附件一

臺中市政府公務出國或赴大陸地區報告提要　　類別：其他

出國報告提要名稱：參加「FIRST 2015（第27屆）年會」報告
含附件：☑是 □否

出國計畫主辦機關：臺中市政府資訊中心
聯絡人： 張碧顯　 電話：04-22289111#22301

出國人員姓名/服務機關/單位/職稱
張碧顯/臺中市政府資訊中心/設備網路科/科長

出國類別：其他 ☑國際會議 □業務接洽 □洽展 □表演 □比賽 □擔任裁判
□海外檢測 □_____

出國期間：104年6月13日至104年6月20日	出國地區：德國
報告日期： 104 年 8 月 31 日(填寫一級機關首長核定日)	

內容：(500字以上)

臺中市政府贏得2013年國際智慧會城市首獎(2013 Smart City of Intelligent Community Forum Award, ICF 2013)，未來也將舉辦各式各樣國際活動，參與本次國際年會得以研習計算機和網絡安全、事故管理、內部威脅處理、軟體安全性等等相關知能，課程內容的議題是國際性的，其中包括最新的資安事件反應、預防、弱點分析、計算機安全、管理和政策面的問題，有助於提高對網際網路資訊安全治理的深度了解，並作為本府未來資訊安全策略及計畫規劃參考。

議程自6月13日開始，有兩天的預備會議，包括教育訓練委員會議對於教材的審驗、轉場（指課程場次中間）教練及人員培訓、會議大使培訓、新人及破冰招待會等，15日起，每日除了專題演講是共同的議程外，基本上分為3組平行課程（Tracks)，可由學員自由選擇參與，額外新增的課程其一是現場實作，另一個是參加挑戰賽，本府並不是會員，所有本次行程主要是以參與課程學習為主。

本次參與國際性的資訊安全年會，接收到CERT組織提出對資訊安全的理念， 包括：德國 （主辦國)、歐盟、巴西、日本以及韓國（明年主辦國）等，深感本國近幾年來已經逐漸失去在資訊科技方面的優勢，如吳國維先生點出的，臺灣脫離國際社會太久了，不知道當前國際趨勢、走向、政策，許多臺灣民眾或政府官員並不清楚訂定全球網路規矩是什麼機構，建議國家應更重視國際交流及支持參與國際政策的討論及標準訂定。

鑑於網際網路是一個以開放及自由為宗旨的平台，參與人員多為工程師，習慣理性思考，不易受政治所影響，政府應積極培育公務員或支持非政府組織（NGO）參與國際性活動，藉以提高能見度，進而爭取國際資源分配，又或可提早獲得新科技趨勢，以協助產業界應對、技術及品質提升，增加國際競爭力。

摘　　要

FIRST 年會每年輪流於各大洲的會員國舉辦，今年是第 27 屆，由德國教育及研究電腦緊急應變小組（DFN-CERT）協辦，於 2015 年 6 月 14 至 19 日在德國柏林舉辦，來自 68 國超過 800 個資訊技術專家帶來專業知識與會交流，主要的目的在提升全世界的數位科技及基礎設施的安全性。

本次年會的主題訂為「整合式安全 - 提升未來生活（Unified Security – Improving the Future）」，FIRST 本身即是一個鼓勵開放、協同合作及分享情資以處理資訊安全事件並緊急應變的組織，這幾年來柏林市一直努力改善投資環境吸引外來投資以改變未來，因此我覺得選定這個主題感覺有特別的意涵，會議探討的主題包括歐盟（含德國）的資訊安全組織及策略、網際網路安全指標、公私組織間資安情資通報及交流、IPv6 及物聯網（IoT）資安議題、殭屍網路偵測破解經驗、最新目標式攻擊分析等等，主辦單位另外安排網路攻防及網路資安鑑識實作坊，與會者可隨本身專長及興趣挑選適合之主題。

主辦單位在 14 日舉辦迎新及破冰晚會，由西門子公司贊助，我及趨勢科技林協理孜穗與日本 NTT 荒金陽助、三菱東京 UFJ 銀行北尾辰也、中國中興通訊平立、APNIC Adli 等人進行短暫的交流，了解到我國國際資訊安全的協調聯繫是由台灣電腦網路危機處理暨協調中心（TWCERT/CC）及行政院國家資通安全會報技術服務中心這兩個單位辦理，這個晚會除了心參加人員外，熱情的會員也都來到會場交流，17 日的歡迎晚宴又多認識了香港電腦保安事務協調中心梁兆昌、中國華為公司陸湛等人，也進行了交流，本次日本、中國及韓國各有超過 10 個以上人員與會，顯見它們對國際交流參與的重視程度，也反映本會議是一個國際性的要事，相對來說，我國政府的重視程度及人員參與是不足的。

談到駭客攻擊，少不了中國及北韓的網軍，值得注意的是有一位講者提出網通產品存在漏洞而遭受攻擊入侵的案例中，我國有兩家公司的產品上榜；另外，巴西及歐洲的網路金融詐騙案例眾多，我國的金融檢查一向嚴格，相對上入侵門檻較高，德國、歐盟的資訊安全組織及法令健全，對於個資及隱私保護一向重視，今年德國聯邦政府批准資訊科技安全法案，將藉由此一法案，建構安全的資訊科技系統和最可靠的關鍵基礎設施，提高保護一般人民和公司在網際網路上的資訊安全，並加強聯邦資訊技術安全局和聯邦刑事單位（BKA）的防衛能力，還規定擴展聯邦刑事調查權力，特別是利用資訊科技攻擊

聯邦設施的案件。他山之石，可以攻錯，雖然我國資訊安全相關法令的進程不亞於其他國家，但終究缺乏強有力的資安管理法、專責資訊政策制定機關及執法調查人力，對未來民生社會及產業的發展有必然的影響，現在中央已經將資安管理法草案送立法院審查，希望透過該法的推行帶動政府機關資訊組織的正常發展，國家資訊安全策略也才能落實。

目　　錄

壹、會議介紹

一、有關 FIRST

回溯到 1989 年，發生第一個網際網路蠕蟲病毒，當時所有透過網網路相互連接的網路都受到了衝擊，因此，不僅是一個使用者或組織的電腦或是主機必須關閉處理，隔年成立了「網路危機處理中心（Computer Emergency Response Team, CERT）」。

網路危機處理中心（CERT）是各個國家、組織或企業自行組成的組織，是一個區域性的組織，為了協調各個 CERT 的行動，並加強各 CERT 組織間的合作，於是成立了一個國際性組織 — FIRST（Forum of Incident Response and Security Team）事故應變與安全團隊論壇，以達到下列目標：

- 各成員發展和分享資安技術、工具、方法、程序和最佳做法的資訊
- 鼓勵和促進發展優質的資安產品、政策和服務
- 發展和揭示電腦安全性的最佳做法
- 促進來自世界各地的組織建立和擴大的事件回應團隊和會員
- 所有成員運用自己的綜合知識、技能和經驗來促進一個更舒適、安全的全球電子環境。

也就是說 FIRST 希望幫助其成員一起分享所擁有的資訊並且處理其共同的問題，甚至訂定未來的策略及計畫，對於事故應變與安全團隊來說，關於互相關心議題的資訊交換和合作是很明確的關鍵問題，比如：新的漏洞問題或廣泛的攻擊 — 特別是核心系統，像 DNS 伺服器、網際網路本身這樣重要的基礎設施。

自 1990 年，當 FIRST 成立以來，其成員已經解決幾乎連續的與安全相關的攻擊串流，包括不斷增長且透過網際網路連接世界各地數以百萬計的電腦系統和網路的安全性漏洞。

FIRST 彙集了種類繁多的安全和事件回應小組，其中特別是包括來自政府、商業和學術部門的資訊安全團隊，會員是自願性的，通常是地區性的網路危機處理中心（CERT），台灣現有 4 個 FIRST 會員，分別是台灣電腦網路危機處理暨協調中心

（Taiwan Computer Emergency Response Team and Coordination Center, TWCERT/CC，委託中山科學研究院代管）、國家電腦緊急應變小組（Taiwan National Computer Emergency Response Team, TWNCERT，行政院國家資通安全會報技術服務中心委託財團法人資訊工業策進會代管）、台灣資安事件處理小組（TaiWan Computer Security Incident Response Team, TWCSIRT，國家高速網路與計算中心自行申請成立）及趨勢科技資安事件處理小組（TrendMicro Security Incident Response Team, TM-CSIRT，趨勢科技公司自行申請成立）。

FIRST 年會由 FIRST 組織所主辦，並由一個地方區域團隊的支援，專注於資安事件應變小組的議題，並彙集了世界各地資安專家，分享他們的經驗和專門知識，至今已成為資訊安全領域的年度盛事。

二、會議名稱

FIRST 2015 年會（ FIRST Conference 2015）

三、會議時間

2015 年 6 月 13 至 2015 年 6 月 19 日

四、會議地點

德國柏林洲際酒店（InterContinental Berlin）

五、會議相關文件

會議相關資料請詳見網站（https://www.first.org/conference/2015）

貳、參與目的

自資訊科技運用以來，除了發展各式各樣的應用外，另一個破壞性的面向也相應而生，例如：個人電腦的病毒、惡意軟體等等，造成系統及資料的毀損；到了網際網路時代，更有網路蠕蟲、木馬程式等入侵到機關組織內部造成破壞或是竊取商業資訊，影響正常的商業運作，近年各機關組織均積極規劃防毒系統、網路監控及防禦設備等，導入資訊安全管理系統（ISMS）作為制度及作業標準，但是，資訊安全事件仍然層出不窮。回溯 25 年前，Robert T. Morris 在麻省理工學院施放第一支網際網路蠕蟲（Morris worm），由於該程式會利用 Unix 系統的漏洞，不斷複製自己，並入侵連網的主機，造成數千台主機當機，整個網際網路基礎設施受到威脅，最後在電腦專家努力下獲得解決，但是這個事件所帶給大家的震撼也是空前的，人們終於體認到，由於系統過於龐大複雜，單憑一己之力是無法完全發現隱藏在其中的漏洞。更重要的是，對於此類事件的處理，若非所有人齊心協力是無法完成的。也因此，促成了網路危機處理中心（CERT）的誕生。

網路危機處理中心（CERT）初期成立的目的，是希望能夠順利的處理危害網路安全的相關事件，保護網際網路設施，以提高電腦系統的安全性，進而預防未來可能的電腦安全事件的發生。由於資安事件是全球性的，為了加強各網路危機處理中心（CERT）組織間的合作，於是成立了一個國際性組織 — FIRST（Forum of Incident Response and Security Team）事故應變與安全團隊論壇，並且每年定期舉辦研討會。

臺中市政府贏得 2013 年國際智慧會城市首獎（2013 Smart City of Intelligent Community Forum Award, ICF 2013），未來也將舉辦各式各樣國際活動，參與本次國際年會得以研習計算機和網絡安全、事故管理、內部威脅處理、軟體安全性等等相關知能，課程內容的議題是國際性的，其中包括最新的資安事件反應、預防、弱點分析、計算機安全、管理和政策面的問題，有助於提高對網際網路資訊安全治理的深度了解，並作為本府未來資訊安全策略及計畫規劃參考。

參、會議過程

議程自 6 月 13 日開始，有兩天的預備會議，包括教育訓練委員會議對於教材的審驗、轉場（指課程場次中間）教練及人員培訓、會議大使培訓、新人及破冰招待會等，15 日起，每日除了專題演講是共同的議程外，基本上分為 3 組平行課程（Tracks），可由學員自由選擇參與，額外新增的課程其一是現場實作，另一個是參加挑戰賽，本次行程主要是以參與課程學習為主，以下就每日專題演講、攻擊案例分析、防禦與監測方案、網路安全指標及策略等主題進行摘要報告：

（一）專題演講（Keynote）

專題演講是所有會議的精隨，會議主辦單位基於策略、組織、安全技術、國際社群、戰略戰術等面向，精心安排 5 場專題發表（Keynote Presentation），首場專題係由地主國，德國國務秘書暨聯邦政府內政部資訊處長科妮莉亞・羅加爾－格羅特（ Cornelia Rogall-Grothe）擔任主講者，題目為「資訊安全：政府、產業及社會未來的挑戰」（IT Security: Future Challenges for Government, Industry and Society），作為整個年會的開場。

Keynote Presentation:
IT Security: Future Challenges for Government, Industry and Society - Potsdam I
Cornelia ROGALL-GROTHE （German State Secretary & Federal Government Commissioner for Information Technology）

由於資安情勢的變化，面對網路攻擊事件，最需要的是協同合作，例如 FIRST 會員基於互相信任，進行資安情資交換，此時，最重要的反而不是技術，而是學習相信對方，推而廣之，政府與政府間應該要信任，政府與民間也要信任，不能只是要求政府做好事情，政府與民間應該是合作夥伴關係，智慧型動裝置的普及造成資安防護更加複雜，手機內存有個人資料，包括交友情形，甚至是銀行資料，可以說是壞人的金礦，物聯網（Internet of Things, IoT）已逐漸盛行，穿戴式智慧裝置存有弱點風險高，網際網路公司蒐集儲存這些個人資料，無形中又提被攻擊的風險，人們越來越倚賴新的技術，面對網

際威脅則希望政府能夠保護且提供安全穩定又可以自由使用的網際網路環境，德國聯邦政府通過 20104-2017 數位議程（Digital Agenda），下個月資訊科技安全法案 （IT-Security Act）即將生效，將要求關鍵基礎設施的資訊安全必須滿足最低標準，這是第一步，德國聯邦資訊安全辦公室（German Federal Office for Information Security, BSI）接著會協同網際網路業者訂定資訊科技安全標準，德國將藉由此一法案，大幅提升資訊科技系統安全與關鍵基礎設施可靠度，網際網路是全球公用資產，所有使用者均希望在其中進行安全和有保障的活動；確保網路安全、執行權利和保護重要資訊基礎設施需要大家共同合作及努力付出，賦予國家、產業和社會共同責任，只有在所有角色做為合作夥伴並共同完成任務情形下，網路安全戰略才得以成功，這樣的道理同樣適用於國際間的網路安全議題上。

Keynote Presentation:
Securing our Future - Potsdam I
Mikko HYPPONEN （F-Secure）

主講者：芬安全（F-Secure）首席研發長米可・施伯能（Mikko HYPPONEN）先生，題目為「保全我們的未來」（Securing our Future），強調電腦安全議題已經從病毒升級為電腦犯罪及個人隱私洩漏的問題，在龐大的網路犯罪利益吸引下，許多駭客透過攻擊系統賺錢；另外，許多的網路服務公司，透過販售個人「隱私」的方式以賺取該公司的利益，因此現行網際網路存在以下兩大問題：

(一)駭客工具自動化：

目前駭客已經發展出電腦自動化入侵及側錄程式工具，並在網路販售，讓一些不具專業人士也可以輕易地運用以駭入別人的電腦，這些變形及加密的駭客程式已經無法使用一般的防毒程式及防火牆等資安工具予以清除或是阻擋，近來勒索軟體橫行，就是一個實證；發展物聯網（Internet of Things）的趨勢已定，智慧裝置已經是潮流，所謂智慧裝置就是可以連上網路，也代表可以被入侵，智慧電視、智慧手錶、甚至是智慧微波爐等都可以連上網路，想像智慧微

波爐被入侵調至高溫甚至爆炸的情景，未來的人身安全堪憂，更有駭客已經證明智慧汽車、連飛機上的控制系統也能入侵，這些都是潛在的威脅。

(二)個人隱私遭販售：

大型網路服務公司，像是 Google 或是臉書等社群媒體，則透過販賣個人的特徵資料以獲取利益，舉例，以 Google 過去 2012 年～2014 年每一季花在機房的費用約是 10 億美元到 20 多億美元不等，而獲利來源，就是當你使用這些免費服務的同時，同時也賣掉你的數位隱私去幫 Google 賺錢，而購買的公司則透過你的行動電話，將你的性別、職業、性趣，甚至是家人的資料透過你的行動電話號碼一點一點拼湊出全貌，作為廣告推播的對象。

「天下沒有白吃的午餐」，目前有許多「免費」的網路服務背後是有一定的代價，不要輕易賣掉自己的數位隱私，做好個人的資料備份，以確保在數位時代的安全。

Keynote Presentation:
Europol's European Cybercrime Centre – punching above its weight - Potsdam I
Philipp AMANN （European Cybercrime Centre, Europol）

主講者：歐洲刑警組織（Europol）的歐洲網路犯罪中心（European Cybercrime Centre）高級戰略分析師菲利普・亞曼（Philipp AMANN）先生，題目為「歐洲刑警組織的歐洲網路犯罪中心 — 以小博大」（Europol's European Cybercrime Centre – punching above its weight）。

歐洲網路犯罪中心（European Cybercrime Centre，簡稱 EC3）自 2013 年 1 月 1 日開始運作，於 11 日在荷蘭海牙正式掛牌宣告成立，為歐洲刑警組織的一個單位，與其他犯罪領域協同工作，將彙集專門知識和資訊，支援刑事調查和推動歐盟範圍內的解決方案，以保護歐洲民眾和公司不受網路犯罪的危害。

歐洲網路犯罪中心被交辦專注於以下三個領域：

- 組織型網路犯罪，尤其是像線上欺詐等，可產生大量犯罪利益者等。

- 對受害者造成嚴重傷害的網路犯罪，諸如線上兒童性剝削。
- 影響在歐盟關鍵基礎設施和資訊系統的網路犯罪 （包括網路攻擊）。

關於以上這三個領域，歐洲網路犯罪中心（EC3）的工作為：

- 作為網路犯罪資訊和情報的中央樞紐
- 通過作業分析、協調和專門知識支援會員國（Member States, 簡稱 MS）的行動和調查
- 提供了各式各樣的策略分析成果，促使戰術和戰略層級做出正確的決策，來打擊和防止網路犯罪的發生
- 建立全面的外聯功能（outreach function）以連接與網路犯罪相關的執法部門與私部門、學術界，以及其他非執法夥伴
- 支援專門知識的培訓和能力的建立，特別是各成員國主管當局
- 對調查作業提供高度專業化的技術和數位鑑識支援能力
- 協助歐盟執法機構之研發要求、網際網路治理和政策發展等推動

歐洲網路犯罪中心 2013 年的預算約為 700 萬歐元（占歐洲刑警組織總預算的 10%），初期工作人員為 30 至 40 人，2015 年目前約有 70 人，人數及經費雖少，卻能有效打擊犯罪，正所謂「以小博大」。

Keynote Presentation:
Collaborative Security - Reflections about Security and the Open Internet - Potsdam I
Olaf KOLKMAN （Internet Society）

主講者：國際網路協會（ Internet Society, 簡稱 ISOC） 的首席網際網路技術長（ Chief Internet Technology Officer ） 歐拉夫・科克曼（Olaf KOLKMAN）先生，題目為「協同合作式的安全--安全和開放的網際網路之反思」（Collaborative Security - Reflections about Security and the Open Internet ）。

開放的網際網路已經證明是促成社會、技術和經濟相互作用的強大驅動力，網際網路的成功基於若干的不變因子，諸如：全球的連通性和完整性、無障礙、自我創新、互通性和共同協議。這些特質不僅帶來繁榮，遭受攻擊情形也日益增加。

當網際網路的安全問題達到全球規模時，一般維護安全的方法已經不能適用；因為一般維護安全的做法通常先面對內部:由參與者檢視本身的資產，以及用最經濟的方式保護他們。

傳統維護安全的方法是以外部和內部的威脅，以及它們對於資產所造成的衝擊為主要考量，換句話說，是基於威脅和自身的利害關係；然而，越來越多人認知到網際網路生態系統的安全模式應基於保護經濟和社會的繁榮為前提，而不是基於簡單的防止傷害模式。網際網路，以其高度互連性和依存性，帶來了另一個層面的風險管理，網際網路的安全性和復原能力並不僅取決於你和你的資產風險管理的程度，而且，重要的是你面對網際網路生態系統風險 — “外在”風險 — 的管理。此外，某些風險是必需多個參與者進行管理，例如：跨國網路犯罪、分散式阻斷服務（DDoS）攻擊等。

這就是集體和共同風險管理的概念 — 與網際網路的“公共利益”概念性質完全一致，也就是「協同合作式的安全」。

協同合作式安全歸結有五個關鍵要素：

1．促進信任和保護商機（Fostering confidence and protecting opportunities）：維護安全的目標是促進對網際網路的信任，並確保網際網路持續成功的作為經濟和社會的創新驅動力。

2．集體責任（Collective Responsibility）：參與者共同分攤網際網路朝向系統完整性的責任。

3．基本特性和價值（Fundamental Properties and Values）：資訊安全解決方案應符合基本人權和維護網際網路的基本特性 — 先前所述的網際網路的不變因子。

4．發展和共識（Evolution and Consensus）：有效的安全倚賴一組廣泛的利害關係者的專門知識所建立的發展步驟。

5．放眼全球，立足本地（Think Globally, act Locally）：它最有可能通過由下而上的自願者組織達成之最有力量的解決方案。

協同合作式安全在標準化作業的活動中可以看到一些實例，諸如：資訊標準架構促進會

結構化資訊標準推廣組織（Organization Advancement Structured Information Standards，簡稱 OASIS）努力制定結構化威脅資訊表示法（Structured Threat Information Expression，簡稱 STIX）供資訊指標信任式自動化交換機制（Trusted Automated Exchange of Indicator Information，簡稱 TAXII） 作為網路威脅情報系統的標準交換格式，另外，網際網路工程任務小組（Internet Engineering Task Force，簡稱 IETF） 先期小組討論制定有關分散式阻斷服務攻擊的方法等等。

Keynote Presentation:
The cybercrime techniques, tactics and procedures（TTP）have evolved towards the mobile apps world - Potsdam I
Mr. Chema ALONSO （Telefonica/Eleven Paths）

主講者：Eleven Paths（一個西班牙電信公司）的執行長（Chief Executive Officer）切瑪・阿隆索（Chema Alonso）先生，他同時也是西班牙馬德里大學（Universidad Europea de Madrid，UEM）資訊安全學院院長和加泰羅尼亞大學（Universidad Oberta de Catalunya，UOC）資訊安全教授，題目為「網路犯罪的攻擊戰術流程（TTP）已經在行動應用程式的世界實現」（The cybercrime techniques, tactics and procedures（TTP）have evolved towards the mobile apps world）。

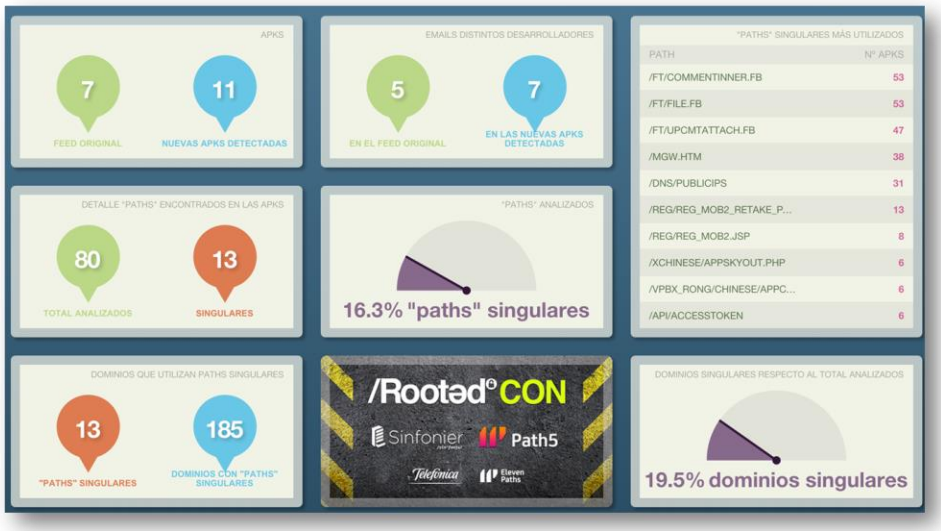
考量在 Google Play 商店中與日俱增的上架申請（2015 年 6 月約 26 萬個新版應用程式），以及容許開發者能以簡單而快速的方式上傳他們的應用程式，對於惡意程式碼檢測只能以一種自動化的方式來執行。這種型態的稽核作法被網路犯罪份子利用來輕鬆跳過保護，並迅速的發布他們的惡意程式。

切瑪・阿隆索在本次演講中展示網路犯罪的攻擊戰術，網路犯罪份子運用許多蒙蔽人心手法，例如：使用與知名的社群軟體（WhatsApp）非常相似名稱、假冒的免費防毒程式或宣稱具有 X 射線透視能力的軟體等等，因為大多數人希望使免費軟體，又“苛求”的

希望防毒軟體沒有誤報，並保護他們免受各種威脅；網路犯罪份子建構殭屍網路與運用被捕獲的用戶，賦予前述應用程式正面評級，甚至創造了有利的評論，都是為了讓更多用戶的信任這些偽冒應用程式，以提高下載安裝的比率。

切瑪・阿隆索的研究團隊在 2013 年發現來自中國山東省的攻擊團隊，以製造假的 WhatsApp 程式當作誘餌的攻擊模式，如同前述，這些程式名稱非常相近，圖示也近乎相同，這些假的應用程式檔案容量比較小，因為不含廣告軟體的識別代碼，也不至於要求太多權限，不會被任何防毒軟體偵測並警示，這些程式不具有應有的功能，主要是用來發送入侵廣告，吸引使用者點閱，這些人安裝了前述的山寨應用程式，就形成了「刷版殭屍網路（ShuaBang Botnet）」。

切瑪・阿隆索現場透過該公司研發的行動裝置資訊安全事件調查系統【Tacyt （音：塔西透）和 Sinfonier （音：辛馮莉亞)】展示資安分析的應用過程，Tacyt 計畫是以建造一個公開來源情報（Open Source Intelligence, OSINT）平台，並蒐集包括 Google Play 商店及其他 Android 應用程式商店所有與應用程式相關資料的大數據，提供資訊安全分析師一個即時線上處理工具，並可以與其他資安工具建立連結，Sinfonier 計劃是一個視覺化編輯系統，用以操作大數據平台數據資料以產生有用的知識，該公司已經將這些工具發現的刷版殭屍網路（Shuabang Botnet）、JSDailer 騙局等研究成果送交歐洲警方、防毒業者及行動安全廠商，以建置檢測機制，這些研發成果有助於提升行動安全及建造更完整的資安生態系統。



圖一： 結合 Sinfonier 及 Tacyt（Path 5）所建立的資安數位儀表板

（二）攻擊案例分析

Kraken BOT（克拉肯殭屍）是一個完全商業化的遠端系統管理工具，通過幾個犯罪集中地下論壇散播，儘管標準包的價格低（約 270 美元），其附加越來越多的功能持續開發建置中。基於這些原因，KrakenBOT 正慢慢成為廉價的和非常有效的惡意軟體工具套件，同時是許多犯罪集團的最佳選擇。

Kraken 殭屍的控制面板及建造器已於今年 3 月被發布在 TrojanForge 論壇，所以，現在 Kraken 已經是不用錢的犯罪工具。專家進行軟體技術解析發現 Kraken 殭屍具有下列功能：

1. 容易執行任務
2. 竊取遊戲寶物
3. 具有比特幣外掛
4. 谷歌瀏覽器帳密蒐集器
5. FTP 帳號密碼竊取
6. 繞過使用者存取控制（User Account Control, UAC）
7. 檢查執行環境是否存在虛擬主機、網路封包（Wireshark）側錄及網站除錯工具（Fiddler）等，用來躲避偵防作業
8. 反病毒程式偵測
9. 反沙箱
10. 與控制主機（command and control, C&C）採加密式通信協定
11. 收集剪貼簿內容
12. 防暴力破解之控制面板

這隻精心設計的殭屍程式自動避開防毒程式的偵測，所有與控制主機的連線都採取加密模式，使用位於世界不同地區的命令控制（C&C）主機，而不是點對點來控制殭屍，每台被感染的電腦都有一個命令控制主機清單，如果目前的命令控制主機被阻擋了，殭

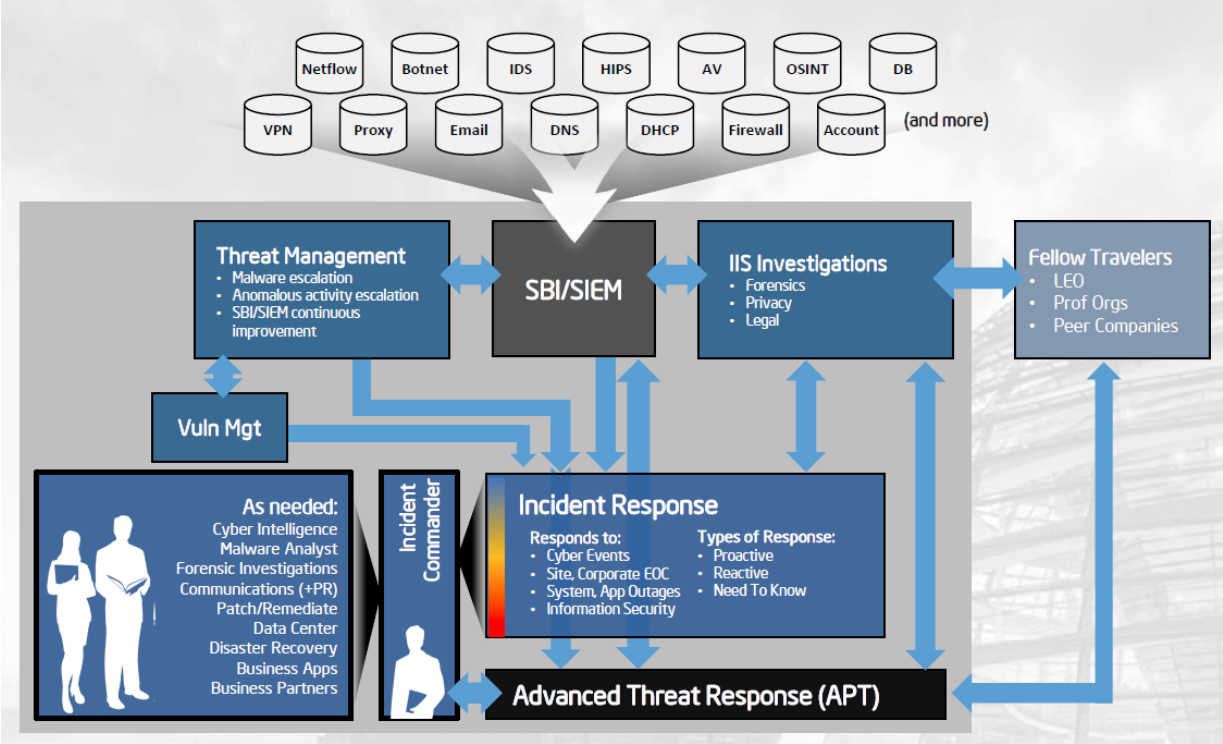
屍電腦會向清單中的下一部控制器報到，這樣的作法造成防火牆及入侵偵測設備難以發現及阻擋，加密連線連網路封包監測都非常困難，具有以上的特性，根據報導已經每天受感染電腦超過 400,000 台，迄今為止存在的最大和最臭名昭著的僵屍網路。

今（2015）年初發現了一款入侵能源組織竊取機密的木馬 Laziok，主要攻擊目標為阿拉伯聯合大公國、 沙烏地阿拉伯、 巴基斯坦和卡塔爾，根據演講者的歸納，Laziok 透過社交工程手法攻擊，利用 EXCEL 存在“Common Controls ActiveX”（CVE-2012-015）這項漏洞入侵，入侵後便嵌入 Kraken 殭屍程式，Kraken 及 Laziok 都會將本身複製到 %APPDATA%\System\Oracle 這個目錄，HTTP 的讀取指令和網路資料流兩者相同，也都用“Dark EYE V3” 加密，根據這些證據，講者推斷認為兩款程式作者應為同一人，這個研究甚至指出就是蘇聯的某一名駭客。

（三）防禦與監測方案

2009 年 12 月可能來自中國的一場網路攻擊 — 極光行動 Operation Aurora — 如同敲響英特爾（Intel Corp.）公司的警鐘，提醒公司必須注意、整備及研究如何對應駭客攻擊，經過檢視，首先公司存在人員、程序及工具的問題如下：

- 新團隊不知道某些資料的擁有者
- 資料的可存取及可用性
- 地理位置的挑戰
- 缺乏即時監控
- 持續應變的挑戰
- 日常工作沒有消失
- 如果再發生進階持續性攻擊（APT）事件？



圖二： 英特爾公司事件應變系統架構

在個去幾年中，英特爾公司建立自己的資料倉儲、分析和安全業務情報（Security Business Intelligence, SBI） 能力。首先，透過“六大”事件來源資料收集，可以查閱何時以及發生了什麼問題。這些事件資料來源是電子郵件頭（SMTP headers）、網頁代理（web proxies）、活動目錄（Active Directory）、動態主機設定協定（DHCP）、虛擬私人網路（VPN）和網域名稱系統（DNS）。投資技術解決方案，使其能夠保有在相對較長的時間內大量的資料，並能以極快的速度來查詢這些檔案，減少 95%的事件回報時間。

另外，印尼成立了網際網路基礎設施安全事件應變小組/協調中心（Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center, ID-SIRTII）目地是為印尼打造一個安全、舒適及有利的上網環境，並主動管理國家網際網路空間風險，以提高國家網際空間安全狀態，印尼國內有 40 個網路接取提供者（Network Access Providers），300 個網際網路服務提供者（Internet Service Providers），7 千 5 百萬個網際網路使用者，12 家電信公司 11 萬座 3G/4G 基地台，2 千 3 百萬家資通訊公司，考量網路安全需求是一個對連續改變的處理程序應變作業，其不僅自行研發的進階網路監視系統—鷹眼，並規劃一組 S.L.A.D （See-Learn-Adapt-Decide） 程序：

- 看見（See） — 將所有網路資訊集中在一處，以利仔細觀察
- 學習（Learn） — 透過智慧引擎洞悉本地網路通訊特性
- 調適（Adapt） — 改變是常態，因此運用開放式架構
- 決策（Decide） — 降低錯誤雜訊，已做出更好的決策

其中學習程序內的智慧偵測引擎是採用支持向量機（Support Vector Machine, SVM）的人工智慧技術（Machine Learning），支持向量機已經被證明是最佳的分類方法之一，經使用美國國防部高級研究計劃局（Defense Advanced Research Projects Agency, DARPA） 的數據進行量測，通過使用 8 個特徵值（features）來進行辨識，可以達到 99%的檢出率。雖然國外有許多的入侵偵測（Intrusion detection system, IDS）產品，該單位通過自行研發，更可以了解入侵偵測系統的關鍵技術，並激勵印尼本地人投入研究和開發自己的產品，這個研究成果（鷹眼系統）已經應用在印尼的網際網路活動的監測上，除了顯示發生事故外，還能辨識事件類別，並整合地理資訊系統產生視覺化的攻擊圖表。

圖三： 鷹眼所產生的全球攻擊視圖

（四）網路安全指標及策略

Cyber Green 計畫為尤里・伊藤（Yurie ITO, Asia Pacific Computer Emergency Response

Team, APCERT 主席） 所提出計畫，參考全球性衛生組織控制疾病和預防的方法，例如：限制傳染性疾病傳播、資訊共享和應對疫情，以及免疫接種、教育、環境衛生宣傳等預防措施和關鍵指標和醫學標準的發展。這些組織，經由整合及協調在地方、州、國家和國際等各級別之資源及一致性的作法，發揮了複雜的跨國挑戰防治中心的角色，一直非常成功改善全球公共衛生條件。

同樣，倡議在網際空間專注全球性的預防和整治，具有潛力彙集先前雜亂無章的做法，以確保網路生態系統，並發展網際健康（Cyber Health）共同規範。目前，公共部門和私營部門所面臨的許多網路風險是由“不健康”的網路生態系統造的症狀，諸如：僵屍網路的流行和蔓延，有增無減的惡意軟體。建立協作和一致的共同做法，有助於解決網路風險系統性根本原因，而不是僅僅減輕其症狀，亦將深遠影響打造安全與彈性全球網路生態系統的信心。

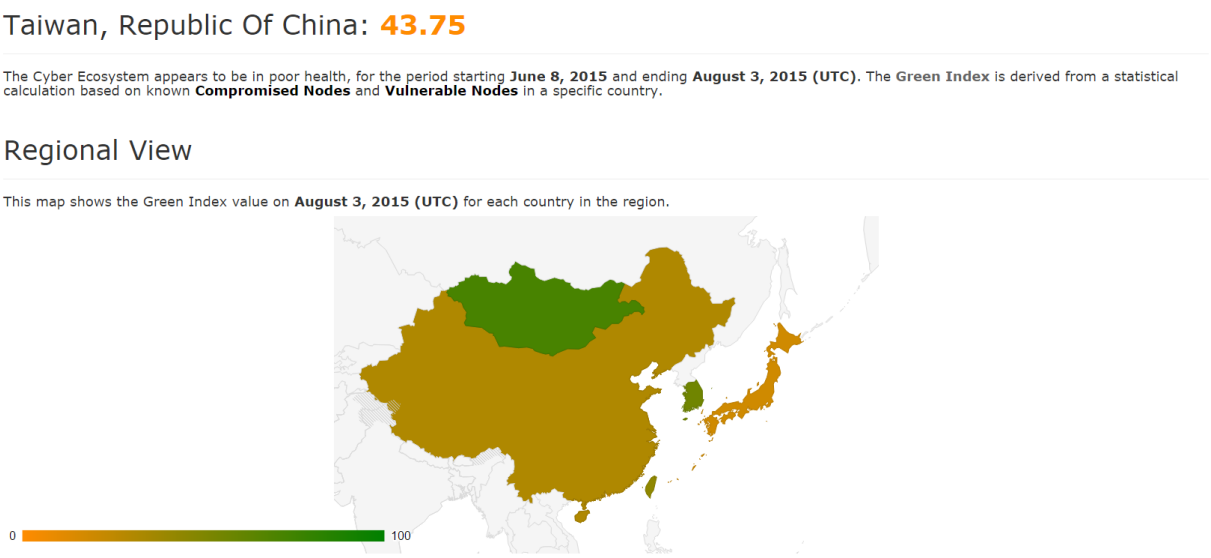
網絡健康（Cyber health）的定義是“經由限制惡意軟體感染，系統漏洞和惡意網路流量，提供所有人可信任和可用性的一個網際生態系統。”經由根因分析，訂出以下網際網路健康風險指標：

- 已知受到攻擊的主機數量：
    1. 殭屍網絡感染主機
    2. 被用於網絡釣魚主機...等
- 已知易受攻擊的主機數
    1. 特定漏洞的客戶端／服務器端主機
    2. 開放 NTP 主機，開放遞歸解析域名主機，...等
- 已知“不請自來”的主機數
    1. 垃圾郵件，DDoS 攻擊，攻擊，掃描器..... 等
    2. 確認發生事件或容量（包括網路及硬碟空間等）被浪費的主機

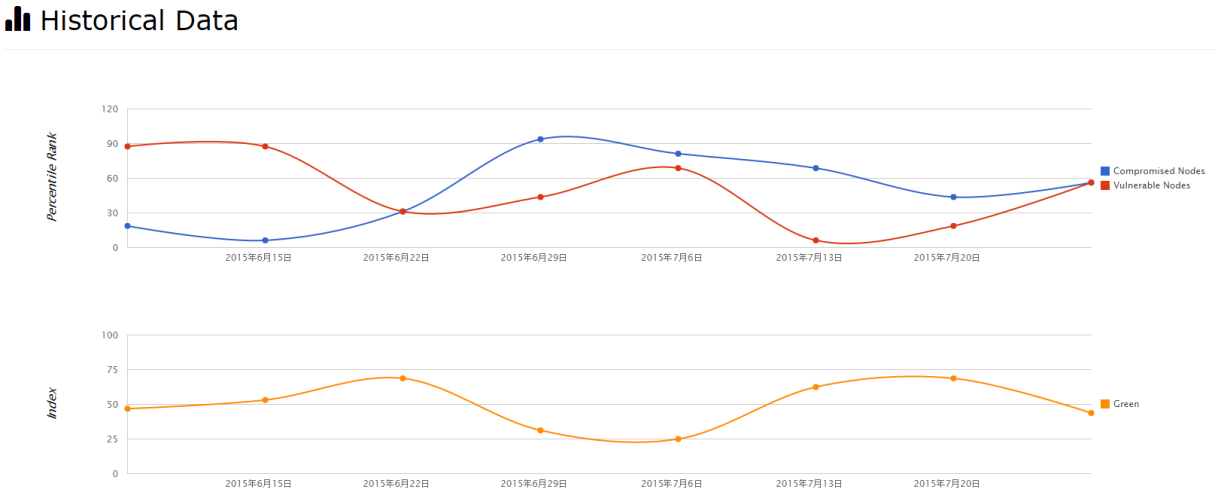
目標是以上指標趨近於“零”，並開發支援各組織之網路安全資料整合工具，將收集到的資料來源分享至 Cyber Green 平台，透過此平台作資料來源統計與分析，並提供網站介面作為資料與安全指標共享平台，建立網路安全指標以表示資安現況，供決策者參考以掌握資安發展趨勢，並持續改善網路環境。

目前 Cyber Green 系統已完成系統建置，已公開計算網路健康狀況之演算法，並邀

請各國加入該計畫提供網路危機處理中心（CERT）的事件通報資料，讓這個專案更具有全球性的指標。以下是 104 年 8 月中華民國某一天的網際綠色指標及歷史資料，因為中學生反課綱事件，引發國際匿名者駭客社群攻擊，資安指標有稍微下降的情形。



圖四： Cyber Green 所產生的亞洲網際網路健康圖



圖五： Cyber Green 所產生之台灣網際網路安全指標歷史曲線圖

肆、心得及建議

本次參與國際性的資訊安全年會，接收到 CERT 組織提出對資訊安全的理念， 包括：德國 （主辦國）、歐盟、巴西、日本以及韓國（明年主辦國）等，深感本國近幾年來已經逐漸失去在資訊科技方面的優勢，在國家策略、法規制度、組織人力、大型活動資安配套等相關面向，應該有努力的空間。

（一）國家策略面：

如同德國聯邦政府內政部資訊處長科妮莉亞・羅加爾－格羅特所表達的，資訊安全是政府、產業和社會將面臨的重要挑戰，如何加強公私部門之間的網路安全合作，並擴及國際間在網際網路議題上的合作都是我國首要的工作，黃勝雄博士在「從 ICANN 多元利益關係人（Multistakeholders）之架構談未來網路治理」一文中指出，2013 年發生的史諾登（Snowden）與美國監聽洩密案，在各國強烈抗議與要求之下，2014 年 3 月 14 日美國國家電信資訊管理局 NTIA 宣布將釋出網際網路號碼分配局（IANA）監管權，將全球網址和 IP 資源分配主導權移交給全球多元利益關係人社群經營（Multistakeholders Community），釋出 IANA 監管權是國際網路政策的一個大改變；同年 7 月 17 至 18 日，美國移交全球網路監管權工作的第一次會議在倫敦召開，我國 National Information Infrastructure, NII 產業發展協進會執行長吳國維先生也獲指派為監管權移交小組的成員之一，不過，吳國維先生也點出，臺灣脫離國際社會太久了，不知道當前國際趨勢、走向、政策，許多臺灣民眾或政府官員並不清楚訂定全球網路規矩是什麼機構，建議國家應更重視國際交流及支持參與國際政策的討論及標準訂定。

其二，今（2015）年 4 月 1 日美國總統歐巴馬（Barack Obama）簽署反制網路攻擊活動之行政命令，授權美國財政部長、司法部長與國務卿 3 人，在面對美國遭受有關國家安全、外交政策與經濟穩定的網路攻擊危害時，有權對發動網路攻擊的駭客進行制裁，並提到目前網路攻擊已經成為美國面臨最嚴重的經濟或國家安全挑戰之一，甚至是一種「國家緊急狀態」，另外，中國也在同（2015）年 7 月 1 日通過「國家安全法」，除將台灣納入中國用以矮化台灣以外，也可以用來要求中國製造的網路通訊產品加入後門；2015

年 6 月本府資訊中心在執行資安監控作業就發現有兩件中國製造的資通產品會自動連線到中國的資安事件，駭客橫行，網路安全已經提升到國家戰略層級，雖然國家安全局「網域安全處」5 月掛牌運作，但是，何時能宣告本國的網際網路主權呢？

鑑於網際網路是一個以開放及自由為宗旨的平台，參與人員多為工程師，習慣理性思考，不易受政治所影響，政府應積極培育公務員或支持非政府組織（NGO）參與國際性活動，藉以提高能見度，進而爭取國際資源分配，又或可提早獲得新科技趨勢，以協助產業界應對、技術及品質提升，增加國際競爭力。

（二）法規制度及資安人力面：

網路犯罪公約是全球第一部針對網路行為規範之國際條約，2001 年 11 月 23 日由歐洲理事會 26 個會員國與 4 個非會員國（美國、加拿大、日本及南非） 於布達佩斯正式簽署通過，歐盟於 2002 年提出「電腦與網路濫用法制建議手冊」，2002 年 12 月布希總統簽署「電子化政府法案」（E-Government Act of 2002），並通過聯邦資訊安全管理法（Federal Information Security Management Act of 2002，FISMA），而我國則於 2001 年成立國家資通安全會報，同年通過資訊公開法，2002 年通過電子簽章法，2003 年增修刑法第 36 章妨害電腦使用罪，劉建良先生在「資安法規面面觀」一文中彙整我國資通安全相關之法律規範，可劃分為網路犯罪、身分認證、通訊保障、資料保護、資訊公開與機密維護及資安治理等六類，其所涉及之法律規範則包含刑法、電子簽章法、電信法、通訊保障及監察法等二十項，我國的法制作業期程並不亞於其他先進國家，然而，除政府機關被要求加強資訊安全作業以外，似乎未見民間企業有相對應的具體作法，iThome 2013 年 10 月「個資法將滿周年 產業因應情況仍紛亂不齊」曾訪問多位學者專家歸納原因有：業者的業務性質橫跨多個主管機關、行業難以認定、沒有專責機構、宣導不足、配套措施不完善以及人力與資源不足的情形，所以，多位專家皆建議，臺灣應該盡快成立個資專責機構，可以借鏡像是香港的個人資料私隱專員公署、德國聯邦資料保護與資訊自由委員會等作法。

檢視各國資訊安全機構設置情形，德國聯邦內政部下設聯邦資訊安全辦公室（BSI），後來成為資訊安全局，韓國科技資訊未來部下設資訊安全局（KISA），新加坡通訊及新聞

部下設資通訊發展管理局（IDA），中國工業和信息化部下設信息安全協調司，我國則於2015 年指定科技部為資通安全主管機關，針對這樣的情形，我不禁聯想到「政府機關共通性資服採購模式之研究」內提到「各部會目前由副首長兼任資訊長，似形同虛設。資訊長功能除協助部會整體規劃如何運用資通訊技術，提升政府效率，替人民與企業服務外，同時也帶領規劃、管理與執行政府資訊專案，並負責 IT 標準、政策、準則及流程，通訊基礎架構與資安問題，不論從工作量或所需之專業與歷練，資訊長均應為專任之職位。無論從中央或到部會的資訊長，從中央資訊主管機關，到各機關的資訊單位，整個政府的資訊組織欠缺法制基礎與前瞻作為，與今日資訊發展已關係國家未來的長遠發展，並影響民眾生活至深且廣的情形，實難以匹配與呼應。」另外，劉建良先生在「資安法規面面觀」內結語「我國尚未發展一套資通安全專屬之法典，未能以資安防護之立場訂定單一全國規範，政府機關於編列預算時亦不易有統合性之資安發展與建設等相關預算，值得深思。」

目前國際間政府資訊人員占比為平均 5.1%，而我國政府機關目前資訊人員（含約聘）僅 1.52%，又比民間企業的 2.67%少，成立專責單位及擴充人力前途未明，政府各機關對於其主管業務，均有其行政法規加以規範，例如：環境保護業務，即有空氣汙染防制法；另有警察法、租稅法、地方自治法，即所謂行政法各論；即使是輔助業務的人事、會計、政風等也有，例如：主計機構人員設置管理條例，政風機構人員設置管理條例。而資訊系統對政府機關，甚至各行各業而言，不只是提升經營績效的利器，也是創造競爭優勢的重要元素，甚至是影響組織生存，已到了沒有它不行的階段，但惟獨資訊法制基礎建設仍然付之闕如，致使非但資訊組織、人力等基礎架構欠缺規範性的法制基礎，多數人寄望於今年提出的資安管理法草案能於立法院通過，希望能團結意志催生此法案。

（三）大型活動資安配套面：

日本東京即將於 2020 接辦奧林匹克運動會，在本次年會中東京的電腦防禦研究院（Cyber Defense Institute） 首席資安分析師 Mariko Miya 從過去、現在及未來的角度分享資訊安全的策略及作法，首先對比倫敦 2014 奧運所面對情境及發生過的事件進行分析，內容涵蓋：通訊監察、行動裝置的普及性、無線網路的使用情形、恐怖組織運用網

際網路狀況以及網際網路攻擊對商業的衝擊等，相對於倫敦 2014 奧運，東京 2020 奧運歸納出以下須注意的面向，包括：恐怖攻擊、地理位置/歷史/政治問題引發的網路攻擊事件、以奧運贊助商作為攻擊目標、來自內部威脅、公共 Wi-Fi 的攻擊、發生自然災害等，爰此電腦防禦研究院從過去的經驗汲取了一些想法：

1. 對參與奧運的工作人員進行忠誠調查及壓力測試
2. 研究通行證新的認證方法
3. 網際網路整備及應對措施的協同合作
4. 加強每天情報收集分析能力及協同合作分享資訊

事實上，2008 北京奧運的開幕式門票，就傳出山寨票券，倫敦奧運時多位知名選手在 twitter 上載倫敦奧運通行證的高解析度照片，無形中洩漏證件條碼等細節，恐讓罪犯有機可乘，引發保安問題，2014 年 FIFA 世界盃足球賽剛在巴西開踢，知名防毒廠商就發現超過 375 種惡意 App ，2014 年的冬季奧運於俄羅斯的索契（Sochi）展開，當時 NBC News 的特派記者 Richard Engel 與趨勢科技的安全研究人員 Kyle Wilhoit 共同進行了一項實驗，發現他攜帶至當地的 3 項連網裝置在 24 小時內就被攻擊。

2008 年北京奧運，當時每天大約有 1200 萬潛在網路攻擊，被網路人員成功攔截。然而，經過四年後，駭客攻擊的實力、規模、複雜性都大大增加在倫敦奧運期間，每天有高達 1400 萬次的網路攻擊，這些事情，運動員、粉絲大概感受不到，但網路技術安全人員則是每天在與這些駭客奮戰。

本府未來幾年都會辦理國際性大型活動，諸如爭取 2017 亞太網路資訊中心年會（APNIC Conference），舉辦 2018 台中國際花卉博覽會等，建議應學習日本，鑑往知來，將資訊安全視為一個重要議題，協同國際資安公司、電信業者及政府資安機構，整合情資，規劃多種攻擊應變的替代措施，提高應變能力，及早籌劃因應，使得活動的進行更順暢及成功。