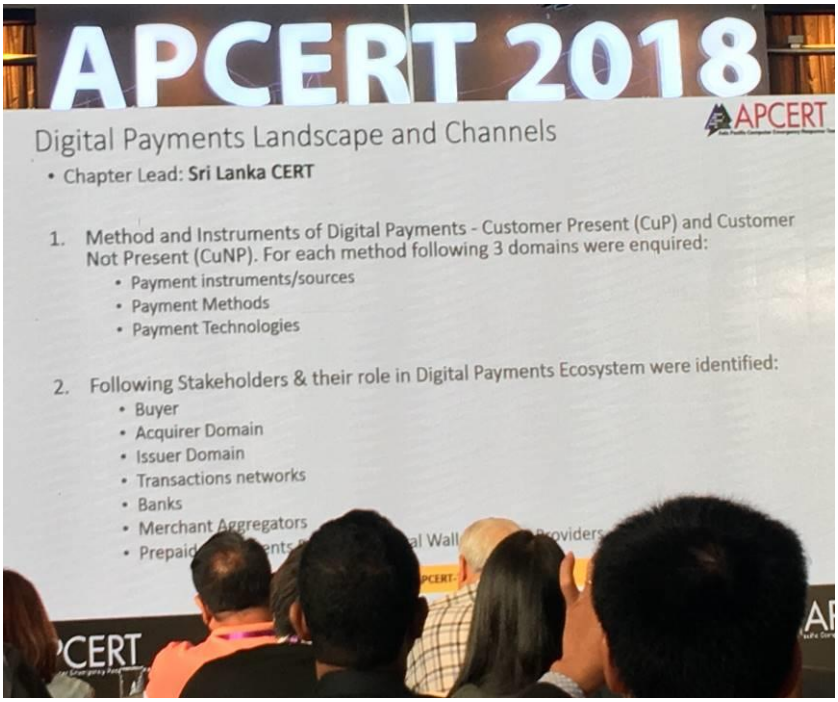
主要目的為確保物聯網裝置安全性的優先權，並建立對物聯網安全性之信任。確定對物聯網系統中的威脅和安全挑戰，並以此提出物聯網系統安全之建議，以及討論現有之物聯網系統安全標準，再以此規劃如何改善。

圖四：IoT-Sec-WG 報告

(5). Draft Working Group

此工作小組分為三個部分進行報告。第一部分是由 Sri Lanka CERT 進行報告，主要針對電子支付之方法和工具進行討論，包括 Customer Present （CuP）以及 Customer Not Present（CuNP）。並且針對每個方法，各別討論三個部分 – 支付工具/來源、支付方法以及支付技術。第二部分由 JPCERT/CC 主持，主要針對電子支付之漏洞和安全問題進行探討。第三部分由 CERT-In 主持，是針對安全電子支付工作小組提出的解決方案和建議，例如計畫未來建立 APCERT Operational Member 和相關利益者之平台建立，以提高式見響應效率和彈性。

圖五：Draft Working Group 報告



圖六：Sri Lanka CERT for Digital Payment

圖七：JPCERT/CC for vulnerabilities and security issues

圖八：CERT-In for Proposed Solutions & Recommendations

(6). Drill Working Group

此工作小組主要為執行每年度之通報應變線上演練活動，此次報告主要決議線上演練活動時間、組織委員會之建立、選擇工作小組之領導 CERT 組織，以及決定 2019 年度 Drill 線上演練主題等議題，並向在場成員尋求意見和推薦，同時也確立 2019 Drill 活動之開辦時間、地點等，目前預計於 2019 年 3 月 6 日開始通訊系統測試，2019 年 3 月

13 日開始進行線上演練活動。

此工作小組，TWCERT 為其中成員，預計於 2019 年度線上演練活動作為玩家和觀察者參與。

圖九：Drill WG 報告

(7). Information Sharing Working Group

此工作小組，主要建立和規範 APCERT 內部情資交換之標準和協定，例如此工作小組建立一情資交換平台 – APCERT DataExchanger（ADE），目前已有 29 個組織註冊、23 個組織使用中，過去已分享 7K 以上安全情資，包括 Conficker 感染之主機、Nitol 感染之主機，以及 malicious URLs 等。除此之外，此 Working Group 也建立了 Mail List，分享 CNCERT 週報、JPCERT 月報、ThaiCERT 每日之 Risk Intelligence 等。同時，也負責維護 APCERT 之 wiki 頁面。最終，此工作小組表達仍致力於改善 APCERT 成員之間的情資分享機制，以及提升 information sharing WG 的工作知名度，希冀各國成員可以更加踴躍地參與。

圖十：Information Sharing WG 報告

2. 2018/10/22：Technical Training: Digital Forensics with a Focus on the Cloud

第二天的會議由 TWNCERT 請到微軟工程師進行教育訓練，主題為 Digital Forensics with a Focus on the Cloud。本次訓練主要針對 Windows 系統中和鑑識相關的主要 Artifacts 及分析 Windows Artifacts 的開源工具做介紹。

(1). Windows Artifacts 可分 Non-Volatile Data, Volatile Data and Semi-Volatile Data，以下分別說明：

I. Non-Volatile Data：指不會消失的資料，包含 OS Information, NTFS File System, Registry Hive, Windows Event Logs, Application Logs, Browser Artifacts, AutoStart Extensibility Points （ASEPs）, Key Additional Artifacts。

i. NTFS File System：NTFS 是一個紀錄檔檔案系統，使用 NTFS 紀錄檔（$Logfile）記錄 MetaData 資料。這是 NTFS 一個非常關鍵的功能（FAT/FAT32 不提供此項功能），可確保其內部的複雜資料結構（如比較重要的如 Volume 分配圖、磁碟重組 API 產

生的資料轉移操作、MFT（主檔案表）記錄的更改情況）和索引（在目錄和安全描述符中使用）即使在作業系統當機後仍然能保證一致性，而當在 Volume 被重新載入後，可以非常容易地還原這些關鍵資料的意外修改。另外 NTFS 檔案系統還提供了 USN 紀錄檔，用於記錄 Volume 中所有檔案、資料流、目錄的內容、屬性以及各項安全設定的更改情況。應用程式可以利用紀錄檔追蹤 Volume 的更改。

ii. Registry Hive：登錄檔是 Microsoft Windows 中的一個重要的資料庫，用於儲存系統和應用程式的設定資訊。登錄檔由 key、subkey 和 value 構成。一個 key 就是樹狀資料結構中的一個節點，而 subkey 就是這個節點的子節點。一個 value 則是一個 key 的一條內容，由 name、datatype 及 data 組成。

iii. Windows Event Logs：Windows 透過不同的錄檔來記錄系統運作的資訊，主要的 3 個記錄檔為：Application、Security 及 System，Application 事件依嚴重性為標準，可區分為「錯誤」、「警告」或「資訊」。錯誤指的是顯著的問題，像是資料遺失。而警告指的是本身並非十分顯著、但以後可能會發生問題的事件。資訊事件則是描述程式、驅動程式或服務的成功操作。Security 事件稱為「稽核」，可根據事件狀況說明成功或失敗，例如使用者嘗試登入 Windows 是否成功。System 事件系統事件。系統事件為 Windows 與 Windows 系統服務記錄，同樣區分為錯誤、警告或資訊。

iv. AutoStart Extensibility Points （ASEPs）：很多惡意程式會在 windows 開機時自動啟動，在進行鑑識時需檢查這些地方，例如：Run and RunOnce, Expolorer Shell Folders, Startup and Shutdown scripts, Active Setup, Servies etc.

v. Key Additional Artifacts：有幾個主要的 Artifacts 也是鑑識會需要搜集的資訊，包括：$Recycle.Bin, LNK Files, JumpList, Prefetch 等。

vi. Browser Artifacts：網頁瀏覽器鑑識也是很重要的一項技術。網

頁瀏覽器能留下許多使用者瀏覽網頁的資訊，以下以 Microsoft Edge 及 Chrome 為例，Microsoft Edge 需留意的資訊為 History File, Last Active Browsing Session, AppCache, Cache, Cookies 等，Chrome 的部份同樣有 History File, Cache Files 及 Extesions。

- Volatile Data：指容易消失的資料，包含 Process Artifacts, Network Artifacts。
- Semi-Volatile Data：雲端服務相關，可能會消失的資料，例如：OneDrive, Email, Telemetry（Win10）, AAD/MSA accounts（Win10）。另外 Windows 10 在比較大的更新時，會將的 windows 系統程式移到 windows.old 的目錄下，所以相關舊的 Registry 和 Event logs 也會移到該目錄下。

(2). Windows Artifacts 分析開源工具：

I. MFTCSV：可將 MFT 表裡的所有紀錄導出成文字檔。

II. ExtractUSNJrnl：取得系統 USN 日誌文件。

III. USNJrnl2CSV：可將 USN 日誌文件導出成文字檔。

IV. Autopsy：瀏覽器資訊安全鑑識工具。

V. RegRipper：Registry 設定檔鑑識工具。

VI. Registry Explorer：Registry 瀏覽工具。

VII. AmcacheParser：Amcache.hve 應用程式紀錄檔分析工具。

VIII. LogParser：紀錄檔分析工具。

IX. Sysinternals：提供了許多工具，現可在微軟網站免費下載，包括了重組工具 Contig 與 PageDefrag、診斷工具如 Process Explorer 與 RootkitRevealer。

X. JumpList Explorer：捷徑清單瀏覽工具

XI. BrowsingHistoryView：瀏覽器瀏覽記錄檢視器

XII. PECmd：Windows Prefetch 解析工具

XIII. WinPrefetchView：系統預先擷取檔（.PF 格式）顯示工具。透過查看這些檔案，您可以知道每個應用程式使用了哪些檔案，或者 Windows 啟動時載入了哪些檔案。

圖十一：微軟代表講授 Digital Forensics 課程

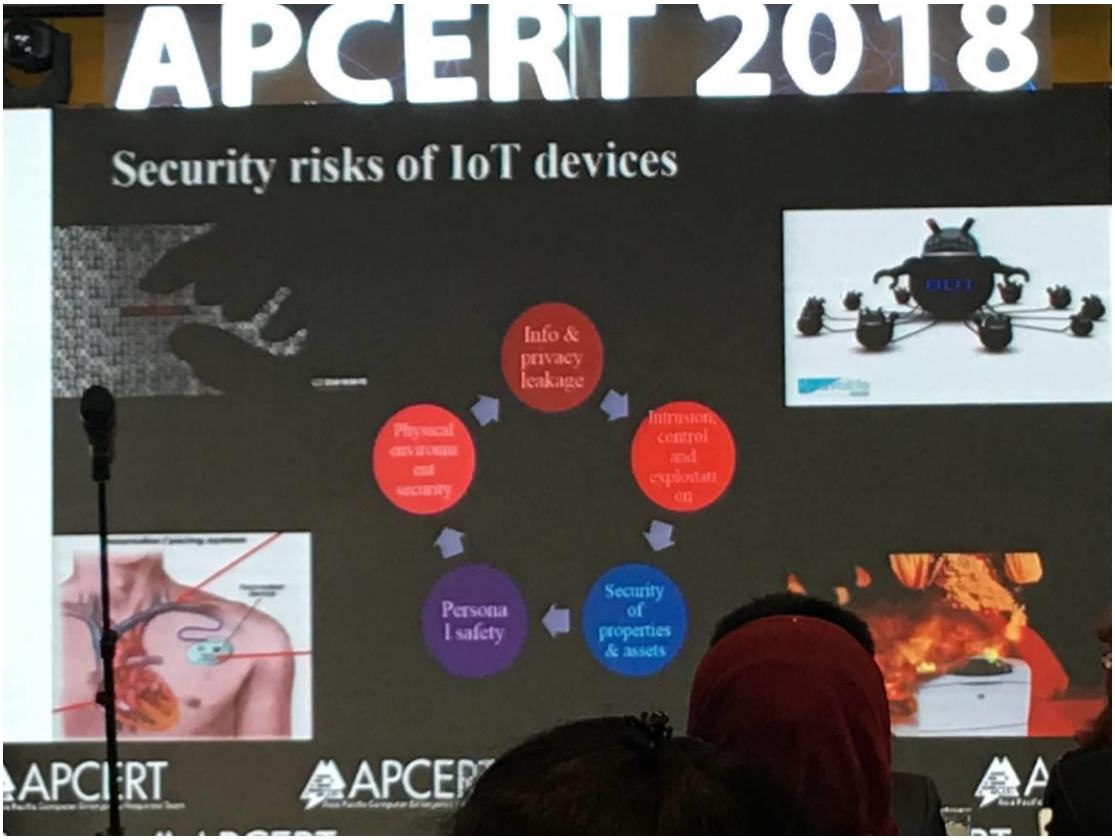
圖十二：Digital Forensics 課程現場照片

3. 2018/10/23：Closed Conference

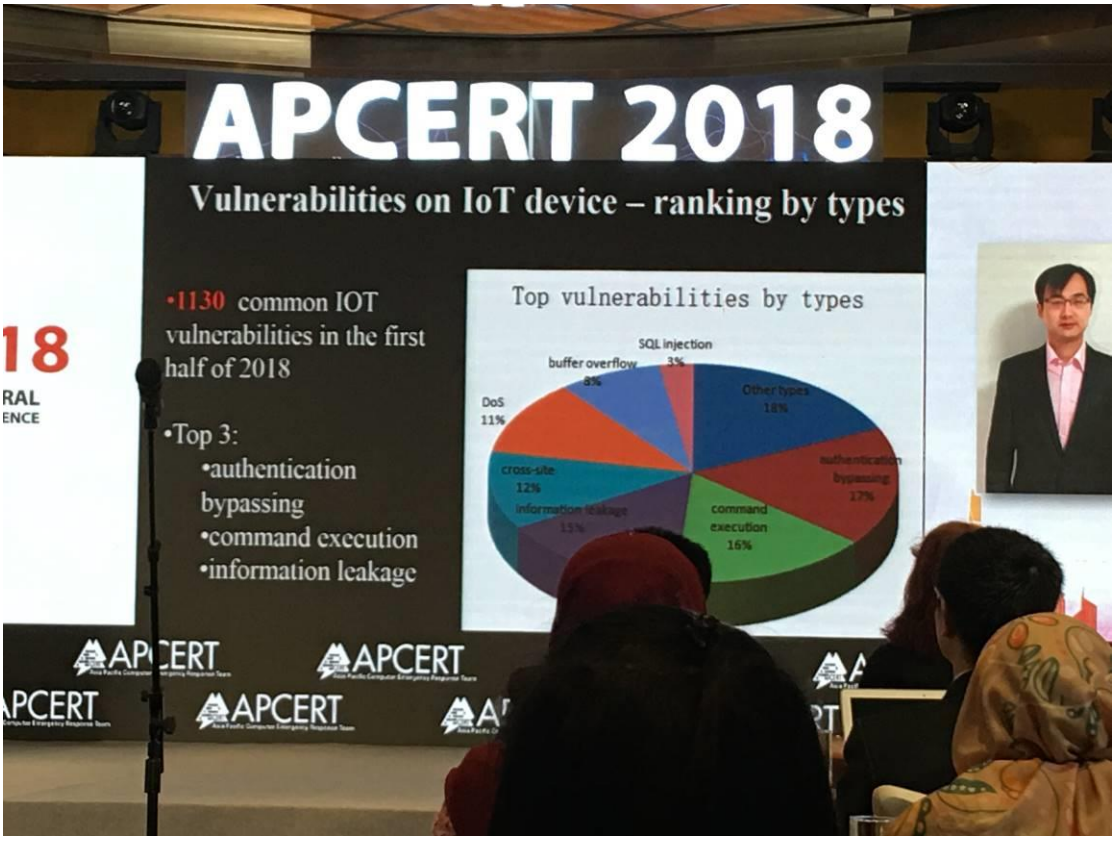
幾個 CERT 組織報告各自於 2018 年度之進度、運作狀況與資訊分享。

(1). CNCERT

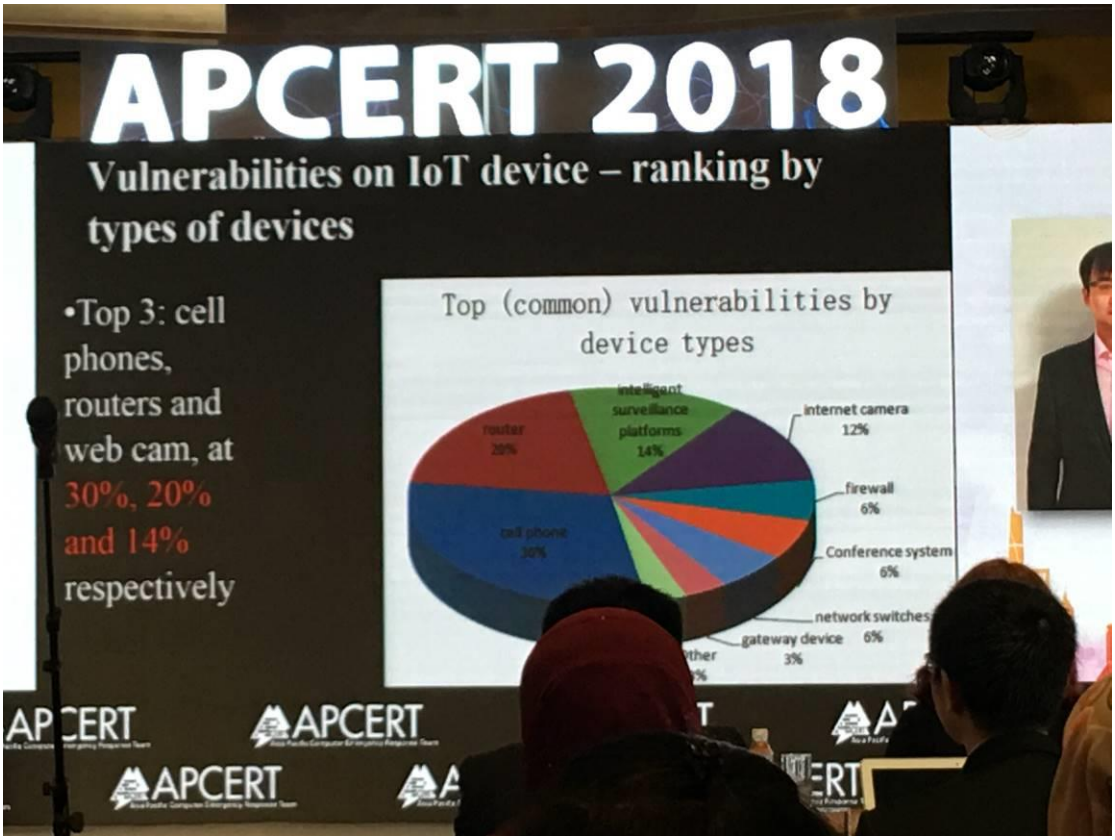
CNCERT 之報告主題為物聯網裝置的安全，探討資訊統計和安全性之風險之間關聯。並且針對物聯網之漏洞形式、以及各裝置漏洞數量等資訊進行統計。



圖十三：IoT 裝置安全風險



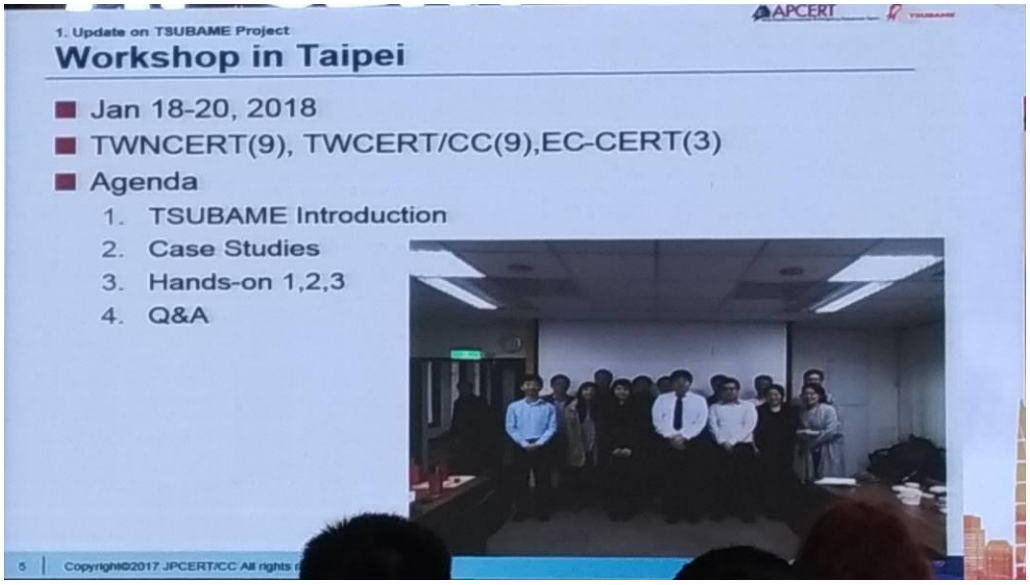
圖十四：物聯網裝置漏洞形式



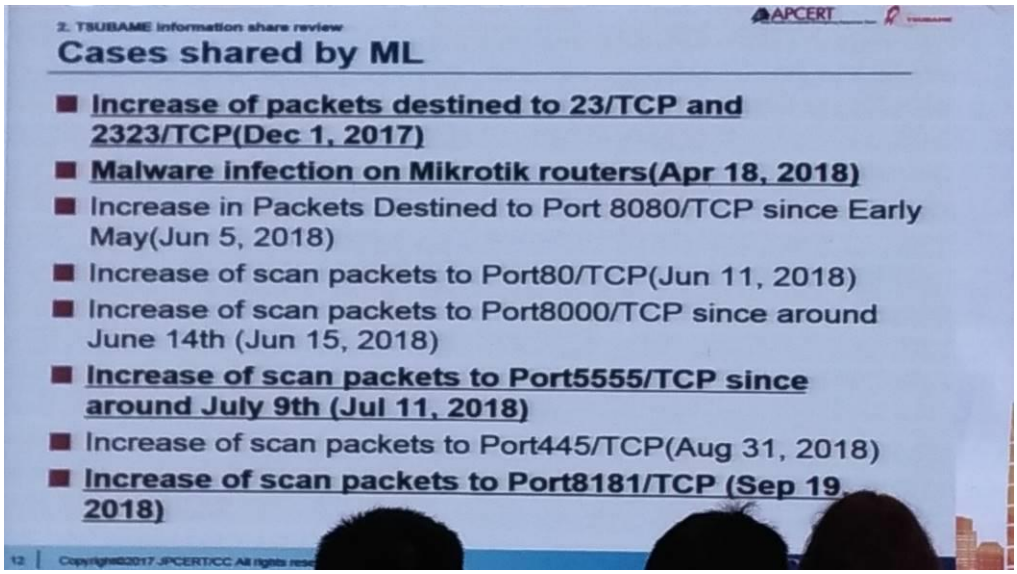
圖十五：物聯網裝置漏洞數量排序

(2). TSUBAME project

此工作小組主要是監測亞太地區網路封包之流動，監測可疑之掃描活動，並將相關情資分享予各國 CERT 組織。目前由日本 JPCERT 主導。於此報告中，JPCERT 除分享了 workshop in Taipei 之外，也顯示了香港 HKCERT 使用 TSUBAME 之實際情形，同時也分享了該計畫相關之資安事件，供在場成員學習。



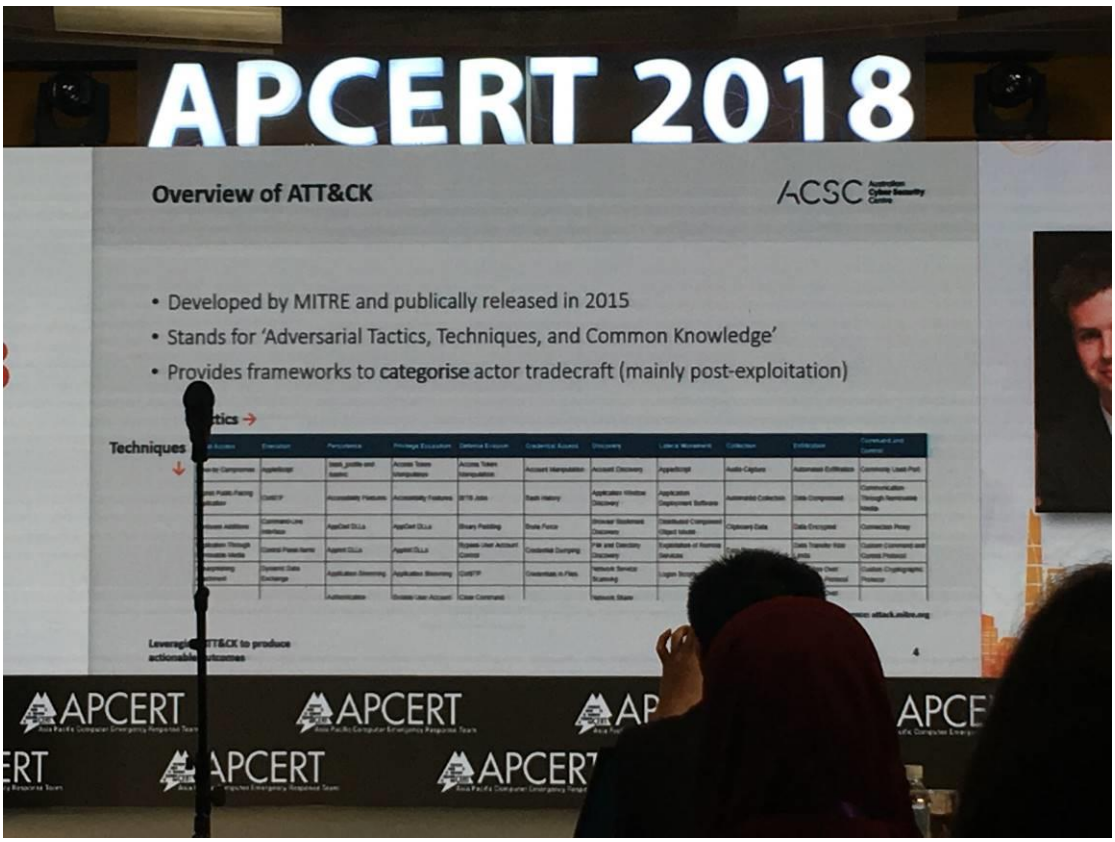
圖十六：Workshop in Taipei



圖十七：Case shared

(3). ACSC Incident Response

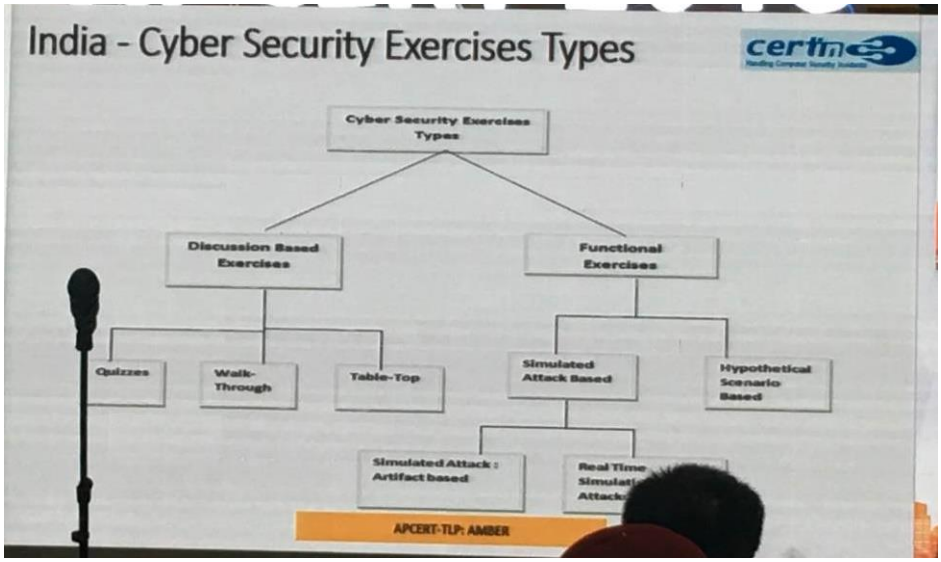
此為澳大利亞網路安全中心之報告，主要是針對 ATT&CK（對抗戰術、技術與常識）的實踐進行分享。其中提出了 common tradecraft 之侵駭形式作為實際案例，並將 MITRE 提供之 ATT&CK 用於解決方案中，期許可以更迅速、有效率地解決資安事件。



圖十八：ATT&CK

(4). India Cyber Crisis Exercise （ICCE）

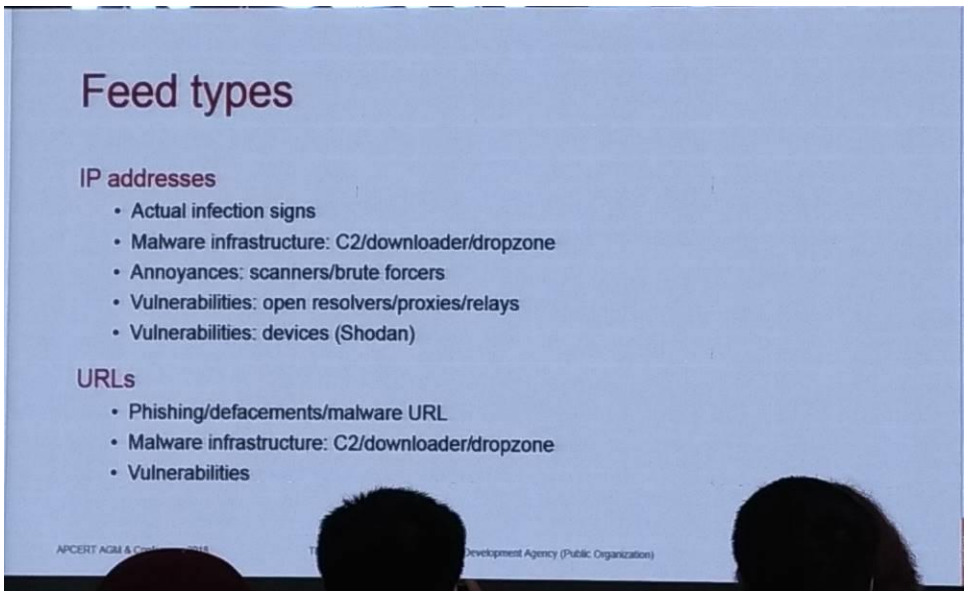
此為 CERT-In 之報告。ICCE 為基於模擬網絡安全攻擊危機情景之系統，類似於現實生活中的網絡安全危機情況，其目的為使組織能夠評估其安全流程和程序的有效性，以及能衡量攻擊檢測、響應、緩解和恢復等。



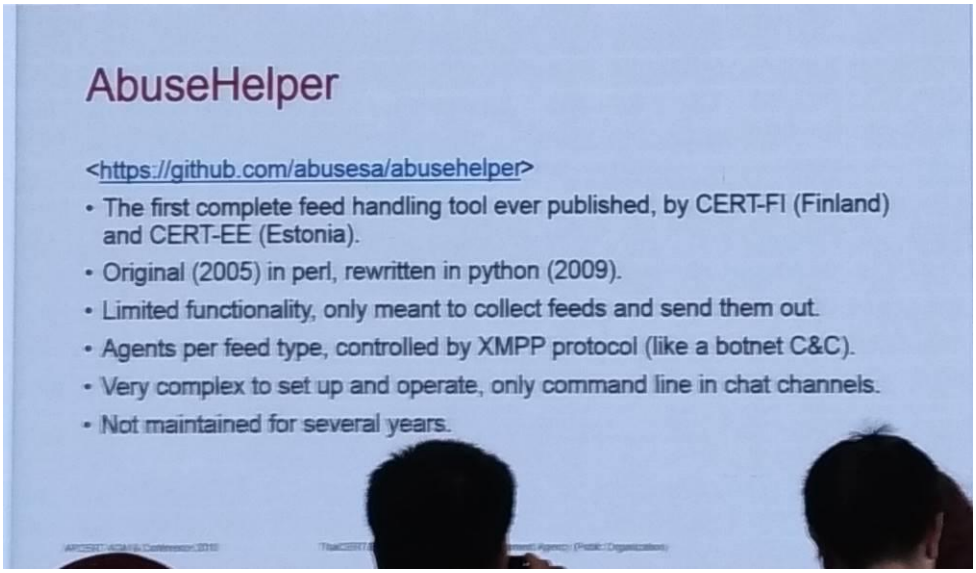
圖十九：ICCE by India

(5). ThaiCERT

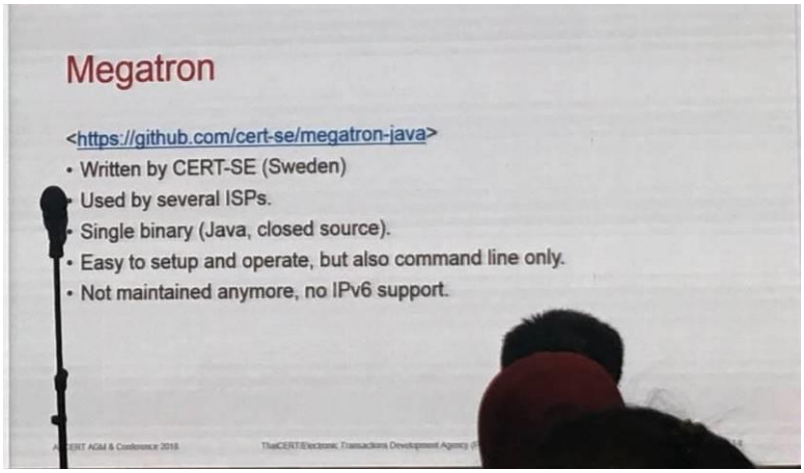
此報告主要是針對資安情資的自動分享，其分享之資料包括了 IP addresses 和 URL 等，並且建立了 Feed Sharing Infrastructure，作為情資分享之用。同時亦分享了許多情資分享之工具，例如芬蘭以及愛沙尼亞建立之 AbuseHelper、瑞典建立之 Megatron、香港之 IFAS、澳洲之 IntelMQ、波蘭之 n6 等。



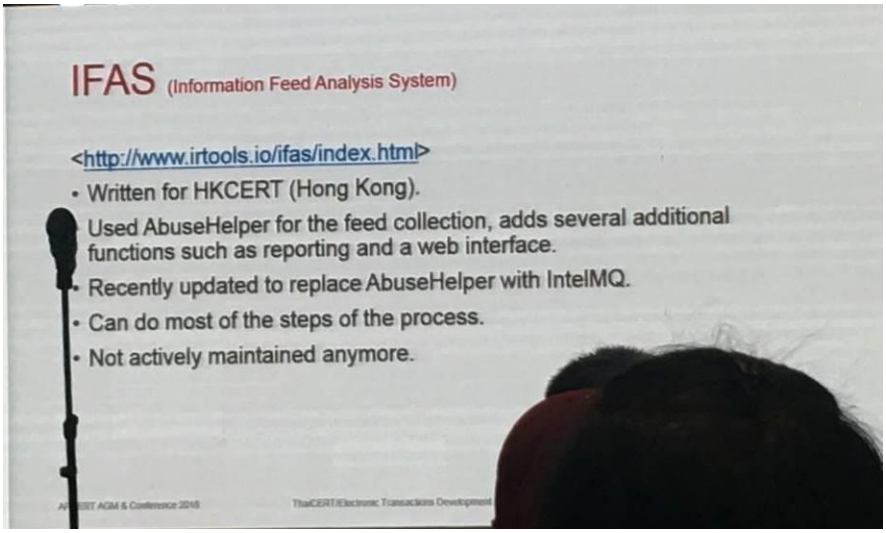
圖二十：Feed Types by ThaiCERT



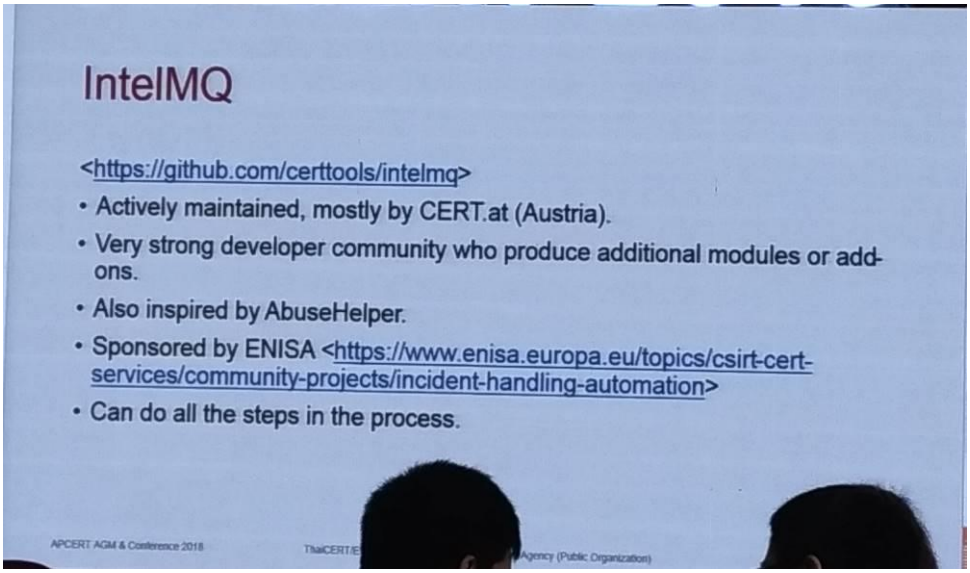
圖二十一：AbuseHelper



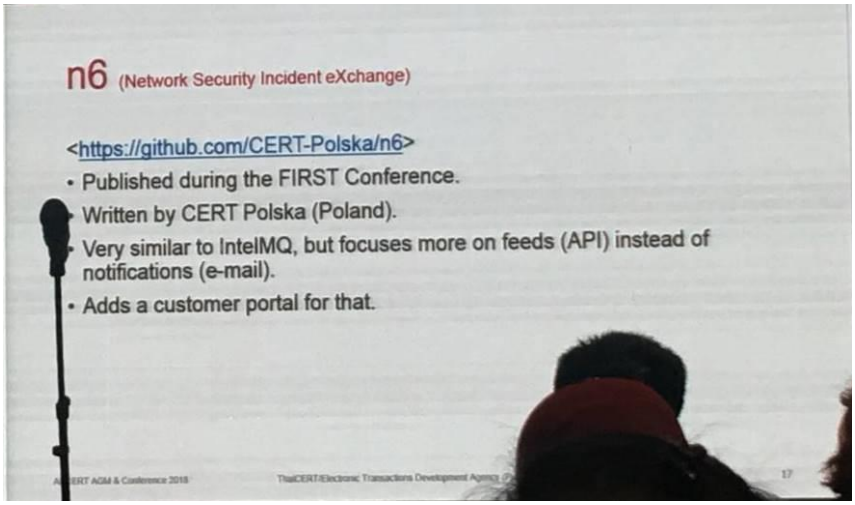
圖二十二：Megatron



圖二十三：IFAS



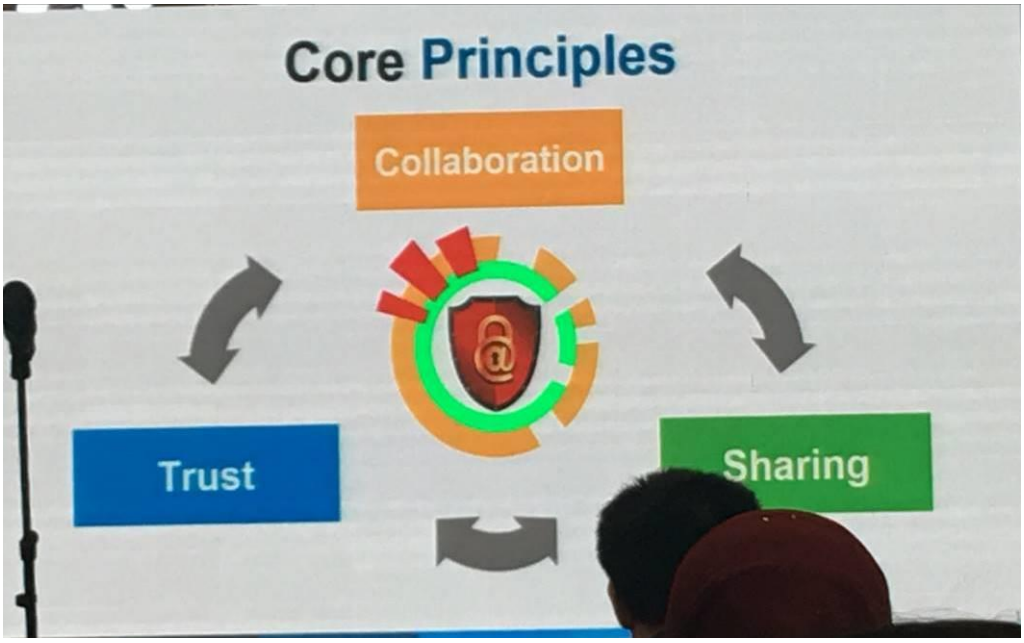
圖二十四：IntelMQ



圖二十五：n6

(6). GovCERT.HK

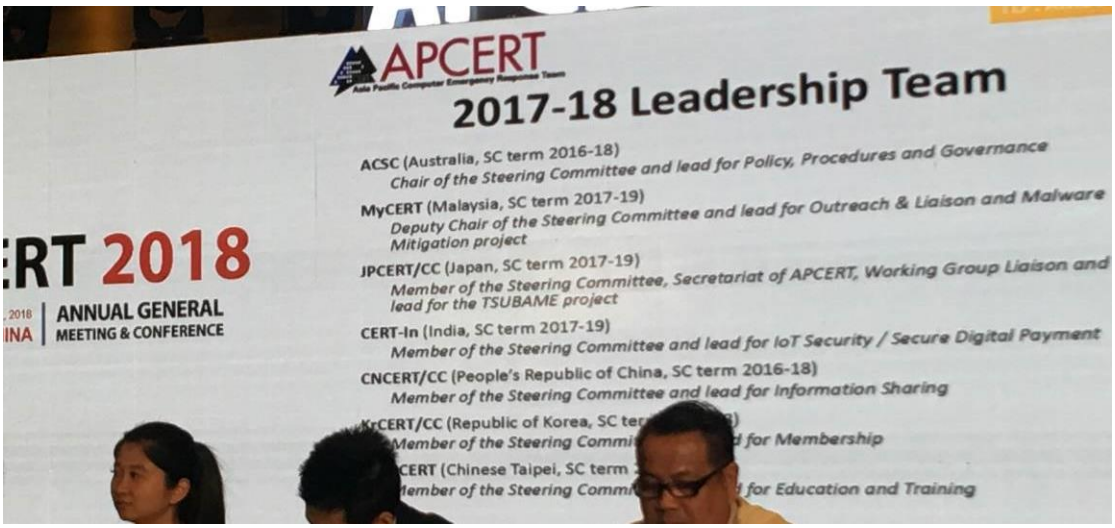
此報告主要是提出了Cybersec Infohub之計畫，為期2年的試點計劃，主要為促進不同部門的地方信息以及利益關係人之間之密切合作。其目標為建立跨部門協作網絡、提供一個協作平台，以更好地了解狀態感知、培養當地的協作文化、以及提升香港的整體網絡彈性。



圖二十六：Cybersec Infohub by GovCERT.HK

4. 2018/10/23：Annual General Meeting

此議程主要是針對所有 APCERT 委員會、Leadership Team、Working Group 進行介紹，以及說明 2017 之國際活動、訓練課程，以及 2017 之成果展示。並介紹所有委員會成員之現況、負責項目等。



圖二十七：Leadership Team

圖二十八：APCERT Working Groups

圖二十九：International Activities & Engagements

圖三十：2017 Training Courses

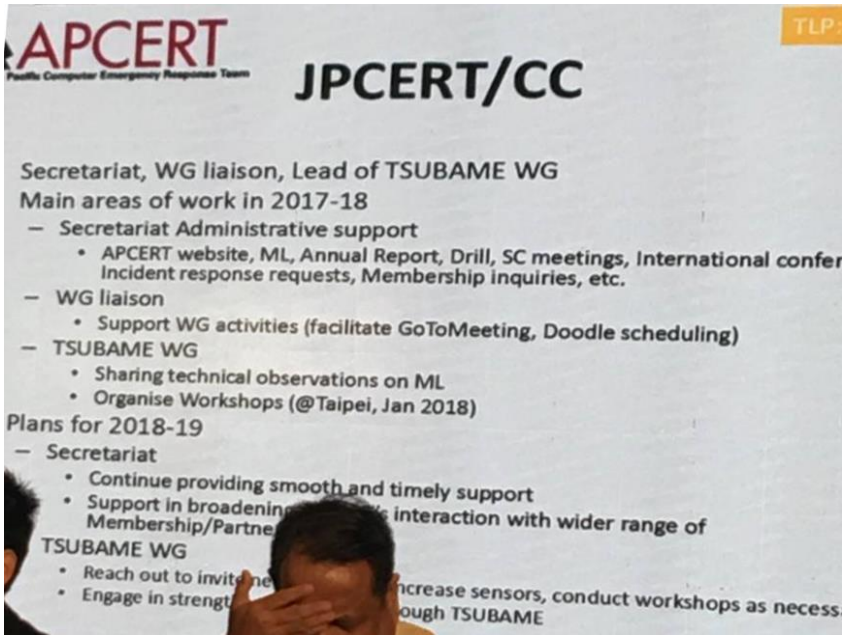
(1). ACSC

澳大利亞 CERT 組織，委員會成員、政策召集人、擔任 Procedures and Governance WG 以及 Convenor of Capacity Building WG 之領導人。

圖三十一：ACSC

(2). JPCERT/CC

日本 CERT 組織，擔任 APCERT 秘書、工作小組聯絡者、TSUBAME Working Group 領導人。



圖三十二：JPCERT/CC

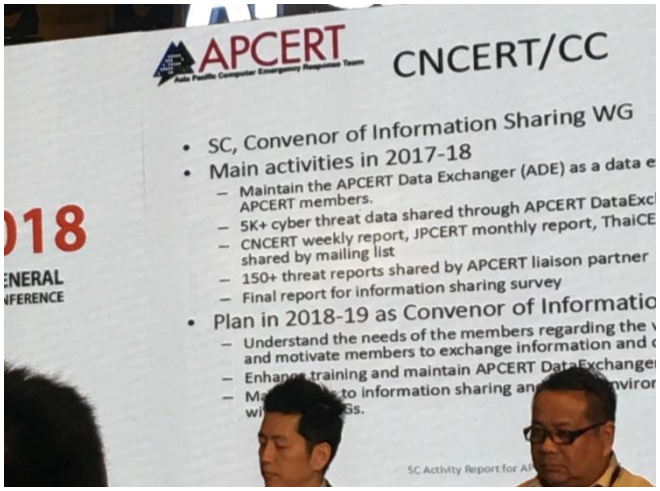
(3). CERT-In

印度 CERT 組織，委員會成員、計畫委員會成員、參與 Drill Working Group、Malware Mitigation Working Group 以及 Information Sharing Working Group 成員。

圖三十三：CERT-In

(4). CNCERT/CC

中國 CERT 組織，委員會成員、Information Sharing Working Group 召集人。



圖三十四：CNCERT/CC

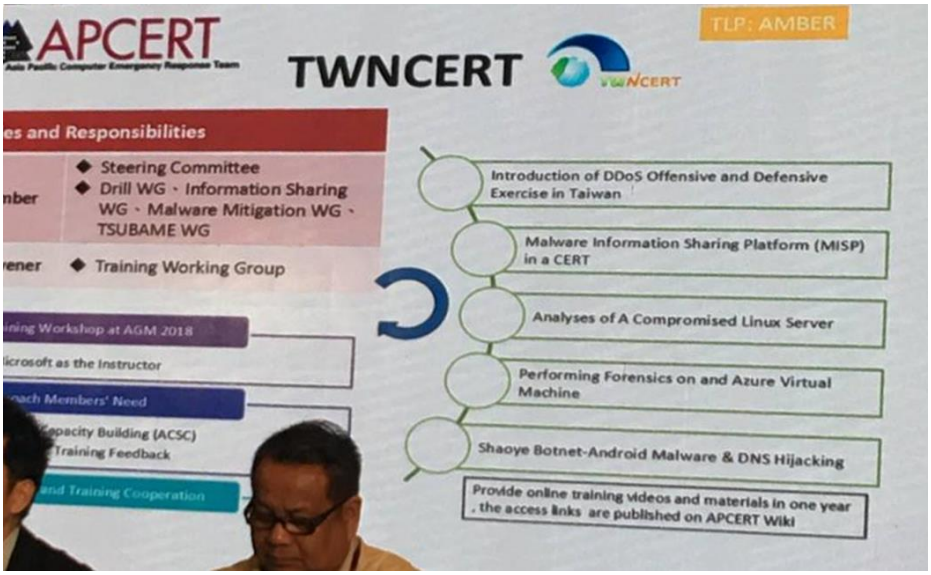
(5). KrCERT/CC

韓國 CERT 組織，委員會成員、Membership Working Group 召集人。

圖三十五：KrCERT/CC

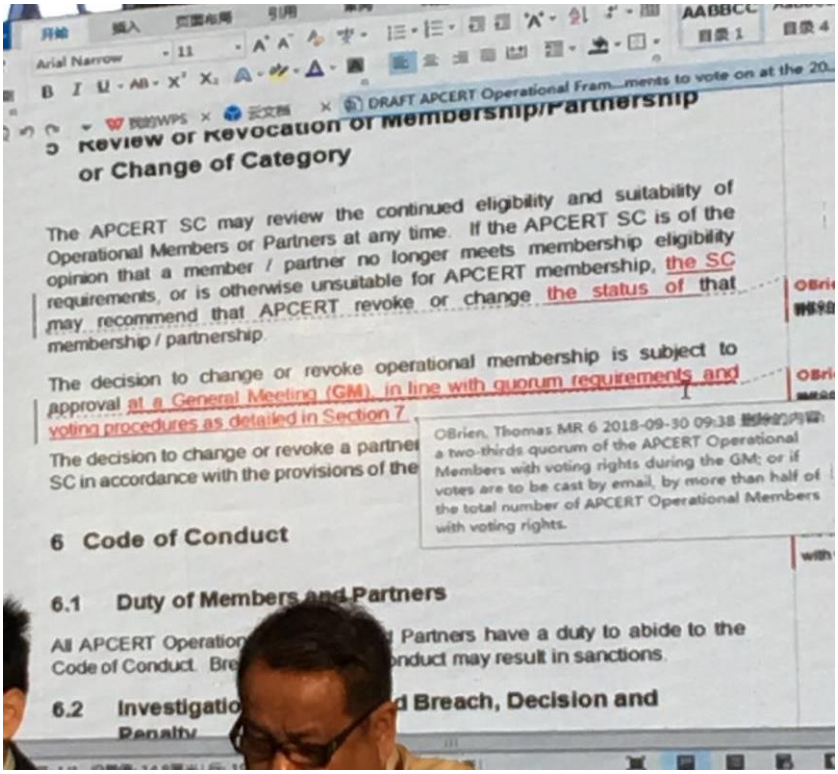
(6). TWNCERT

台灣 CERT 組織，委員會成員、Training Working Group 召集人，Drill Working Group、Information Sharing Working Group、Malware Mitigation Working Group、TSUBAME Working Group 成員。



圖三十六：TWNCERT

(7). 針對運作條文進行修改，例如投票之最少有效人數、決議所需成員比例，以及細微修整。並令在場成員進行投票，此次投標由全場一致通過條文之修正案。



圖三十七：條文修正

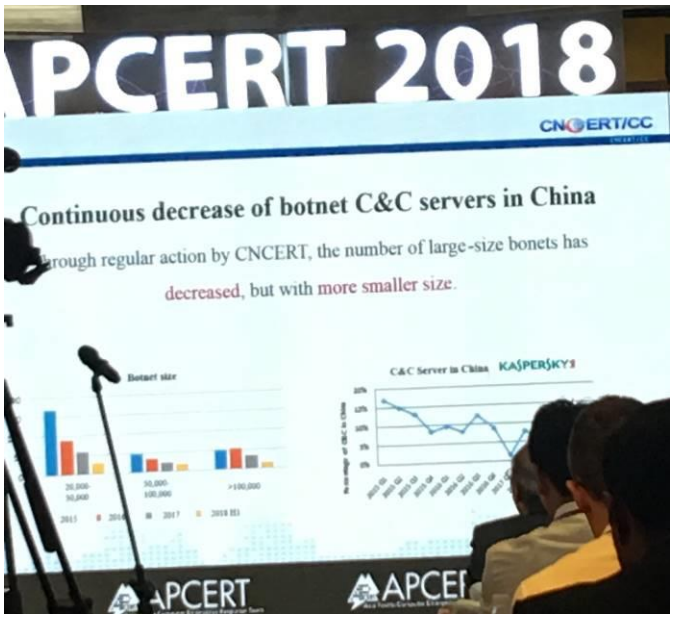
圖三十八：修正案投票通過

5. 2018/10/24：Keynote Speech

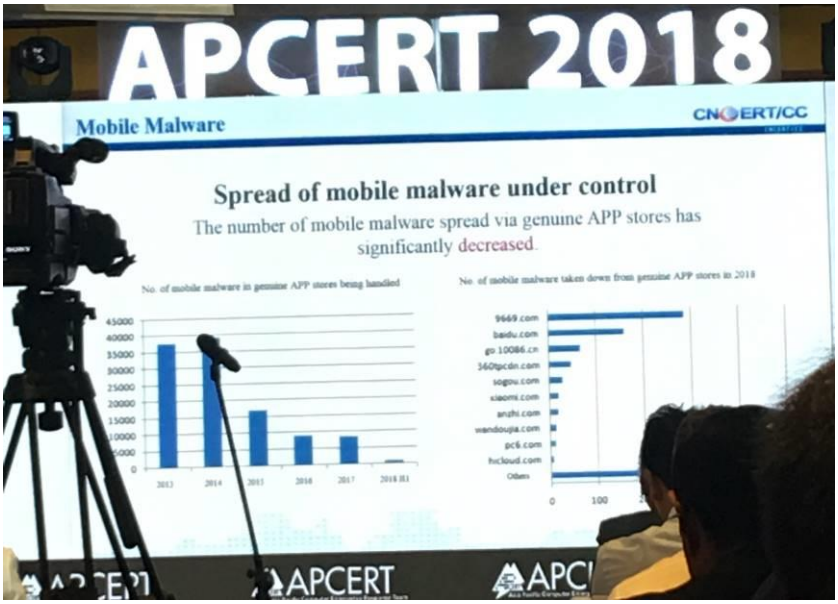
(1). Recent Cybersecurity Trends in China and International Cooperation

Practices of CNCERT

主要為 CNCERT/CC 報告關於中國之資通訊安全情形，並且提出目前主要的幾個資安風險和威脅，例如 Ransomware、DDoS、IoT、ICS，以及 APT。並說明現今中國之大規模殭屍網路中繼站數量之減少，以及行動網路之惡意軟體之管控、DDoS 統計以及 APT 攻擊統計等資訊。以及 CNCERT 和國際資通訊安全組織之合作狀況和未來發展。

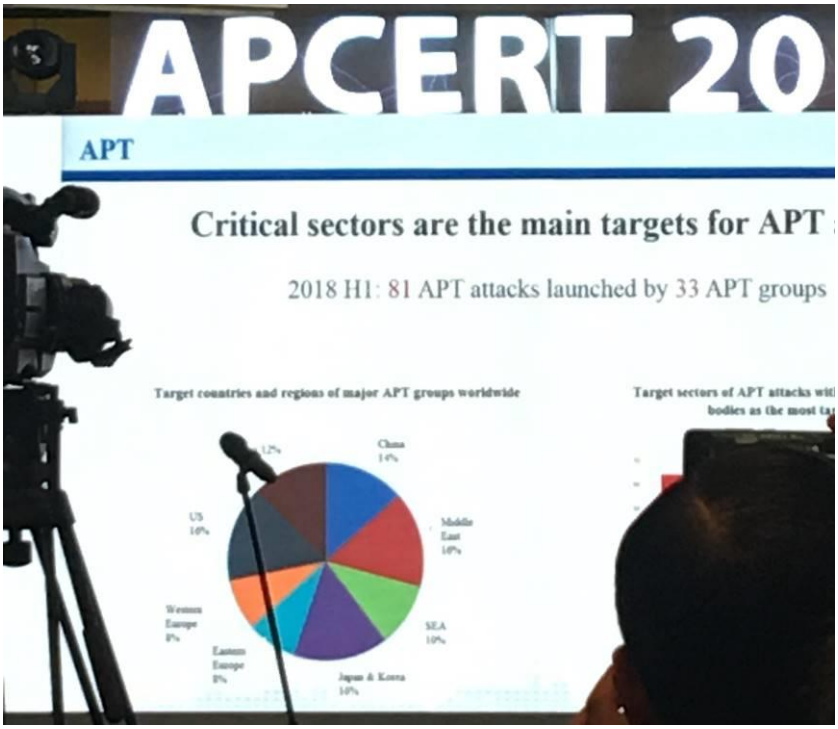


圖三十九：C&C servers in China

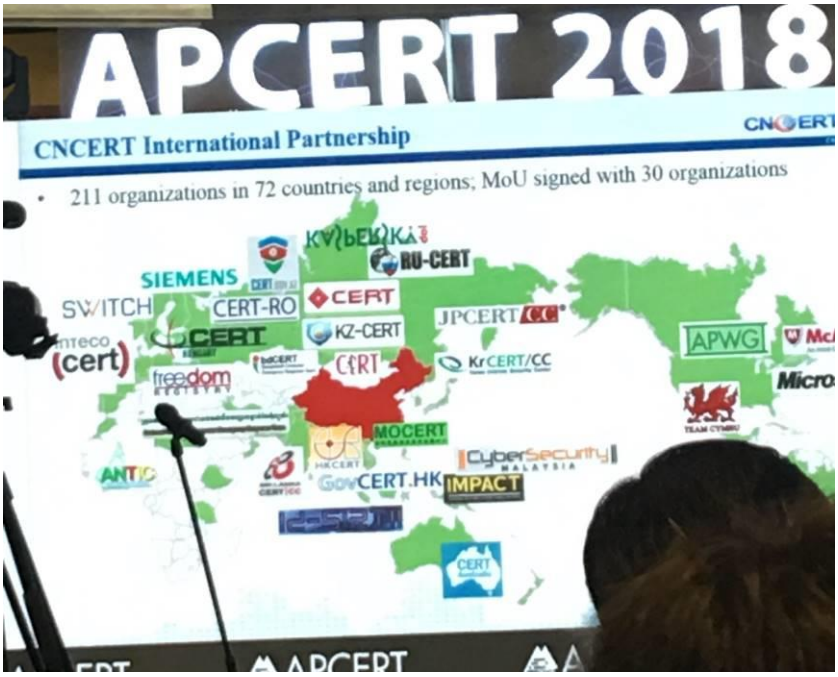


圖四十：mobile malware

圖四十一：DDoS



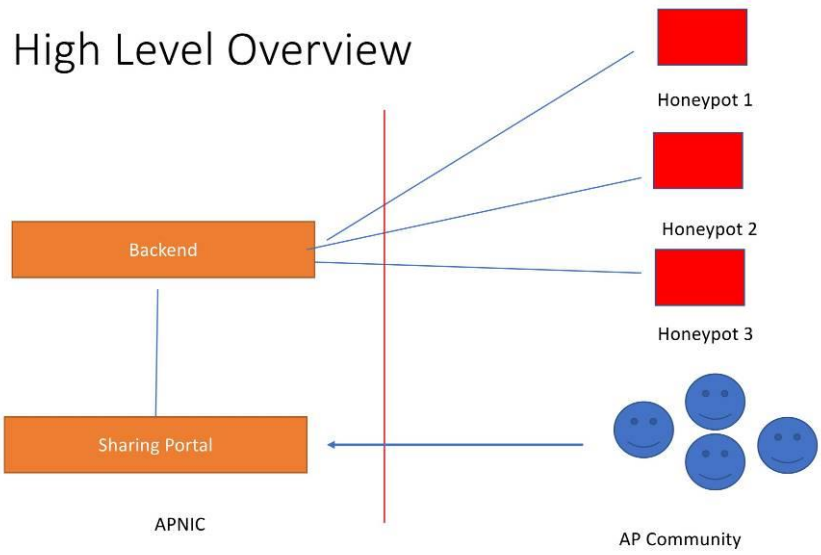
圖四十二：APT attack



圖四十三：CNCERT 國際合作夥伴

6. 2018/10/24：APNIC Community Honeynet Project

由 APNIC Adli 說明 APNIC 在推動的 Honeynet Project，這個 Project 開始於 2015 年，目在在收集 internet 上網路攻擊的真實資料，這個 Project 開放給任何人都可以參與，不一定要是 CERT 的成員，APNIC 提供 Honeypot 相關教育訓練，並提供 pre-installed data 的 VM 可進行部署，加入的成員負責部署和維護 Honeypot，APNIC 則負責維護後端系統，架構如下：



圖四十四：Honeynet High Level Overview

四、 建議意見

茲就本次參加會議之心得，提供結論與建議如下。

1. 加強 TWCERT/CC 在 APCERT 中之參與能量，擴大與國際資通訊安全相關組織之連結。目前，TWCERT 已陸續加入 Malware Mitigation WG、TSUBAME WG 以及 Drill WG，但參與之角色尚未彰顯，本次參加會議後，建議未來能加強以下兩點：

   (1). 將資安事件處理能量透過 Malware Mitigation WG 進行國際分享

   建議增加於中山大學、台灣大學、交通大學及成功大學之佈點，達成完整之誘捕系統建立。如此，不但可以增加國際誘捕系統之能量外，亦可提升台灣於資通訊業界之知名度。

   (2). 與各會員組織進行案例交換

   TWCERT/CC 是國家級 CC 角色，因此需增加在資通訊安全方面之活動參與，尤其於 APCERT 中之 Working Group，除了已加入之三個工作小組外，需增加參與之範圍，加入更多不同之 Working Group，相互交流、學習並進行意見交換，進而做到國際性通報聯防。

2. 關注 APCERT 新型態 WG，帶動國際合作機會

   APCERT 的會員來自亞太地區，針對資訊成熟國家，可互相探討技術合作，針對資訊較不及臺灣國家，透過各式分享與交流機會，建議可進行所內技術推廣，並帶動國內新興資安業者：

   (1). 與較成熟之 Malware Mitigation WG、TSUBAME WG 等探討技術合作

   這次大會中可了解 JPCERT 推動之 TSUBAME 系統，透過自動化方式，發現封包流量異常狀況，提前對遭受攻擊的裝置做預警及事件處理措施；同時 MYCERT 亦分享了從情資到異常分析的系統；TWNCERT/CC 未來可再了解這些系統做法，評估其技術學習、或是合作之可行性。

(2). 了解甫成立的 IoT Security WG、Secure Digital Payment WG 實質內容，評估未來參與方式

目前 IoT 資安領域是國家發展重點，而 IoT Security WG 由印度 CERT 主持，建議需了解這些甫成立的 WG 實質內容，未來也可在此領域中適度分享與交流。

3. 擴大 TWCERT 在國內外社群與廠商的連結力，進行資源交換與整合

CERT 的參與本質為社群連結，目前正在重新檢視並建立 TWCERT/CC 與國際交流之活動，透過本次大會的參與，建議未來 TWCERT 在國內外社群與廠商連結上的作法如下：

(1). 加強與國內相關 CERT 的互動，並擴大與國內外資安社群與廠商的合作

TWCERT/CC 目前與國內 CERT（表 5）的連結可持續擴增並加強，建議可逐步再與國內外資安社群與廠商進行合作，擴大合作範圍，建議可規劃的合作包括：

I. 針對資安事件處置經驗進行分享交流。
II. 合作辦理資安宣導活動、推廣資安意識。

表 5 國內 CERT 盤點如下表

單位簡稱	中文名稱	領域別	主管機關/ 維運單位
TWCERT/CC	臺灣電腦網路危機處理暨協調中心	民間領域/國內各大關鍵資訊基礎建設組織	行政院資通安全處/中科院（108 年起改為 TWNIC）
TWNCERT	國家電腦事件處理中心	國內政府機關	行政院資通安全處/資策會資安所
EC-CERT	電子商務資安服務中心	電子商務	經濟部商業司
NCC-CERT	國家通訊傳播委員會電腦危機處理中心	處理國內網際網路接取服務業者所屬網段的用戶資安事件	國家通訊傳播委員會
TACERT	台灣學術網路危機處理中心	國內學術網路使用單位，資安事件通報、資安教育訓練	教育部/ 中山大學
TWCSIRT	臺灣電腦安全事件應變中心	處理學研網路資訊安全事件、發展前瞻資訊安全技術	國家高速網路與計算中心（國網中心）
DTTW-CSIRT	勤業眾信台灣數位安全事件應變團隊	資安事件應變流程設計、資安威脅預警通報、資安事件調查及演練	勤業眾信台灣
TM-CSIRT	趨勢科技電腦安全事件應變中心	（服務企業會員用戶）	趨勢科技

資料來源：本報告整理

(2). 邀請國外 CERT 或組織來臺，參加 TWCERT/CC 相關計畫活動

TWCERT/CC 目前會固定舉辦台灣資安通報應變年會，亦會視主管機關或合作單位等資源，參與特定主題之活動。未來 TWCERT/CC 可利用這些資源，邀請國外 CERT 或組織來臺，進行意見分享與交換，探討資通訊安全通報之合作以及相關標準運作模式，做為鞏固國外社群連結之方法，帶動更具國際觀點之國內資安通報能量。

五、 其他相關事項或資料

1. APCERT 2018 會議日程表、簡報資料、照片瀏覽

   (1). 會議日程資料與簡報皆可至：http://apcert2018.cert.org.cn/ 下載及瀏覽。

   (2). 大會官方照片：

   https://v.alltuu.com/albumNoMark?id=1011073208&verification=4661dba5ec00703e9326e2fd522584f6.