試論我國公務機關資通安全管理機制的現況、困境與可行回應對策---以中國大陸的華為案為核心

A Study On the Current Situations, Dilemmas, and Feasible Response Countermeasures for the Information and Communication Security Management Mechanism of the Public Administration Organizations of the R.O.C---Focusing on the Information and Communication Products of the Huawei Company of the Mainland China

柯雨瑞[1]、張育芝[2]、黃翠紋[3]、曾麗文[4]
Y. R. Ko[1], Y. C. Chang[2], T. W. Huang[3], L. W. Teng[4]

[1] 中央警察大學 國境警察碩士班專任教授
The Border Police Graduate Program of the Central Police University

[2] 台南市政府警察局 第五分局行政組巡官(中央警察大學國境警察研究所法學碩士)
The Fifth Precinct of the Tainan City Police Department

[3] 中央警察大學 行政警察研究所專任教授兼所長
The Administrative Police Graduate Program of the Central Police University

[4] 彰化縣警察局 彰化分局實習所長、實習巡官（彰化師範大學工業教育與技術研究所博士）
The Changhua Precinct of the Changhua County Police Department

目次

摘要

「華為」資通事件，業已成為全球熱門之議題，全球各國因為資訊安全與 5G 網路未來之挑戰，各國有不同之意見與表態。然而我國面臨「華為」之問題，中央與地方機關之現況與困境為何？又有何種可行之解決對策？本文一共分成 4 大點來探討，首先探討各國現行之資通安全管理法制現況、我國公務機關資通安全管理之法制現況、我國公務機關資通安全管理機制之困境以及我國公務機關資通安全管理機制之可行回應對策，期待能為我國公務機關資通安全管理之機制，提出可行之方案與建議，藉以精進我國公務機關資通安全管理之量能。
關鍵字：資訊安全、陸資產品(華為手機)、國家安全、第五代行動通訊技術(5G)。

ABSTRACT

The "Huawei" telecommunications equipment products have formed a global issue. Countries have different opinions and attitudes between their national security policy and the future challenges and commercial merits of 5G networks. However, what are the current situations and predicaments facing by the central and local authorities in dealing with the "Huawei" telecommunications equipment products in Taiwan? What are the suggested , feasible and nice solutions to this issue? This paper has listed four major points to discuss about this issue. Firstly, it discusses the current legislative policy of the national security in different countries such as the United States, Germany, Japan, China, South Korea and European Union of the world. Secondly, analyze the current status of our national security defense network in our central and local government. And what kinds of struggles and dilemmas facing by our government should be solved? Finally, this article suggested some feasible recommendations to solve this significant and complicated issue.
Keywords: technology security; Huawei telecommunications equipment; national security; Critical Information Infrastructure(CII)

1. 前言

隨著「華為」事件登上國際版面，美中關係緊張到極點，美國開始使用貿易制裁來抵制華為產品進入美國，認為陸製產品有設置「後門」，能將資訊傳輸到大陸情資中心，危害國家安全，各國政府亦開始對華為資通產品展開一連串之禁止與抵制，然而各國真正衡量的是未來 5G 之發展商機與機會。因華為公司在 5G 科技之發展上已是全球三大電信公司龍頭，如果各國採取禁止與華為在未來通信方面之合作，將會在 2020 年 5G 之未來發展上失去全球之競爭力。此令各國政府相當困擾，須在國家安全、資通安全與未來 5G 之發展商機與機會三者之間，取得一定之平衡。如何取捨？考驗各國政府之專業、能力與企圖。

我國在面對陸製華為資通產品及未來 5G 之潮流下，我國政府將該如何面

對這些未來之挑戰?由於我國與中國大陸有著特殊之政治關係，對於華為產品，我方無法僅從單純之商業利益考量。究竟華為產品是否會影響到我國之資訊安全及國家安全，這些均是政府應該思考之方向。我國政府須在中華民國之國家安全、資通安全與未來 5G 之發展商機與機會三者之間，取得一定之平衡。如何取捨之？考驗我國政府之智慧、專業能力與企圖心。

目前我國政府已經在 2019 年 1 月由行政院公告中央公務機關禁止使用華為陸製產品，隨著中央之禁令，地方政府亦紛紛效應，至於國營企業及相關 8 大基礎建設之民營企業則尚未有明確之準則，目前我國政府面對華為所產生之資訊安全及未來 5G 之發展困境與建議均會在本文中探討。

2. 各國資通安全管理機制

世界各國已進入網路之爭奪戰，因此對於資訊安全之防護與立法有其重要性，尤其是各國對於資安之管理與建立，莫不提升至國家(中央政府)層級，並設立專門部門及法律加以管理。各國資通安全管理機制之概述如下：

（1）美國在 2014 年提出聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014, FISMA 2014），聯邦資訊安全現代化法(FISMA 2014）授權給美國國土安全部對於各公務機關進行監督與管理、管制重大資安事件之通報與受到侵害時之處置。另外，美國歐巴馬政府上台之後，於 2009 年 2 月，美國制定「國家網絡安全綜合倡議」(Comprehensive National Cybersecurity Initiative(CNCI)，發布對美國目前網路安全狀況之重要評估報告及建議。

（2）德國聯邦議會於 2015 年通過資訊科技安全法(IT-Sicherheitsgesetz)保障民眾與國家基礎設施之網路安全，讓德國成為網路進程中成為全球科技系統之先驅及模範（郭沐鑫，2016）。

（3）日本基於網路安全，2014 年通過「網路資訊安全基本法」（サイバーセキュリティ基本法），針對於政府機構與民間單位之資訊安全，「網路資訊安全基本法」進行規範並設立網路安全戰略本部（サイバーセキュリティ）。網路安全戰略本部於 2018 年 7 月 27 日發布網路安全年度計畫 2018(サイバーセキュリティ 2018)，持續提升國家安全之三大目標，包括：1.「提昇經濟社會活力與永續發展」；2.「實現國民安全且安心生活之社會」；3.「維持國際社會和平、安定與保障日本安全」(資訊工業策進會科技法律研究所，2018)。

（4）中國大陸於 2017 年 6 月實施「網路安全法」，總共有 7 章 79 條，立法目的在於防制網路詐騙和網路攻擊、保護關鍵基礎設施、網路用戶實名制預防犯罪事件及具有爭議之第 58 條「因維護國家安全和社會公共秩序，處置重大突發社會安全事件之需要，經國務院決定或者批准，可以在特定區域對網路通信採取限制等臨時措施」來限制級保障國家安全(數位時代，2016)。中國大陸政府之資通安全管理法制，最具爭議性的，係為「中華人民共和國國家情報法」，尤其是該法第 14 條規定：「國家情報工作機構依法開展情報工作，可以要求有關機關、組織和公民提供必要之支持、協助和配合。」第 14 條之前述規定，備受全球各國政府之批評。批評力道最強者，則為美國。

（5）南韓資訊安全署（Korea Internet & Security Agency）因應資訊安全帶來之威脅提出資訊與通訊基礎設施保護法（Laws on the Internet and Information Security of Korea），對於不同之網路犯罪訂出相關之法律規範。

（6）歐盟於 2013 年發布網路暨資訊安全戰略(Cyber security Strategy of the European Union)，希望提供一個開放、安全與可靠之網路空間(An Open, Safe and Secure Cyberspace)，以實現網路安全防護、減少網路犯罪、建立歐盟安全之網路空間及促進歐盟之價值核心為主軸與訴求（王家宜，2014）。再者，於 2016 年，歐盟發布一項新的指令，名稱為歐盟網路與資訊系統安全指令（Network and Information Security Directive, NIS Directive），以管制資通安全(資策會科技法律研究所，2019)。

(7) 由於歐盟在 2016 年發布歐盟網路與資訊系統安全指令（Network and Information Security Directive, NIS Directive），英國亦於 2018 年，頒布電子通訊之網路與資訊系統規則（The Network and Information Systems Regulations 2018），英國之該規則，係實施與踐行歐盟 2016 年網路與資訊系統安全指令（Network and Information Security Directive, NIS Directive）之相關要求(資策會科技法律研究所，2019)。

3. 我國公務機關資通安全管理機制之現況

3.1 我國公務機關資通安全管理之法制現況

吳啟文（2018）在「資通安全管理法之挑戰與因應」文中提到我國行政院於 107 年 6 月 6 日公布「資通安全管理法」規範公務機關及提供關鍵基礎設施之非公務機關，以風險管理為核心訂定相關之資通安全維護辦法及應變計畫，除資通安全管理法為我國資訊安全之母法外，另外，尚包括：刑法第 36 章(妨害電腦使用罪章)、電信法、電子簽章法、國家機密保護法、個人資料保護法、金融控股公司法、銀行法、醫療法及人體生物資料庫管理條例等相關子法(吳啟文，2018）。

依據上述「資通安全管理法」所頒布之相關行政命令，計有：各機關對危害國家資通安全產品限制使用原則(行政院於民國 108 年 4 月 19 日公布)、大陸委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 18 日)；中央銀行所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 22 日)；內政部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 12 日)；公務機關所屬人員資通安全事項獎懲辦法 (民國 107 年 11 月 21 日)；文化部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 18 日)；外交部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 01 月 31 日)；交通部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 25 日)；行政院原子能委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 04 日)；行政院農業委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 13 日)；金融監督管理委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 27 日)；科技部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 23 日)；原住民族委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 06 日)；特定非公務機關資通安全維護計畫實施情形稽核辦法 (民國 107 年 11 月 21 日)；財政部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 26 日)；國防部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 03 月 27 日)；國家通訊傳播委員會所管特定非公務機關資通安全管理作業辦法 (民國 108 年 04 月 01 日)；經濟部所管特定非公務機關資通安全管理作業辦法 (民國 108 年 02 月 23)；資通安全事件通報及應變辦法 (民國 107 年 11 月 21 日)；資通安全情資分享辦法 (民國 107 年 11 月 21 日)；資通安全責任等級分級辦法 (民國 107 年 11 月 21 日)；資通安全管理法施行細則 (民國 107 年 11 月 21 日)；僑務委員會所管特定非公務機關資通安全管

理作業辦法 (民國 108 年 02 月 13 日)。

3.2 我國公務機關資通安全管理政策受到美國外交政策之重大影響

美國政府前中央情報局(CIA)分析員 Jack Davis 曾指出，情報分析員必須在恐怖事件發生前，判讀充分之預警情資，以便讓美國政府能採取保護作為，鑒於對大量數據進行分析相當複雜，須有情報之前置作業時間，以令美國之預警能力會更好。

我國公務機關在資通安全管理之政策走向方面，向來是受到美國外交政策之重大影響，起先，美國態度強硬，向同屬「五眼聯盟」（Five Eyes，FVEY）之英國、加拿大、紐西蘭及澳洲盟友提出勿採用陸製華為之相關資通設備，若有國家選用華為設備並安置在重要系統內，則美方就不能與該國共同分享情報，以此作為威脅華為 5G 進入美國市場。為台美友好關係，我國政府便於 2019 年 3 月公告公務機關禁止使用華為大陸通訊設備。然而時間隨著美國總統川普對於華為設備之態度趨漸軟化，川普希望美國亦盡快推出 5G 技術與中國進行公平之技術之爭。為此我國工商團體亦強烈表明呼籲政府停止觸動大陸之網軍之戰，以免台灣商品受到抵制、台商企業困境雪上加霜，更何況由政府帶頭抵制更是容易引起兩岸敏感之政治議題（黃有容、王玉樹，2019）。我國工商團體對於行政院公告公務機關禁止使用華為大陸通訊設備之政策，非常不以為然。由此可看，我國工商團體在意者，係為商機，國家安全與資通安全部分，則非我國工商團體所關注者。由此，亦可顯示行政院公告公務機關禁止使用華為大陸通訊設備之政策，有著正反面之看法與意見。基本上，我國工商團體極力反對行政院之上開政策。本文認為，我國工商團體之作法，似恐有違反「資通安全管理法」之相關立法精神意旨。

3.3 使用華為陸製資通產品隱藏重大國安危機

至於我國公務機關若使用陸製華為設備是否有非常大之國安危機？尖端科技軍事雜誌社長畢中和(2019)即提到「因為華為之強大，引起西方國家之警惕」，華為 5G 之發展已使得全球許多先進國家與其合作使用該公司之通訊設備，未來十年內之網路軟硬體發展必將讓華為在全球佔有一席之地，而華為之影響力亦將讓中國在網路戰上對全球各國經濟、軍事及政治上，造成某種程度之威脅。同時亦嚴重影響到我國兩岸未來之戰爭型態，及我國易成為對岸之網路攻擊目標，且令人有疑慮的，是華為帶有濃厚軍方之色彩，中共可能在華為之產品設置「後門」，藉以傳輸我國重要之國安、資安數據，在戰時，其有能力癱瘓我國國軍、公務機關、民間之行動通訊系統，此部分，是我國中央政府特別擔憂之區塊。

3.4 地方政府對於陸製華為之資通產品所造成之國安危機未有充分之認知

各國因為資安考量紛紛下令禁用華為手機及資通設備，目前我國政府亦於 2019 年 1 月 15 日起由工研院帶頭禁用華為手機和電腦使用內部網路。但其實早在 2013 年，國家通訊傳播委員會（NCC）在 4G 釋照案時，即依照「行動寬頻業務管理規則」第 43 條規定，要求系統建設業者應考量國家安全，禁止使用中國製之網路和相關基地台之資通設備（徐子捷，2019）。

以上，是中央政府之態度，然地方政府對於陸製華為設備所造成之國安危機，在回應對策上，尚在研議過渡汰換、觀察、消極不配合階段，有些地方政府，甚至是非常不配合中央之行政院於 2019 年 1 月所發布行政命令禁止採購及使用陸資產品之處理原則。本文擬提出一個觀點：資安即國安，有關資安、國安之課題，

應無中央、地方之明顯區別。茲舉一例證明之，有關國家元首、副元首、重要部會首長之人身安全維護，內政部警政署警官隊亦為負責單位之一，如國家元首、副元首擬至各地方巡視，內政部警政署警官隊會與各地方政府之警察局共同合作，維護國家元首、副元首之人身安全，假若，各地方政府之縣市警察局各科室之資通系統，亦採購及使用陸資產品，恐將國家元首、副元首之人身安全及行踪，完全曝露於中國大陸之國安、情報、軍事機關之掌控之下，毫無機密可言，具有極高度之人身安全之風險，恐亦非良策。

此亦可證明，若干地方政府對於陸製華為之資通產品所造成之國安危機未有充分之認知。本文認為，若干地方政府，消極不配合中央行政院之禁止採購及使用陸資產品之處理原則之作法，似恐有違反「資通安全管理法」之相關立法精神意旨。如僅著眼於發展地方上之商機與觀光，而漠視國家安全、資通安全，在心態上、作法上，似亦有可議之處。亦即，地方政府對於陸製華為之資通產品所造成之國安危機未有充分之認知，本文不表贊同。事實上，資通安全即為國家安全，資安即國安，地方政府亦有憲法上、法律上之法定義務，共同維護國家安全、資通安全。此種之法定義務，不限定在中央政府。承上所述，台南市政府則對於陸製華為之資通產品，所造成之國安危機，較有有充分之認知，且有意願配合中央之禁止採購及使用陸資產品之處理政策，本文敬表贊同之。依據作者實地訪談台南市政府相關機關所得，台南市政府智慧發展中心曾行公文給各台南市政府所屬機關，針對機關內部是否使用陸資產品並依資安防護相關規定進行盤點，盤點之內容針對 4 大要項，如下所述：

（1）台南市政府不得採購陸資產品；
（2）倘清點物品屬陸資產品，應訂定汰換時程；
（3）已屆使用年限者產品，應逾 1 年內汰換；
（4）嚴禁非公務使用之個人行動裝置等資通訊產品，連接台南市政府及所力機關內部網路。

4.　我國公務機關資通安全管理機制之困境

4.1 禁止連結陸方網站與使用陸製資通產品(含手機)，中央政府與地方政府不同基調

為了避免來自中國之資安危機，同時亦讓公務機關有明確依循準則，我方中央政府由行政院於 2019 年 1 月發布行政命令禁止採購及使用陸資產品之處理原則及公務手機電腦連結到中國大陸 5 大知名社群網站，如新浪微博、騰訊微博、微信、人人網及百度等搜尋引擎等，並且包含修圖程式，至於禁止我方公務機關之電腦連結至相關陸方網站之詳細清單，尚未有明確之依據，尤其是連結特定敏感之網站（李欣芳，2019）。

我方行政院發言人 Kolas(谷辣斯，2019)表示依照「行政程序法」規定，國營事業不納入中央機關適用範圍，但依「資通安全管理法」之規定，國營事業相關之水、電及通信等八大關鍵基礎設施，係在「資通安全管理法」適用之範圍內，因此，地方機關及國事營業是否要納入遵守該原則？目前政府尚未有定案，尚在詳細評估之中。

行政院資通安全處長簡宏偉（2019）表示，公務機關在上班時間原本即禁止連結至大陸特定敏感之網站，至於禁止連結陸方網站之清單，由地方各單位自行評估，由此可見地方政府目前，對於禁止公務機關電腦及手機，連結到陸方網站，並未有統一之規定。

承上所述，以台南市政府為例，該府研考會智慧發展中心全面地、澈底地盤

點所屬資通訊設備，並全力配合中央資通安全政策，全面禁止使用華為設備。研考會智慧發展中心表示，已函文台南市政府所屬各機關，要求所屬成員之個人行動裝置，應避免連上台南市政府及其所屬機關之內部網路(禁止連上內網)，研考會智慧發展中心另提醒資安網路設備之所有採購案件，應考量資安洩漏至中國大陸國安機關、情報機關之風險，將資安洩漏風險列為資安網路設備所有採購案件之評選、評分參考，研考會智慧發展中心另要求台南市政府及其所屬機關盤點所屬資通訊設備是否有華為設備(臺南市政府智慧發展中心，2019)。

公務機關涉及禁止採購及使用陸資產品之區塊，在 2013 年 10 月，國安局即禁止華為公司在台投標，國安局並對國內各中央、地方公家機關建議，勿使用中國產品。行政院於 2019 年 1 月，曾發布行政命令禁止採購及使用陸資產品，對於此一處理原則，各地方政府反應皆不相同，彰化縣政府、南投縣政府、雲林縣政府並未禁止使用之，明顯地，這些縣政府並無意願配合中央之資安政策；屏東縣政府迄今尚未使用華為產品，屏東縣政府高度願意配合中央之資安政策；另外，高雄市政府現在未禁止華為產品，但高雄市政府表示，若中央政府行文禁用，則會照辦；此外，台中市政府表示，禁用部分大陸製造之資訊產品已行之有年，之後，會配合、遵守行政院規畫之相關命令(三立新聞網，2019)。據上所述，禁止連結陸方網站與使用陸製資通產品(含手機)之區塊，目前，中央政府與地方政府不同調。

4.2 我國民間之資通大廠業已與華為公司血脈緊密地相連，已成生命共同體，兩者之商業利益，環環相扣，著實不易切割

美國利用加重貿易關稅之脅迫下，呼籲歐洲各國禁用華為公司等陸製之資通產品，然而，華為產品之優勢，極具吸引力。歐洲民間電信商卻對於華為產品之優勢，及良好品質等特點，表現出高度之欣賞，尤其是華為已晉升為全球四大電信公司，包括瑞典 Ericsson、芬蘭 Nokia 及南韓 Samsung 等，且未來 5G 第五代行動通訊技術基地台之供應與技術上，華為更是不遑多讓，這亦是各國在華為之安全疑慮與商業利益上之考量上，非常費心，究竟要如何取得平衡(張正芊，2019)？

對於美國及我國政府禁用華為相關電子設備，民間企業並不認同，三三三會會長許勝雄(2019)認為各民間企業、尤其是電子企業均有相關之資安機制，不只是華為產品，各國之產品，亦均設有防駭客、防資訊盜用等機制，民間企業重視的是經濟，有關資安方面之問題，應交給資安專家來解決，而非一味的禁用華為公司之資通設備。

台灣若禁止華為及其他相關陸製資安產品，中國可能會利用經濟報復之手法，制裁我國在貿易上之輸入，禁止進口我國生產之某些 5G 相關產品及電子設備，而我國之電子大廠鴻海等多在對岸有設立廠房，如爆發報復戰，兩岸嚴重之對立情形，勢必會重挫我國經濟，產生強大之骨牌效應(林忠正，2019)。

4.3 禁用華為公司之相關資通產品之後，我國是否有能力邁向 5G 時代，仍有待進一步觀察

日本總務省 2019 年 4 月 10 日核准國內 4 家電信公司 DOCOMO、KDDI、SOFTBANK 和樂天公司提出之 5G 營運申請案，而出於安全之理由，日本總務省排除大陸通信設備，如華為技術等產品，4 家公司將在 2020 年投入 1.6 兆日圓（約 4500 億新台幣）於基地台之建設，而這亦是 21 世紀之核心基礎設施（楊家鑫，2019）。

歐盟對於華為公司 5G 之技術，則保持著合作之關係，中國與歐盟 2014 年通過「中歐合作 2020 戰略規劃」其中在今年 2019 年雙方之第 21 次會談中談到 5G 技術之交流及不強制轉讓技術，共同致力於世界貿易組織 WTO 之多邊貿易體制，雖然美國總統川普極力反對並使用貿易加稅之手段或是情資無法共享來懲罰盟友，但基於各國利益間之考量及政治衝突，各國在追求自身利益下亦持續與大陸企業進行 5G 產業領域合作(蕭徐行，2019)。

國家通訊傳播委員會（NCC）從 2018 年起，積極規劃 5G 應用與產業創新為發展方向，期待從 2017 年至 2020 年各階段能將 5G 系統最優化及大規模之應用於國內各場域，如下圖所示。除規劃高/中/低頻評估及修改電信管理法廢除電信事業分類，將特許制、許可制修正為登記制，鼓勵市場參進。

圖 1：提供 5G 技術及整合試煉平台
資料來源：(行政院DIGI+會議， 2018)

然華為技術台灣總代理訊崴技術總經理雍海（2019）則認為，5G 在台灣之發展還有很長之時間要走，今年(2019 年)不會落地，明年(2020 年)難度亦很大，從其言談中就發現我國在 5G 之研發上仍具有極大之挑戰(雍海，2019）。

5.我國公務機關資通安全管理機制之可行回應對策

我國政府2001起至2016在國家資通安全發展政策中，推動連續四期之重大資安政策進程：第一期機制計畫建構整體資安防護體系；第二期機制計畫健全整體資安防護能力；第三期發展方案安全性之智慧台灣，安心優質之數位生活；以及，第四期發展方案建構安全資安環境，這四期之內容，說明政府初期以建構資安認知宣導、系統建置、人才培育、技術研發、法律及國際合作方面等提昇我國之資訊安全環境（行政院，2018）。

如今2020年更是迎向全球5G潮流之時代，面對未來資安之挑戰、數位經濟與物聯網(Internet of Things, IoT)時代，行政院於2018年提出DiGi+法案「數位國家．創新經濟發展方案 (2017-2025 年)」，推動「友善法制環境」、「跨域數位

人才」、「先進數位科技」等三項數位國家配套措施，打造安全可信賴之「數位創新基礎環境」及「網路社會數位政府」，而華為事件之影響，亦考驗我國政府在資安專業人才與資安防護對策之提出（行政院，2018）。

5.1 有必要準確地評估華為公司資通產品之國安危機

在資訊安全之防護上我國「國安會資安辦、行政院資安處及國家通訊傳播委員」形成三個資安鐵安角為我國之國家安全及 8 大關鍵基礎設施加強防護，透過「強化早期預警、持續控管與維運、通報應變與協處改善」等 4 大面向來建立 8 大關鍵基礎設施領域之聯防機制(國家資通安全戰略報告，2018)。

於 2018 年之下半年,日本政府日前正式宣布禁用華為公司之相關資通產品,日本政府發現華為公司之相關資通產品內，隱藏有「間諜晶元」,「間諜晶元」威脅到日本國家安全。此外，華為公司之網路資通設備，亦被批評留有後門，令中共軍方、國安、情報機關，可以隨時藉由華為公司之網路資通設備，存取任何資料，備受海內外各國政府之質疑(羅婷婷，2018)。

復次,依據英國資訊安全雜誌「SCmagazine」及美國科技網站「Lightreading」之報導，華為公司資通產品確實隱藏後門。微軟工程師拆解華為筆記型電腦之後，發現華為筆記型電腦中有類似於美國國家安全局所使用的「後門」技術，此種之「後門」技術，可以讓無權使用者，改變其身分，而成為超級用戶，並有權限建立盜取程式(羅綺，2019)。

因華為或是陸制資通產品(手機、筆記型電腦、、、等)，被全球各國政府高度懷疑設置「後門」,是以，各國對於與大陸華為公司開放 5G 之合作方案態度，亦各有正反之表態，如五眼聯盟：美國、澳洲、紐西蘭、英國、加拿大及日本等多國，基於國安、資安之疑慮，抱持著反對之政策，而某有些國家如：歐盟、葡萄牙、印度、德國卻是抱持著贊同或不表態之意見，這些認同之國家認為未來 2020 之 5G 潮流，需要與華為公司之協助，始能幫助其擴展更大之商業利益與國家競爭力，至於國家安全，則是採取雙方合作並加強資安之防護。對於華為陸製產品之態度,我國政府目前基於國家安全理由是採取官方禁止使用及採購，至於民間機構則無相關禁止使用之規定。本文建議，仍有必要準確地評估華為公司資通產品造成之國安危機，儘可能地限縮禁用之範圍，以利在國安、資安與台灣之 5G 發展方面，取得平衡點。

5.2 地方政府與中央政府之資通安全管理機制宜同調

鑑於兩岸之特殊關係,我國政府相較於其他國家更應在華為事件上更加謹慎防止資訊外洩及國家安全之防護，除了加強政府機關公部門機構禁止採購及使用華為等陸製資訊產品外,建議對於國營企業、國家安全相關或是 8 大關鍵基礎設施之民營企業等均應列入禁止使用之範圍，避免我國之國家機密資訊長期暴露在風險之中。

此外，地方政府目前尚未進行全面之調查機關內是否仍有採購華為等陸製資通設備，筆者建議各機關政府可參考臺南市政府之作法。臺南市政府智慧發展中心行文給各台南市政府所屬機關之公文規定之中，下令各機關應全面清查相關之陸製資安產品數量、未來禁止繼續使用、採購陸製資安產品及訂定產品淘汰期程，此種之作法，有利各級地方政府防堵資訊安全之漏洞，值得公務機關參考之。

5.3 我國公務機關資通安全管理機制宜在美國與中國爭奪全球資通霸主之角力

中，尋找最適配之模式

2016 年我國首次出現外籍人士到台灣第一銀行 ATM 盜領鉅額款項，車手不需提款卡提款，國際駭客單靠惡意程式則可提領巨額資金顯示出我國官股銀行出現資安大漏洞，讓國際駭客集團在全世界橫行無阻，雖然我國有查獲提款車手，但是對於幕後之駭客集團仍未有進一步之收穫，尤其是跨國性之犯罪更是需要國際高度之合作與國際刑警組織提供相關之情資始能免於跨國犯罪集團之駭入（呂昭隆，2018）。然而我國並非聯合國成員，因此許多資訊安全之交流與情資，我國並未能及時更新與接收，因此在我國面對兩岸關係及中美貿易大戰之拉鋸戰中，我國政府對開放使用華為資通之商品之態度與作法，則成為兩國角力之對象。

美台商業協會會長 Rupert Hammond-Chambers(2019)指出，美國對台使用華為產品之態度，美國政府強硬的對台灣表示，如果使用華為網路設備，美國將會取消與台灣有關任何合作，如技術或是情資之分享與合作。基於國家安全理由，美國政府建議台灣及所有國家在公務機關應該全面禁止使用華為設備，至於民間團體之部分，雖不能強硬之禁止，但需要利用教育及宣導，勸戒民間個人或團體不要使用該國之相關資通產品(鍾錦隆，2018)。

在美國宣布抵制華為產品之後，華為公司公布 2017 年之財報指出，華為之營收可分為 4 部分，最大之銷售數量以中國為最，佔 50.5%、亞太市場約 12%、歐洲中東和非洲是 27%，而美洲市場只占 6.5%，詳如圖 2，從數據中顯示就算美國抵制華為手機，但是實際影響華為之銷售訂單並無太大影響，更何況華為公司之產品有其價格便宜、品質好、照相品質功能佳等銷售競爭力，故民間企業團體及個人反而會相對購買較具高價性能之華為(鍾張涵，2019) 。

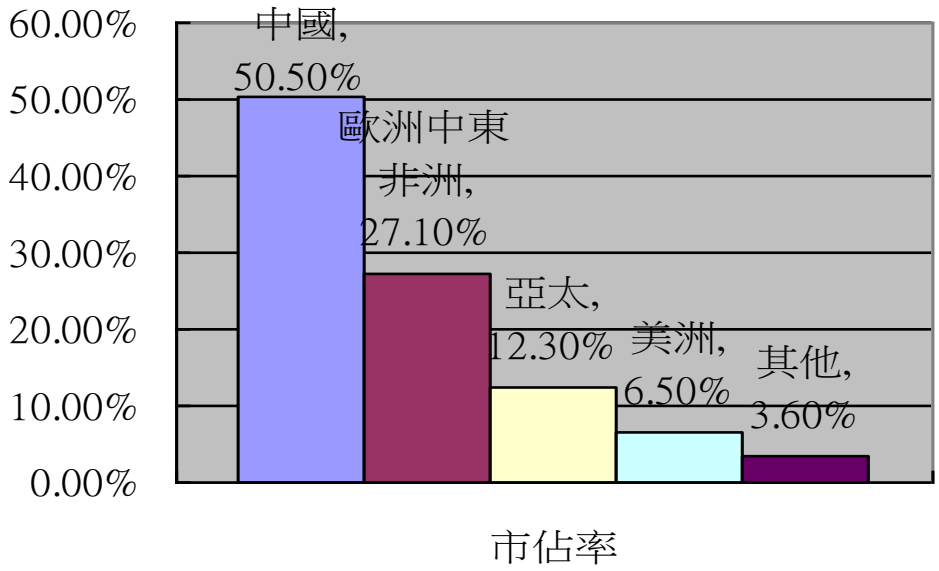


圖 2：華為全球市佔率
資料來源：(華為2017年財報，2019)

華為事件已成中、美間之政治與貿易大戰，我國之定位又該何去何從?如何在國安、資安與經濟發展間，取得一個平衡之位置，實屬我國政府應該仔細思

考之一個議題。本文建議，在不影響國安、資安之大前提之下，國安、資安與經濟發展三者平行發展為佳。

5.4 落實資安宣導，宜強化政府與民間對於華為公司之資通產品所造成國安危機之認知與共識

在打擊網路犯罪之預防上，2002 年我國政府提出「電子簽章法」利用公鑰基礎建設（Public Key Infrastructure, PKI）建立民間企業與政府利用線上身份辨識系統及電子文件資訊分享促進政府效能。2003 年制訂「國家機密保護法」落實國家公務機密之保護及制訂 2005 年「政府資訊公開法」流通政府資訊及促進人民對公共事務之瞭解，2009 年修訂「資通安全規範整體發展藍圖」參照前全球先進國家資安發展經驗，並考量我國政府機構現行法制與資訊環境特性建立資安國家標準與發展，而對於民眾個人隱私及資料之防護上，法令則有「個人資料保護法」、「刑法」、「通訊保障及監察法」及「電信法」及 2018 年行政院提出 DiGi+法案「數位國家．創新經濟發展方案」，這些均是我國政府目前與地方政府所進行之資安政策與防護（李如霞，2019）。

而對於華為事件對我國帶來之資安風險，中央與地方政府、國營企業及 8 大關鍵基礎建設之民間企業或可依照國家安全、國土安全之相關規定，禁止使用與採購陸製資安設備；相對而言，另對於民團體及個人則以柔性宣導或是教育之方式避免民眾購買陸製手機，避免資安外洩之疑慮。

於 2019 年 1 月，我國工研院公告下令禁止使用華為手機，成為公務機關禁止使用華為手機、資通設備之首位發聲者，之後，國研院與資策會陸續跟進，相繼宣布禁止華為設備連上國研院與資策會之內網。而至於華為手機是否真正有資安之疑慮，有傳輸之後門系統？目前仍無相關之明確性證據，但有許多之資安專家表示，華為的確有其資安風險，因為它的商業模式與其他的智慧型品牌不同，有可能會被使用於政治性用途，我們目前尚未能驗證其安全性，為了國家安全起見，台灣之中央與地方機關應該要禁用華為設備與手機(Lynn，2019)。

除了鼓勵與宣導在尚未證實華為手機通過資安之安全檢測前，民眾及企業盡量減少購買或是使用華為等相關設備，除了硬體之使用外，對於大陸開發之軟體 APP 微信等亦盡量減少下載使用及連結到大陸網站，避免個資遭到連結傳輸與散布。

5.5 政府與民間宜儘速完善其內部之資安規範

根據國會立委最新之調查顯示，我國有近 8 成之中央政府機關，尚未仔細、詳盡之評估國外公務或國外民間機構，其對於個資保護之程度與機制，以致於我國公、私部門傳送到國外公務或國外民間機構之資訊，存有非常大之資通安全漏洞，令個資保護之相關法令，已形同具文。再者，政府部門亦無法了解我國私部門、業者之雲端資料庫，是否設置在中國或外國何處(蘇芳禾，2019)？雲端資料庫可儲存大量之資料與情資，而我國私部門、業者之雲端資料庫究竟設置何處？我國政府部門、民間機構均無法清楚知曉之。

國家通訊傳播委員會曾在 2012 年公告「限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區」，但，其他之中央目的事業主管機關，則未頒布類似之法令。究竟我國之私部門、業者之雲端資料庫，可否設置在中國大陸？或者，將所屬用戶之個人資料傳遞至大陸地區？目前之狀況，仍屬非常模糊之地帶(蘇芳禾，2019)。本文建議，中央目的事業主管機關宜比照國家通訊傳播委員會所

公告之「限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區」之機制，亦頒布相關之管制、監控、管理之法令，以免重大情資(含國家安全情報)被傳送至中國大陸之國安、軍事部門。

再者，我國私部門、業者所蒐集之個人資料，如要委託至境外處理，目前，在國內之部分，僅有金管會對於金融機構所蒐集之個人資料，如要委託至境外處理，需事前得到該會之核准，其他之中央目的事業主管機關，亦未有相關之管制機制(蘇芳禾，2019)，建議政府之其他之中央目的事業主管機關，宜比照上述金管會對於金融機構之監控機制為佳。

5.6 我方宜持續地善意建議中國大陸政府，修改其「中華人民共和國國家情報法」，避免侵犯人權及其他國家或地區之國家安全

有關中國大陸政府之「中華人民共和國國家情報法」區塊，根據該法第 1 條之立法目的，係「為了加強和保障國家情報工作，維護國家安全和利益，根據憲法，制定本法。」是以，「中華人民共和國國家情報法」之最核心目的，係為維護中華人民共和國之國家、生存、安全和利益，具有極高度之政治色彩。

另外，根據該法第 14 條之規定：「國家情報工作機構依法開展情報工作，可以要求有關機關、組織和公民提供必要之支持、協助和配合。」是以，依據「中華人民共和國國家情報法」第 14 條之要求，當國家情報工作機構命令華為公司提供相關之情資時，華為公司不得拒絕。

在此情況下，國家情報工作機構業已嚴重侵犯民眾之隱私權、秘密通訊之自由，而這些均是極其重要之人權。再者，亦可能侵犯到其他國家或地區之國家安全(含台灣)，是以，本文建請中國大陸體認民眾之隱私權、秘密通訊之自由，宜妥善加以保護之。在此脈絡下，中國大陸政府其「中華人民共和國國家情報法」，不宜侵犯民眾之隱私權、秘密通訊之自由，及其他國家或地區之國家安全(含台灣)。

6. 致謝

本文特別感謝 2019(第十七屆)危機管理學術研討會暨 2019 工業工程與安全管理學術研討會之大會相關籌辦人員、空軍軍官學校航空管理系王心靈教授(現為社團法人中華民國危機管理學會秘書長)諸多行政上之協助；另外，作者亦感謝台南市政府警察局第五分局負責資通安全之相關承辦人員之協助，提供相當寶貴之專業、實務意見及資料，在此，一併致上非常誠摯之謝意、敬意。

7.附件：各機關對危害國家資通安全產品限制使用原則
行政院 2019 年 4 月發布

各機關對危害國家資通安全產品限制使用原則

一、為推動資通安全管理法（以下簡稱本法）第五條第一項所定資通安全整體防護事宜，強化中央與地方機關（構）、公立學校、公營事業及行政法人（以下簡稱各機關）之資通安全防護，降低國家資通安全風險，特訂定本原則。

二、本原則所稱危害國家資通安全產品，指對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務。

三、本法主管機關應基於國家安全、國際情資分享、潛在風險及衝擊分析等因素，蒐集相關機關意見綜合評估，據以核定生產、研發、製造或提供前點產品之廠商清單。

本法主管機關應定期檢視前項核定之廠商清單，並依前項因素重新評估後，視需要調整。

四、各機關除因業務需求且無其他替代方案外，不得採購及使用第三點之廠商產品。

各機關必須採購或使用第三點之廠商產品時，應具體敘明理由，經本法主管機關核可後，以專案方式購置，並列冊管理及遵守下列規定：

（一）應指定特定區域及特定人員使用。

（二）不得與公務網路環境介接。

（三）不得處理或儲存機關公務資訊。

（四）測試或檢驗結果應產出報告。

（五）購置理由消失，或使用年限屆滿應立即銷毀。

五、各機關應依下列規定定期辦理資產盤點：

（一）對本原則生效前已使用之第三點之廠商產品，應於廠商清單提供後三個月內列冊管理，不得與公務網路環境介接，並應移至非敏感或非重要環境。

（二）前款之廠商產品已屆使用年限者，應於廠商清單提供後，即刻編列預算於該年度內汰除；未達使用年限者，應定明汰除期限。

六、各機關應向所屬人員宣導使用危害國家資通安全產品之風險。

七、中央目的事業主管機關應督導本法所定關鍵基礎設施提供者及政府捐助之財團法人，參考本原則之規定辦理。

8. 參考文獻

(1)中文資料

Lynn (2019). 美國提起訴訟宣戰，華為資安風暴來襲，比起華為手機能不能買，其實更危險的恐是這種 APP. Lynn 寫點科普，觀點筆記部落格.

Marc Goodman(2016)，林俊宏譯，未來的犯罪，新北：木馬文化。

William Brittain-Catlin 著、李芳齡譯(2007)，境外共和國：揭開境外金融的秘密，天下雜誌出版。

十二屆人大常委會：個人信息怎麼保護(2016)，華律網，2016 年 10 月 31 日，http://www.66law.cn/laws/159822.aspx。

三立新聞網(2019) . 台南市府開第一槍！禁用華為相關產品， 2019 年 02 月 18, 取自 https://www.msn.com/zh-tw/news/national/。

土城分局(2015)，刑事局偵破 3 仟萬城堡別墅機房兩岸電信詐欺集團案，新北市政府警察局新莊分局，上網瀏覽時間：2015/10/01, http://www.xinzhuang.police.ntpc.gov.tw/cp-492-11757-18.html。

中華人民共和國公安部(2015)，公安部與美國警方聯合摧毀全球最大中文淫穢色情網站聯盟，瀏覽日期：2015/10/30，網址：http://app.mps.gov.cn:8888/gips/contentSearch?id=2871356。

內政部警政署(2010)，警察偵查犯罪手冊，台北：內政部警政署。

王勁力(2010)，論我國高科技犯罪與偵查－數位證據鑑識相關法制問題研究，科技法律評析，第 3 期，高雄：國立高雄第一科技大學。

王勁力(2013)，電腦網路犯罪偵查之數位證據探究，檢察新論，第 13 期，台北：台灣高等法院檢察署。

王郁倫、唐子晴(2019). 華為苦日子說打破美好想像，工研院說：5G 慢慢爆是

好事 2019 年 4 月 12 日, 取自 https://www.bnext.com.tw/article/52037/huawei-5g-2019-slow-step-itri-

王家宜(2014). 歐盟網路安全策略 2019 年 4 月 8 日, 取自 http://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1361

王乾榮(2004)，犯罪偵查，臺灣警察專科學校，第 369-372 頁。

王翔正(2011)，網路即時通訊詐欺犯罪偵查，刑事雙月刊 45 期，42-45 頁。

王寬弘(2011)，大陸地區人民進入台灣相關入出境法令問題淺探，2011 年人口移動與執法學術研討會，桃園：中央警察大學。

王寬弘(2012)，大陸地區人民進入台灣相關入出境法令問題淺探，國土安全與國境管理學報，第 17 期，桃園：中央警察大學，頁 155-185。

立法院(2015)，防治網路霸凌公聽會：立委王育敏召開公聽會，研商網路霸凌防治，瀏覽日期：2015/11/12，http://www.ly.gov.tw/03_leg/0301_main/public/publicView.action?id=6512&lgno=00004&stage=8。

刑事警察局偵查第 9 大隊(2015)，國內首宗兩岸合作偵破最大網站賭博第 3 方支付中心，上網瀏覽時間：2015/10/01, http://www.cib.gov.tw/news/Detail/29436。

朱昌俊(2016)，網路安全法不能取代個人信息保護法，2016 年 11 月 09 日，http://webcache.googleusercontent.com/search?q=cache:gNer_oileoQJ:http://ep.ycwb.com/epaper/ycwb/html/2016-11/09/content_186075.htm%2B%E7%B6%B2%E7%B5%A1%E5%AE%89%E5%85%A8%E6%B3%95++%E5%80%8B%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E8%AD%B7%E6%B3%95&hl=zh-TW&gbv=2&ct=clnk。

行政院(2018). 國家資通訊安全發展方案.行政院國家資通安全會報.頁 1-18.

何芸欣(2005)網路詐欺之研究，國立臺北大學碩士論文。

余德正（2000）不法使用網際網路之刑事責任。東海大學法律學系研究所碩士論文。

吳啟文 (2018).資通安全管理法之挑戰與因應,2018 數位 X -資安轉型論壇,台灣.

呂昭隆(2018).一銀 8,300 萬 ATM 盜領案，退休國安高層揭破案內幕，2019 年 04 月 17,取自 https://www.chinatimes.com/newspapers/20181029000310-260202?chdtv

呂惠娟(2017)，物聯網與電子商務的發展趨勢，紡織月刊，第 249 期，頁 28-32。

李如霞(2019). 新編國家安全與國土安全精粹：網路恐怖攻擊應變機制,士明,台北,213-221.

李欣芳(2019). 防中國竊密公務手機禁連微博等 4 大社群網站,自由時報.

李進建(2015)，論大數據於犯罪偵查之挑戰與因應，全國律師，頁 60-70。

汪毓瑋(2015)，國土安全理論與實踐之發展，國土安全與國境管理學報，第 23 期，頁 1-47。

周漢華(2006)，個人信息保護法（專家建議稿）及立法研究報告，北京：法律。

孟維德(2015)，跨國犯罪，台北：五南，頁 397-434。

孟維德(2005)，海峽兩岸跨境犯罪之實證研究－以人口走私活動為例，刑事政策與犯罪研究論文集（13），頁 137-184。

孟維德、黃翠紋(2012)，警察與犯罪預防，台北：五南。

林山田、林東茂（1997）。犯罪學。臺北：三民。
林文龍（2003）線上遊戲犯罪偵查模式之研究。佛光人文社會學院資訊學研究所碩士論文。
林宜隆（2009）。網路犯罪：理論與實務，網際網路與犯罪問題，修訂第三版，桃園：中央警察大學。
林宜隆、邱士娟(2003)，我國網路犯罪案例現況分析，中央警察大學資訊、科技與社會學報。
林宜隆、張志宋（2008）。台灣地區網路犯罪現況分析-以刑事警察局破獲之案例為例，知識社群與系統發展學術研討會，臺北：文化大學。
林宜隆、黃讚松（2002），建構網路犯罪預防整體概念，中央警察大學資訊、科技與社會學報。
林宜隆、葉家銘(2008)，論述 ISMS 資訊安全管理系統發展網路犯罪預防策略的新方法，發表於教育部 TANet 2008 研討會，台北：教育部，瀏覽日期：2015/11/1，網址：http://www.powercam.cc/show.php?id=678&ch=23&fid=119。
林忠正(2019).禁用華為產品，合乎台灣的利益嗎 2019 年 04 月 17, 取自 https://forum.ettoday.net/news/1386135/
邱俊霖(2015)，近年科技犯罪趨勢與犯制對策，刑事雙月刊，第 65 期，台北：內政部警政署刑事警察局。
邱琳雅(2008)，德國聯邦個人資料保護法（BDSG），金融聯合徵信雙月刊，第 8 期，頁 60-64。
宣律師(2016)，圖解式法典：憲法及相關法規，台北：高點，頁 50-56。
施能新(2005)，電子郵件犯罪偵查機制之研究，中央警察大學資訊管理研究所碩士論文，16-30 頁。
柯雨瑞、蔡政杰(2016)，從犯罪預防觀點探討兩岸跨境網路犯罪之治理，收錄於全球化下之國境執法，台北：五南，頁 33-62。
洪文玲(2005)，行政調查制度之研究，內政部警政署警察法學，第 4 期。
范國勇，江志慶(2015)，ATM 轉帳詐欺犯罪之實證研究，刑事政策與犯罪研究論文集（8），頁 185-208。
個人資料保護法之總說明及部分條文修正說明，https://www.moj.gov.tw/lp.asp?CtNode=28007&CtUnit=805&BaseDSD=7&mp=001。
徐子捷(2019). 你的希望政府早實現了工研院禁用華為引鄉民許願，總統府：六年前就全面禁用中國手機， 2019 年 04 月 17,取自 https://buzzorange.com/2019/01/15/government-has-banned-to-use-the-phone-from-china-for-six-years/
徐振雄(2010)，網路犯罪與刑法妨害電腦使用罪章中的法律語詞及相關議題探討，國會月刊，第 38 卷第 1 期，台北：立法院。
徐源隆（2003）網路拍賣詐欺犯罪之偵查對策，第七屆資訊管理學術計警政資訊實務研討會。
高信雄(2012)，跨境網路犯罪研究:基於犯罪偵防策略模型，中央警察大學資訊管理研究所碩士論文。
張正芊(2019). 華為 5G 優勢難抵制 歐洲官方民間態度分歧,中央社.
張理國(2019). 陸企產品黑名單陷長考處理原則難產,中國時報.
張樹德，翁照琪（2010），兩岸毒品犯罪型態與防治作為之實證研究，2010 非

傳統安全－反洗錢、不正常人口移動、毒品、擴散學術研討會，桃園：中央警察大學。

教育研究院雙語詞彙、學術名詞暨辭書資訊網(2015)，上網瀏覽時間：2015/10/01, http://terms.naer.edu.tw/。

曹明、程永進、張哲、曹銳生、鄭新傑(2015)，台灣全科醫學模式之我見，上網瀏覽時間：2015/10/05，http://gp.cmt.com.cn/detail/30561.html。

梁添盛(2011)，論警察權限之強制手段與任意手段，中央警察大學學報，48 期，頁 223～260。

畢中和(2019). 美國為何封殺華為？安全只是其一,自由亞洲電台亞洲報導. 2019 年 04 月 17,取自 https://www.facebook.com/RFAChinese/posts/

移民署(2015)，公務統計數據，上網瀏覽時間：2015/10/01, http://www.immigration.gov.tw/ct.asp?xItem=1291286&ctNode=29699&mp=1.

莊忠進（1996）。電腦犯罪偵查與立法之研究，臺北：警專。

許春金（2007）。犯罪學，修訂第五版。臺北：三民。

許春金，陳玉書(2013)。犯罪預防與犯罪分析，二版，台北：三民。

許春金，陳玉書，蔡田木(2015)，中華民國 103 年犯罪狀況及其分析-2014 犯罪趨勢關鍵報告，(法務部司法官學院 104 年委託研究計畫：法務部)，瀏覽日期：2015/11/1，網址：http://www.moj.gov.tw/ct.asp?xItem=392644&ctNode=35595&mp=302

許春金、陳玉書(2013)，犯罪預防與犯罪分析，台北：三民，頁 7-11。

許慈健(2005)，網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究，93-134 頁。

許福生(2016)，犯罪學與犯罪預防，台北：元照。

郭沐鑫(2016). 何謂德國資訊科技安全法(IT-Sicherheitsgesetz), 2019 年 4 月 8 日, 取自 https://stli.iii.org.tw/article-detail.aspx?no=57&tp=5&i=6&d=7598/

郭桓甫(2015)，兩岸人格權之比較研究－以個人資料保護為中心，嘉義：國立中正大學財經法律學研所碩士學位論文，頁 1-141。

陳立昇(2015)，疾病篩檢基本概念，上網瀏覽時間：2015/10/05，http://www.hpa.gov.tw/BHPNet/Portal/File/ThemeDocFile/2007082059425/050427%E7%96%BE%E7%97%85%E7%AF%A9%E6%AA%A2%E5%9F%BA%E6%9C%AC%E6%A6%82%E5%BF%B5_2.pdf。

陳孟君(2016)，WTO 擬參考主要 FTA 架構制定電子商務新規則－以 TPP 電子商務為例，經濟前瞻，第 168 期，頁 97-100。

陳明傳(2007)，跨國(境)犯罪與跨國犯罪學之初探，收於第一屆國土安全學術研討會論文集，桃園縣：中央警察大學。

陳明傳(2015)，各國入出國管理系統之比較研究，發表於中央警察大學移民研究中心 2015 年人口移動與執法學術研討會，桃園縣：中央警察大學。

陳彥驊(2015)，濫用社群網站，人蛇集團效率高，台灣醒報網站，上網瀏覽時間：2015/10/01, https://tw.news.yahoo.com/%E7%A4%BE%E7%BE%A4%E7%B6%B2%E7%AB%99%E4%BE%BF%E4%BD%BF-%E4%BA%BA%E8%9B%87%E9%9B%86%E5%9C%98%E6%95%88%E7%8E%87%E6%8F%90%E5%8D%87-091523250.html。

陳惟凡、陳振楠、伍台國(2016)，電子商務平臺之安全風險評估模式：植基於 ISO27001 資訊安全管理系統與個人資料保護法，電腦稽核，第 34 期，頁 28-42。

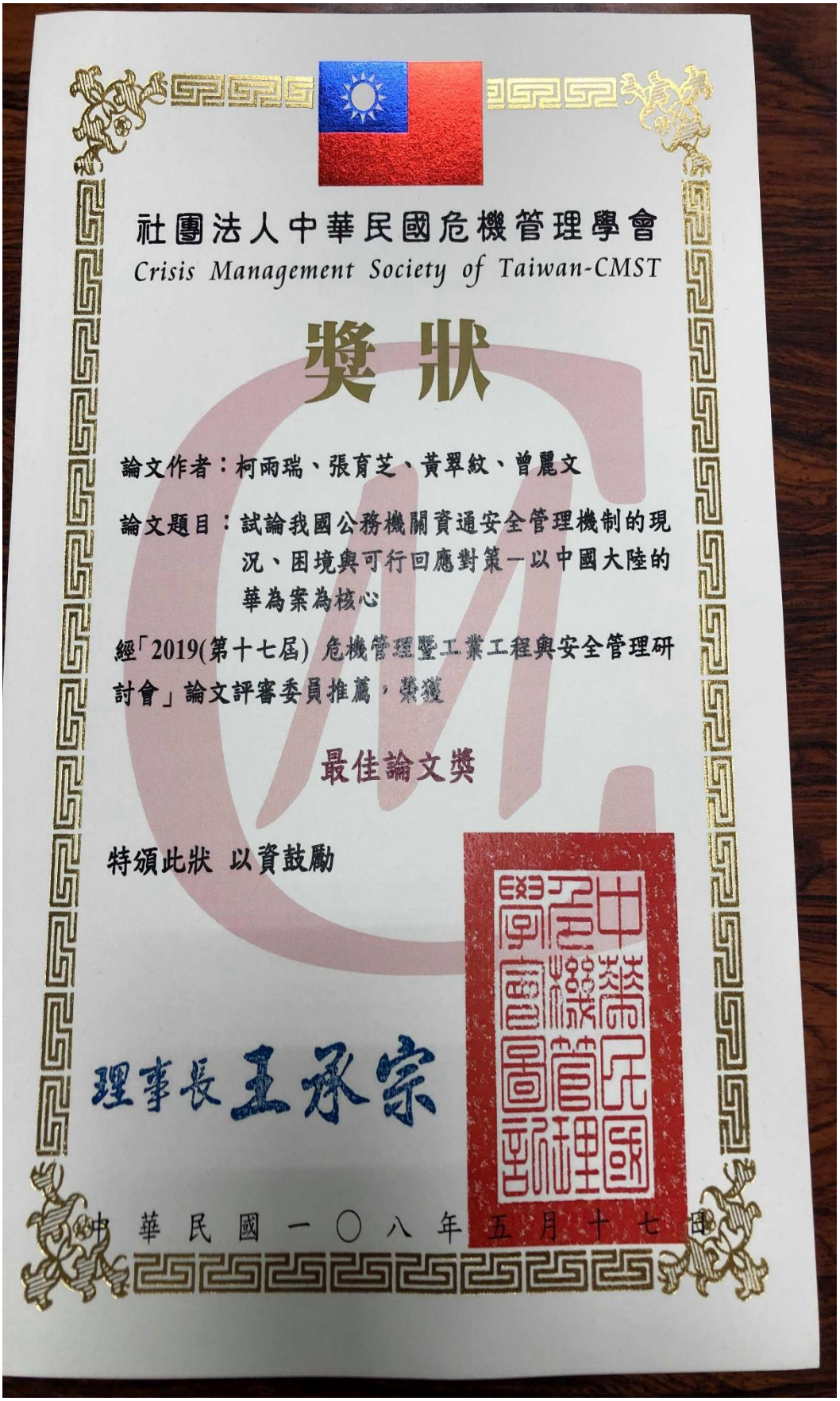
陳嘉玫(2011)， 網路安全的社交工程，科學發展 461 期。
黃有容、王玉樹 (2019) .　憂台企受累工商界籲政府停手,中國時報.
黃明凱（2002），網路犯罪輔助偵查專家系統雛型之建構，中央警察大學資訊管理研究所碩士論文。
黃秋龍(2008)，中國大陸網路犯罪及其衝擊，展望與探索，第 6 卷第 12 期，台北：法務部調查局。
黃登銘(2013)，網路犯罪模式分析與偵查機制之研究－以網路詐欺為例，國立宜蘭大學多媒體網路通訊數位學習碩士在職專班碩士論文。
楊永年、楊士隆、邱柏嘉、李宗憲(2009)，網路犯罪防治體系之政府職能與角色分析，行政院研究發展考核委員會委託國立臺灣大學研究報告。
楊秀莉(2015)，中國內地與澳門網絡犯罪的刑法比較及完善建議，一國兩制研究第 1 期，瀏覽日期：2015/10/27 網址：http://www.ipm.edu.mo/cntfiles/upload/docs/research/common/1country_2systems/2012_1/p176.pdf。
葉雲宏（2008），網路詐欺犯罪被害影響因素之研究，中央警察大學犯罪防治研究所碩士論文。
詹鎮榮(2015)，公務機關間個人資料之傳遞－以臺灣桃園地方法院行政訴訟 102 年度簡字第 2 號判決出發，法學叢刊，第 60 卷第一期，頁 1-25。
資訊工業策進會科技法律研究所(2018) . 日本 2018 年 7 月 27 日發布最新 3 年期網路安全戰略（サイバーセキュリティ戦略）, 2019 年 04 月 08 日, 取自 https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=77&d=8120&lv2=77
資策會科技法律研究所(2015)，加拿大保護加拿大國民遠離網路犯罪法生效，保障國民免受網路霸凌，瀏覽日期：2015/11/12，https://stli.iii.org.tw/ContentPage.aspx?i=6845。
資策會科技法律研究所(2019) . 英國頒布電子通訊之網路與資訊系統規則，2019 年 01 月 18, 取自 https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=77&d=8083。
廖有祿、李相臣（2003）。電腦犯罪-理論與實務，初版一刷。臺北：五南。
廖福村(2007)，犯罪預防，台北：警專。
維基百科(2015)，網路犯罪公約，上網瀏覽時間：2015/10/01, https://zh.wikipedia.org/wiki/%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA%E5%85%AC%E7%B4%84。
網絡安全法的立法定位、立法框架和制度設計(2016)，大陸地區網信網，2016 年 11 月 10 日，http://www.npc.gov.cn/npc/lfzt/rlyw/2016-11/21/content_2002310.htm。
臺南市政府智慧發展中心(2019) . 有關中國華為資通訊產品引發各國資安疑慮與抵制，本府全面盤點所屬資通訊設備，配合中央資通安全政策，全面禁止使用，2019 年 01 月 19，取自 https://www.tainan.gov.tw/News_Content.aspx?n=13371&s=3737475
臺灣地區法規資料庫(2015)，上網瀏覽時間：2015/10/01, http://law.moj.gov.tw/Index.aspx。
劉佐國，李世德(2015)，個人資料保護法釋義與實務—第二版—如何面臨個資保護的新時代，台北：碁峰。
劉邦乾(2012)，海路毒品販運組織及犯罪手法之研究，台北：國立臺北大學犯罪學研究所碩士論文。

數位時代(2016) . 中國強力通過網路安全法,背後沒說的事， 2019 年 04 月 08 日, 取自 https://technews.tw/2016/11/11/behind-china-internet-law/
蔡美智（1998）。電腦駭客入侵的法律問題，資訊與電腦雜誌。
蔡德輝(2009)，犯罪學，台北：五南。
鄧煌發(1997)，犯罪預防，桃園：中央警察大學。
鄧煌發、李修安(2012)，犯罪預防，台北：一品。
鄭厚堃(1993)，犯罪偵查學，中央警察大學出版社，第 1-32 頁。
震宇(1997)，論網路商業化所面臨的管轄權問題（上），資訊法務透析第 9 期，第 18-34 頁
蕭季慧編(1993)，犯罪偵查與蒐集證據，中央警官學校出版社，第 30-38 頁。
蕭美惠(2018) . 美警告台:用華為產品避封殺.， 2019 年 04 月 17, 取自 https://chinatimes.com/newspapers/20181215000222-260202/
蕭徐行(2019) . 蕭徐行觀點歐中峰會談經貿，衝突又合作的相互關係， 2019 年 03 月 18, 取自 https://www.msn.com/zh-tw/news/other/。
賴錦宏(2017)，網路安全法，大陸明天上路，聯合報，2017 年 5 月 31 日，版 A8。
謝立功(2004)，由大陸觀光客脫團事件論我國國境管理機制，展望與探索第 2 卷第 9 期，台北：法務部調查局，頁 14-20。
謝孟珊(2016)，美國電子商務政策與重要法制簡介，科技法律透析，第 28 卷第 4 期，頁 50-69。
鍾張涵(2019) . 川普打壓華為激起愛國商機!那些供應鏈受惠?天下雜誌第 667 期.
鍾錦隆(2018) . 韓儒伯：台灣若用華為設備 對美台合作會有負面影響，2019 年 01 月 18, 取自 https://www.rti.org.tw/news/view/id/2005136。
顏旺盛、陳松春(2011)， 迎接 21 世紀跨境犯罪之挑戰， 刑事雙月刊 39 期，第 57-60 頁。
羅婷婷(2018) . 華為產品藏間諜晶元？日本曝光重大證據，2019 年 02 月 18, 取自 https://www.ntdtv.com/b5/2018/12/11/a102463552.html。
羅綺(2019). 微軟工程師 揪出華為筆電後門，2019 年 01 月 18, 取自 https://ec.ltn.com.tw/article/paper/1278552。
譚淑珍(2019) . 禁用華為， 許勝雄:民間企業自有防範機制,中時電子報.
蘇芳禾(2019) . 資料庫後門恐通中國 林昶佐爆 8 成部會未評估，2019 年 02 月 18, 取自 https://news.ltn.com.tw/news/politics/breakingnews/2761622。
蘇柏毓(2016)，104 年之個人資料保護法修正簡評，科技法律透析，第 28 卷第 4 期，頁 13-17。

(2)英文資料
American Government. (2010). Comprehensive National Cybersecurity Initiative(CNCI), Technical report, Retrieved April 19 , 2019, from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf.
Bart van der Sloot & Sascha van Schendel(2016). Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study. Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC), Vol. 7.
Britz, Marjie T.(2009). Computer Forensics and Cyber Crime : An Introduction, Second Edition.USA: Prentice Hall.

Clough, D.(2010). Principles of Cybercrime. UK: Cambridge University.
Council of Europe(2015), “Convention on Cybercrime”, Retrieved on 2015/10/02, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=11&DF=6/21/2007&CL=ENG.
Data Protection Act 1998(1998), legislation.gov.uk, 1988/7,http://www.legislation.gov.uk/ukpga/1998/29/contents.
Evans, K. (2011). Crime Prevention: A Critical Introduction. USA: SAGE Publications Ltd.
Fennelly, L. & Crowe, T.(2013). Crime Prevention Through Environmental Design, Third Edition.USA: Butterworth-Heinemann.
Frederick, C.(2010). Information assurance technical framework. Release 3.1. National Security Agency, Retrieved February 19 , 2019, from https://www.iad.gov/library/ -iacf.cfm .
Lab, P. (2013). Crime Prevention: Approaches, Practices, and Evaluations. 8th Edition. USA: Routledge.
Mackey, D & Levan, K(2011). Crime Prevention. USA: Jones & Bartlett Learning.
Public Safety Canada(2011), Bi-National Assessment on Trafficking in Persons , Public Safety Canada,https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-ssssmnt-trffckng-prsns/index-en.aspx.
Reyes, A. (2007). Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors.USA: Syngress.
Schneider, S.(2014). Crime Prevention: Theory and Practice, Second Edition. USA: CRC Press.
The United States Department of Justice(1974), “Privacy Act of 1974,”https://ww-w.justice.gov/opcl/privacy-act-1974.
Todd, G. & Bowker, A. (2014). Investigating Internet Crimes : An Introduction to Solving Crimes in Cyberspace. USA: Steven Elliot.
Twelfth United Nations Congress on Crime Prevention and Criminal Justice(2015), “Working paper prepared by the Secretariat on recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, A/CONF.213/9”, Retrieved on 2015/10/02, http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/V1050320e.pdf .

附錄：相關照片



社團法人中華民國危機管理學會
Crisis Management Society of Taiwan-CMST

獎狀

論文作者：柯雨瑞、張育芝、黃翠紋、曾麗文

論文題目：試論我國公務機關資通安全管理機制的現況、困境與可行回應對策－以中國大陸的華為案為核心

經「2019(第十七屆) 危機管理暨工業工程與安全管理研討會」論文評審委員推薦，榮獲

最佳論文獎

特頒此狀 以資鼓勵

理事長 王承宗

中華民國一〇八年五月十七日

2019(第十七屆)
危機管理暨工業工程與安全管理
學術研討會審稿通知

2019 年 4 月 30 日

論文編號： CCM190517381
論文題目： 試論我國公務機關資通安全管理機制的現況、困境與可行回應對策---以中國大陸的華為案為核心
作　　者： 柯雨瑞、張育芝、黃翠紋、曾麗文

先生/女士大鑑,

經危機管理學術研討會審稿委員審議，您的投稿論文已獲推薦發表，特函通知。有關論文發表之場次、時間及地點將另行通知。

論文品質(分為：優佳可差)					
原創性	完整性	文獻回顧與引用	文字圖表格式與清晰度	論文架構	綜合意見
佳	佳	優	佳	佳	□不推薦 ■推薦發表 □修正後推薦發表

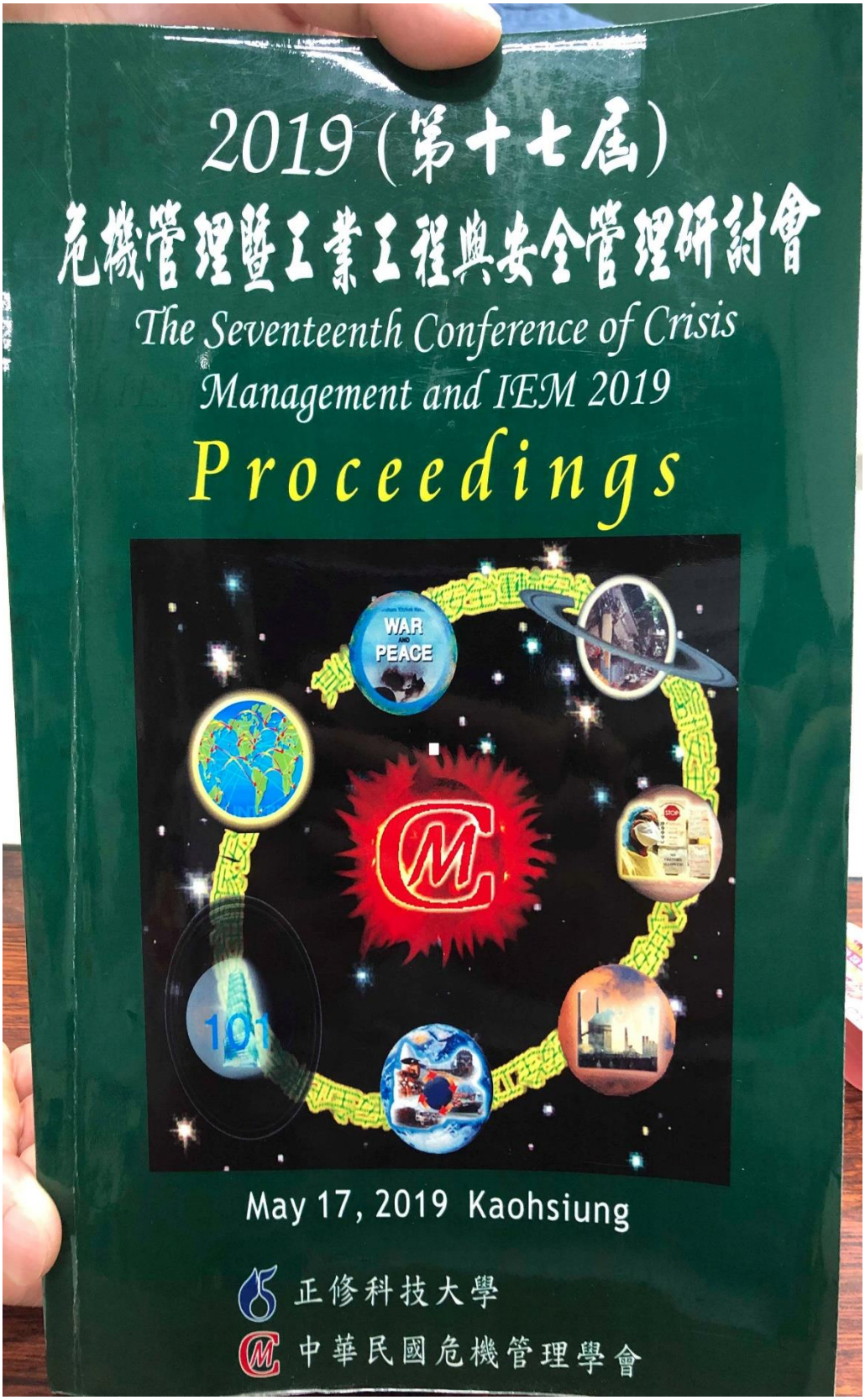
● 格式與內容之審稿結果

1. 論文主題符合本研討會主旨。
2. 質性研究難度甚高，資安問題舉世皆然，台灣公務機關是認知不足或因應能力不足尚無定論，可確定的是絕對刻不容緩，應積極因應。
3. 文獻探討確實引用恰當。
4. 政府與民間之資安規範有相當落差，政府要兼顧國安、資安與經濟發展確實不易，本文將現況困境與可行因應對策作一基本探討、梳理，極具參考價值，並強烈建議相關議題，應再持續其廣度與深度進行後續研究。


危機管理暨工業工程與安全管理學術研討會


正修科技大學
工業工程與管理系


機制之現況
之法制現況
全管理法」規
機關，以風險
及應變計畫，
外，另外，尚
電信法、電子
護法、金融控股
庫管理條例等


2019 (第十七屆)
危機管理暨工業工程與安全管理研討會
The Seventeenth Conference of Crisis Management and IEM 2019
Proceedings
WAR AND PEACE
May 17, 2019 Kaohsiung
正修科技大學
中華民國危機管理學會

2019(第十七屆) 危機管理暨工業工程與安全管理研討會 高雄，中華民國108年5月17日
The Seventeenth Conference of Crisis Management and IEM 2019 Kaohsiung, Taiwan, May 17, 2019

試論我國公務機關資通安全管理機制的現況、困境與可行回應對策 －以中國大陸的華為案為核心

A Study On the Current Situations, Dilemmas, and Feasible Response Countermeasures for the Information and Communication Security Management Mechanism of the Public Administration Organizations of the R.O.C－Focusing on the Information and Communication Products of the Huawei Company of the Mainland China

柯雨瑞[1]、張育芝[2]、黃翠紋[3]、曾麗文[4]
Y. R. Ko[1], Y. C. Chang[2], T. W. Huang[3] and L. W. Teng[4]
[1]中央警察大學 國境警察碩士班專任教授
[2]台南市政府警察局 第五分局行政組巡官
[3]中央警察大學 行政警察研究所專任教授兼所長
[4]彰化縣警察局 彰化分局實習所長、實習巡官

摘要

「華為」資通事件，業已成為全球熱門之議題，全球各國因為資訊安全與 5G 網路未來之挑戰，各國有不同之意見與表態。然而我國面臨「華為」之問題，中央與地方機關之現況與困境為何？又有何種可行之解決對策？本文一共分成 4 大點來探討，首先探討各國現行之資通安全管理法制現況、我國公務機關資通安全管理之法制現況、我國公務機關資通安全管理機制之困境以及我國公務機關資通安全管理機制之可行回應對策，期待能為我國公務機關資通安全管理之機制，提出可行之方案與建議，藉以精進我國公務機關資通安全管理之量能。

關鍵字：資訊安全、陸資產品(華為手機)、國家安全、第五代行動通訊技術(5G)。

ABSTRACT

The "Huawei" telecommunications equipment products have formed a global issue. Countries have different opinions and attitudes between their national security policy and the future challenges and commercial merits of 5G networks. However, what are the current situations and predicaments facing by the central and local authorities in dealing with the "Huawei" telecommunications equipment products in Taiwan? What are the suggested , feasible and nice solutions to this issue? This paper has listed four major points to discuss about this issue. Firstly, it discusses the current legislative policy of the national security in different countries such as the United States, Germany, Japan, China, South Korea and European Union of the world. Secondly, analyze the current status of our national security defense network in our central and local government. And what kinds of struggles and dilemmas facing by our government should be solved? Finally, this article suggested some feasible recommendations to solve this significant and complicated issue.

Keywords: Technology Security; Huawei Telecommunications Equipment; National Security; Critical Information Infrastructure (CII)

2019(第十七屆)危機管理暨工業工程與安全管理研討會

中華民國 108 年 5 月 17 日出版發行

編　著　者：社團法人中華民國危機管理學會

發　行　人：王　　承　　宗

出　版　者：社團法人中華民國危機管理學會

電　　話：07-6295322

劃　　撥：42164016

住　　址：高雄市橋頭區德松村成功北路 113 巷 2-1 號

登　記　證：

ISBN：978-986-96420-0-2