

2021 年第 24 屆資訊管理學術暨
警政資訊實務研討會
——「運用智慧科技創新警政服務」

論文集

目 錄

大會組織.....	I
序言.....	II
1 區塊鏈在交通事故數位證據保全上的應用 (王逸嵐、董正談、鄧少華).....	01
2 我國不能安全駕駛之酒精濃度與肇事實證研究(吳國清).....	11
3 能載舟亦能覆舟之文字隱碼研究(吳國清).....	25
4 疫情下的 VDI 替代方案(范修維、郭明煌).....	41
5 惡意程式分析流程之研究(郭明煌、廖鴻圖、林翔哲).....	48
6 智慧型警車攔截圍捕輔助系統之研究(古淳寶、董正談、鄧少華).....	57
7 The influence and strategy of the development of artificial intelligence on law enforcement agencies(鄭宇森).....	68

**2021 年第 24 屆資訊管理學術暨
警政資訊實務研討會
——「運用智慧科技創新警政服務」
大會組織**

大會主席：

陳校長擇文

大會副主席：

蘇副校長志強

籌備及議程委員會主席：

黃主任勝源

廖主任有祿

籌備委員：

黃主任勝源、廖主任有祿、王教授朝煌

吳教授國清、鄧教授少華、王教授旭正

林教授曾祥、顏副教授志平

董助理教授正談

執行秘書：

簡助教羚茜

序 言

本校與內政部警政署為促進資訊管理學術與警政資訊實務之交流，結合資訊管理學術與警察資訊實務工作，期經由警察資訊應用技術的開發來提昇警察工作效能，進而促使警察能夠採取更經濟有效的方法來服務社會。為具體落實此項目標，本校定期舉辦資訊管理學術暨警政資訊實務研討會，期能藉由舉辦研討會交流學術研究成果與實務經驗智慧，共同研討尋求解決方案。此外有鑒於資訊科技不斷地創新應用與發展，資訊科技不但已經成為現代化社會、生活與工作的必備利器，更讓我們能夠突破時空的侷限來進行過去無法完成的事項；而社會環境不斷地變遷，對於警察角色的定位也有所轉變，已經從法律與治安的維護者，擴大為社會與民眾的服務者，因此如何整合並運用資通訊科技來維護治安與打擊犯罪，並以創新的思維來面對警察工作的挑戰已成為迫切的課題。本次研討會主題為「運用智慧科技創新警政服務」，相信在各位作者的熱情參與下，對於警察資訊人員如何以創新的思維跟上時代的脈動並順利完成各項警察工作，將會有更宏觀的認識與啟發。

論文發表部份，本屆研討會因疫情關係，改為線上發表方式，總計刊登 7 篇文章，分別探討「區塊鏈在交通事故數位證據保全上的應用」、「我國不能安全駕駛之酒精濃度與肇事實證研究」、「能載舟亦能覆舟之文字隱碼研究」、「疫情下的 VDI 替代方案」、「惡意程式分析流程之研究」、「智慧型警車攔截圍捕輔助系統之研究」、「The influence and strategy of the development of artificial intelligence on law enforcement agencies」，涵蓋學術與實務領域，契合本研討會之宗旨。

本屆研討會得以順利舉辦，首先要感謝陳校長、蘇副校長、林院長以及各級長官的鼎力支持與協助，為資訊管理學系添購各項軟硬體設備，並充實教學與研究環境，其次感謝本系所有教師以及學校各單位同仁通力合作共襄盛舉，並感謝本系簡羚茜助教及所有在幕後任勞任怨付出與幫忙的所有審查委員們，最後感謝各位先進、前輩、校友以及警界同仁的熱情參與，希望藉由大家的參與交流集思廣益，能夠進一步提昇國內資訊管理學術與警政資訊實務的發展與研究水準。

中央警察大學資訊管理學系主任廖有祿敬序

中華民國 110 年 6 月 1 日

區塊鏈在交通事故數位證據保全上的應用

王逸嵐

中央警察大學資訊管理所研究生

im1093062@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授

tung@mail.cpu.edu.tw

鄧少華

中央警察大學資訊管理所教授，通訊作者

pdeng@mail.cpu.edu.tw

摘要

交通與治安為警察工作之核心，面對交通事故時，適當運用資訊科技，能有效提升工作效率、重建交通事故現場。鑑於車輛普及率逐漸上升，使交通事故發生機率亦隨之增加，因此交通事故處理後之數位證據保全重要性不可忽視，而現今研究多著重於刑事證據之保全，未對交通事故數位證據進行研究。交通事故數位證據如現場照片、行車影像畫面、筆錄之錄音錄影檔等皆為駭客攻擊之目標，或是交通事故之當事人賄賂交通事故處理流程之相關員警竄改或刪除數位證據，致使警方製作錯誤的道路交通事故初步分析研判表，影響民眾民事、刑事及行政責任，因此交通事故現場之重建，除了要即時蒐集行車影像畫面與現場照片外，還需要確認及驗證行車影像畫面與現場照片之內容是否正確。交通事故現場之證據如同刑事案件，須做好證據監管鏈，確保交通事故相關數位證據從民眾交由警方，及警方交給行車鑑定委員會的過程中，未遭受任何竄改、刪除或變更，才能有助於交通事故的重建及行車鑑定委員會製作鑑定意見書。本研究引入區塊鏈技術建構跨單位間的數位證據交換系統，以區塊鏈之去中心化、分散式帳本無法遭竄改等特點，確保資料的完整性與安全性；採用智能合約，使其能夠以角色為區分彈性設定其權限控制，符合不同單位的需求，協助交通事故處理流程之相關人員能夠節省檢驗證據之時間，並有效識別出有證據價值的交通事故數位證據，確保證據一致性、完整性、不可竄改性，提昇交通事故鑑識之品質。

關鍵字：證據監管鏈、數位證據、區塊鏈。

一、前言

交通事故與刑事案件之不同，就現場處理部分而言，交通事故現場不能長時間大範圍封鎖採證、處理人員不如刑事鑑識人員專業、人力亦不足，反之刑事案件現場可長時間保留，因此多利用交通事故現場照片將易消失之跡證、人事物相關位置與車體損壞碰撞情形進行紀錄，並進行現場測繪、肇事車輛調查、路面跡證調查及筆錄詢問等文字敘述的書面資料，為現場照片之輔助資料。

現今研究多著重刑事案件之數位證據保全與交換，但交通事故數位證據之重要性卻被忽略，如交通事故數位證據（現場照片、行車紀錄器影片、筆錄詢問之錄音錄影檔）遭人為竄改、刪除或變更，或是發生意外、天災等導致數位證據毀損或變更，將嚴重影響民眾之民事、刑事及行政責任之歸屬。依據交通部道路

交通安全督導委員會統計109年全國交通事故發生件數為362,259件[19]，交通事故有逐年上升之跡象；而警政署公布之109年刑案總數為259,713件[18]，刑案發生率逐年下降，可知交通事故件數遠遠高於刑案件數，但目前研究多著重於刑案證據，而忽略交通事故數位證據保全之重要性，如遭有心人士對交通事故數位證據執行惡意操作，將對民眾權益造成巨大影響，因此重視交通事故之數位證據保全刻不容緩。

目前科技發展，多以資料庫解決單位間管理資訊問題，卻無法實現單位間可信、可靠資訊管理、高效能合作及共享，且資料庫無法詳細追蹤資料歷程，存在資訊不對稱問題，導致黑箱問題。除此之外，資料庫為主從式架構，只有單一伺服器端，中心節點的處理效能有

限，往往會造成網路的瓶頸，當中心節點發生故障時，整個系統皆會癱瘓。

以交通事故處理為例，事故一方當事人如對行車影像畫面、交通事故現場照片及「道路交通事故初步分析研判表」(以下簡稱初判表)之正確性提出質疑，影像是否遭受到竄改或變更，影響肇事責任之歸屬，尤其是現今最流行 Deepfake 技術，如被有心人士運用於交通事故，將導致警方製作錯誤的初判表，嚴重影響相關當事人權益。初判表由警察機關進行判斷製作，因此「初判表僅供參考，不具任何法律效益」。如當事人對初判表有疑異，或想更深入了解交通事故的主、次要肇因，可向「車輛行車事故鑑定委員會」(以下簡稱車鑑委員會)申請鑑定意見書。而行車紀錄器畫面證據，如在事發時有交給處理的警察，原則上警察機關會直接提供給車鑑委員會，因此在行車影像傳輸時亦可能遭受竄改，如何確保其證據力，是警方未來的一大課題。

為補足資料庫管理系統功能上不足，本研究目的在於針對交通事故數位證據提供一個證據保全架構與方法，使證據轉移時能保持來源狀態，依循數位證據監管鏈基本原則，協助交通事故處理各流程人員提升調查效率及製作更有證據價值之初判表或鑑定意見書。為確保所取得及製作之交通事故數位證據之證據力，防止遭有心人士惡意竄改，本研究以區塊鏈方式將交通事故數位證據加密上傳區塊鏈，搭配分散式資料庫，確保資料完整性，提升其證據力，是重建交通事故現場之關鍵。區塊鏈將所有網路參與者視為對等者，打破中心伺服器的傳統，改為依賴參與者共同維護網路結構，具有極強的可靠性，單一或少量節點故障都不會影響系統運作。密碼學讓鏈上資料以加密方式存在，藉由智能合約設定只有相關的交易用戶可以在設定權限內讀取加密資料，使區塊鏈具備防竄改及可追溯特性，讓資料難被修改或抹除，並可追溯全部資料的歷史紀錄。區塊鏈所具有完整性、歷史性與一致性的優勢正好符合數位證據監管鏈的需求[16]。

二、文獻探討與基礎知識

1. 證據監管鏈 (chain of custody)

證據監管鏈原則，指數位證據在識別、蒐集、擷取、封緘與運送過程中，需要確保數位證據的一致性、完整性，有明確的紀錄保存，

避免數位證據遭到污染。換言之，證據監管鏈是用於記錄與維護證據時間歷史的過程[14]。數位證據蒐集須滿足三點共通性原則：i. 確保數位證據未受外力影響、ii. 執行人員須有專業能力、iii. 完整記錄證據監管鏈。

(1) 數位證據特性

數位證據並非可直接察覺的具體存在事物，通常以電磁或電波方式儲存於電子媒體上，透過電子設備加以讀取、分析及顯示，呈現為視覺可判讀之資訊型態。數位證據具備易消失、不易取得蒐集、易偽造、難保存及不易證明所擷取之證據與原始狀態相同，難以被民眾、司法機關採信，因此需透過資訊科技確保數位證據之公信力及證明力。故，數位證據具備(A)無限複製及無差異複製、(B)不著痕跡增刪修改、(C)復原可能性、(D)不易製作人確定、(E)無法以人之知覺直接認識、理解其內容及(F)對環境具有依賴性等六種特性[1][5]。

(2) 證據能力

指可作為證據之資格，依刑事訴訟法第154條2項規定：「犯罪事實應依證據認定之，無證據不得認定犯罪事實。」因此，能證明犯罪事實之證據，必須先具備證據能力，在經過合法調查程序，依法官自由心證決定其證據之證明力程度。

2. 區塊鏈

「區塊鏈」最早於 2009 年由中本聰在「比特幣：一種點對點的電子現金系統」中所提出，指依據 P2P 網路、密碼學技術、時間戳技術、區塊鏈技術等的電子現金系統的構架理念而產生比特幣[15][17]。

(1) 區塊鏈定義

依《區塊鏈技術和應用發展白皮書2016》解釋，狹義區塊鏈指一種按照時間順序將數據區塊以順序相連的方式組合成的一種鏈式數據結構，並以密碼學方式保證不可竄改和不可偽造的分散式帳本；廣義區塊鏈指利用區塊鏈之數據結構來驗證和儲存數據、利用分散式節點共識演算法來產生和更新數據、利用密碼學的方式保證數據傳輸和存取的安全性、利用自動化指令碼程式碼組成的智能合約，以程式設

計和運算元存取的一種全新的分散式基礎架構與計算範式。

區塊鏈網路的構成要素說明如下[2]：

- (A) P2P：指網際網路上的電腦或伺服器互相連結通訊的網路，在多個不特定節點間建立通訊。所有端點是請求檔案的客戶端，亦是回傳檔案的伺服器端，彼此是對等關係，非主從關係。
- (B) 區塊鏈網路的參與者：實際連結上網路的是電腦或是伺服器等節點，可再將參加網路對象分為使用者與礦工。使用者負責傳送虛擬貨幣，執行匯款；礦工負責產出區塊，以獲得虛擬貨幣為報酬。
- (C) 交易：交易中包含匯款人、收款人及金額等資訊。使用者進行虛擬貨幣匯款時所發出的命令，並透過各節點傳遞廣播。
- (D) 區塊(block)：由礦工所產出，在區塊中存有多筆交易，主要目的是保障交易資訊的安全。
- (E) 分散式帳本：所有被傳遞的區塊會儲存在各節點的分散式帳本（資料庫）中，即使其中一個節點故障，亦可從其他節點的帳本來確認交易情形。每個區塊會保存上一個區塊的資訊（雜湊值），使區塊如同鏈狀方式互相連結，形成區塊鏈。
- (F) 挖礦：礦工運用大量計算能力互相競爭產出新區塊的行為。

(2) 區塊鏈基礎技術

(A) 雜湊運算

將任意長度的輸入值藉由一定的計算，產生出一個固定長度字串，即為輸入值的雜湊值。如SHA-256為常用之雜湊函數，代表其輸出值長度為256bit（32byte）。主要用來驗證所傳送訊息的正確性，避免訊息於傳送過程中遭竄改，輔助安全機制裡的鑑定性需求[3]。

雜湊運算之三大特性如下：

- ① 又稱單向函數，具不可逆性，難以從雜湊值反推原始輸入值。
- ② 不論輸入值長度為何，輸出值皆為固定長度。
- ③ 原則上不會發生不同輸入值卻產出相同輸出值的情況。

(B) 數位簽章

數位簽章指依附於電子文件中，用來確認及辨識電子文件的發送者的身分與電子文件的真假，功能與親筆簽名相似。數位簽章使用

非對稱式密碼系統，每位使用者有一對金鑰，一把為私密金鑰，另一把為公開金鑰。私密金鑰不可對外公開，用於對電子文件簽署，接收電子文件者利用發送者之公開金鑰驗證數位簽章的有效性。

數位簽章有以下特質[6]：

- ① 可鑑定訊息發送者之身分與簽章之日期、時間。
- ② 可由第三方進行驗證確認，發送者無法否認曾簽署過文件。
- ③ 簽章具唯一性，無法被偽造。
- ④ 被簽章之文件具完整性，無法被竄改。
- ⑤ 簽章易產生、易辨識、易驗證。

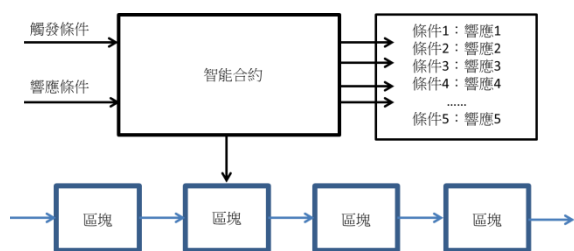
(C) 共識演算法

區塊鏈所有節點皆參與記錄數據，為確保節點都記錄同一份的正確數據，避免惡意節點故意阻礙訊息傳遞或傳送假數據，須採用共識演算法。

工作量證明(Proof of Work, PoW)，指所有節點互相競爭記帳權，對每一次的記帳（產出區塊）都給予一個「難題」，能解出難題的區塊才算有效，並將有效區塊以最長鏈原則結合。難題，具有難以解答但容易驗證正確性，其難度（平均的解答時間）可透過控制難題中的部分參數調整。解決難題即尋找一個隨機值的過程，區塊中Nonce欄位即為難題的解答[8]。

(D) 智能合約

1995年學者Nik Szabo提出智能合約概念，定義為「一個智能合約是一套以數字形式定義的承諾，包括合約參與方可以在上面執行這些承諾的協議。」換言之，智能合約是一種能自動執行的電腦程式。Solidity是編寫智能合約之高階語言，能免於直接編寫在以太坊虛擬機底部之程式碼，使合約程式碼更容易維護。智能合約若部署在區塊鏈，所有節點皆會依既定邏輯執行。運用於區塊鏈的智能合約含事務處理機制、資料儲存機制以及狀態機，用於接收和處理各種條件，而事務的觸發、處理及數據保存都必須在鏈上進行。當達成觸發條件時，智能合約會根據設定之邏輯，採取相對應措施，並將結果永久保存於鏈上（圖一）[11]。



圖一：區塊鏈上的智能合約運作模式

(3) 區塊結構

區塊中除了交易資料或連結前一區塊的連結外，還儲存許多資訊[4]，其結構如表一。

表一：區塊的結構

區塊欄位	說明
Block Size	從下一個欄位到區塊最末端的資料容量
Block Header	區塊標頭的資訊
Transaction Counter	區塊內含的交易數量
Transactions	交易清單

區塊標頭欄位	說明
Version	軟體/協定版本資訊
Previous Block Hash	父區塊的雜湊值
Merkle Root	Merkle Tree的根雜湊值
Timestamp	區塊產出時間
Difficulty Target	區塊產出時的PoW難度，雜湊值必須小於它
Nonce	計算雜湊所使用的值

(4) 區塊鏈運作機制

區塊鏈架構是由許多區塊所連接而構成。每一區塊中，交易紀錄(transaction)代表區塊所攜帶的數據，如比特幣。交易紀錄代表比特幣由A使用者轉送到B使用者的紀錄，交易紀錄的資料儲存內容會隨著應用於不同的場合而有不同。區塊間連接的方法，是透過每一區塊中包含前一個區塊的雜湊值，形成區塊鏈。換言之，一種由許多個區塊所構成的資料鏈稱為區塊鏈[7]。

(5) 區塊鏈發展歷程

區塊鏈發展歷經加密虛擬貨幣、滿足企業應用及互聯網應用，其說明如下[9][13]：

(A) 區塊鏈1.0：加密虛擬貨幣

主要應用聚集於加密虛擬貨幣領域，典型代表為比特幣，建構一個去中心化、透明公開及防竄改的帳本系統。但比特幣在全球範圍內僅能支援每秒七筆交易，交易記帳後追加六個區塊才能被認為是安全交易，而追加一個區塊約十分鐘，表示一小時才能確認交易，因此無法即時滿足要求較高的應用需求。

(B) 區塊鏈2.0：企業應用

解決區塊鏈1.0之效能問題，增加群眾募資及溯源應用，支援智能合約，降低社會交易間的信任成本，提高行業間及行業內的合作效率，典型代表為以太坊系統。智能合約，是藉由電腦實現的，以數字方式達成共識、履約、監控及驗證結果的自動化合約，大幅擴充區塊鏈的功能。以太坊系統將產出區塊鏈之時間縮短為15秒，提升區塊鏈效能，滿足大多數應用，使區塊鏈技術擴大至公證、物流、投票等領域。

(C) 區塊鏈3.0：價值網際網路

從技術角度，應用CA認證、數位存證、電子簽名、識別生物特徵、分散式計算儲存，使區塊鏈實現去中心、公開透明、防竄改可追蹤的平台，建構一個可信社會。雲端計算、人工智慧、大數據與區塊鏈等技術，促進網際網路與實體經濟結合，重建數位經濟發展。

(6) 區塊鏈分類

根據參與節點特性、網路範圍、設計結構及功能，區塊鏈被分類為公有鏈、聯盟鏈及私有鏈等三種[9][12]。

(A) 公有鏈

公有鏈指任何人皆可維護區塊鏈與讀取其內容，無須透過中央機構，資料完全公開透明。公有鏈系統因無中央機構，須依照事先設定之規則在公開網路環境下，建構出可被信任的網路系統。目前，虛擬貨幣系統及群眾募資系統皆為公有鏈。

在公有鏈中，因無法確定節點數，無法得知節點實際身分，可能被擁有大量運算能力的惡意者進行51%攻擊，因此公有鏈採用共識演算法及P2P達成資料同步，確保資料一致性。

公有鏈存在之問題如下：

- ①隱私問題：因公有鏈上資料的傳輸及儲存都是公開可見，僅透過密碼學將交易雙方進行隱私保護，但其他參與者仍可以透過分析交易紀錄取得有用之資訊。
- ②效率問題：區塊鏈存有分岔問題，可能會導致剛產生的區塊被還原，因此，在公有鏈中，每個區塊都需等待若干個（約6個）後續區塊產生，才能夠被認為是安全區塊，而這段時間約1小時。
- ③最終確定性：因公有鏈無法提供即時確定性，即使交易被寫入區塊也可能發生還原，無法確定交易是否最終會被包含進區塊中。

(B) 聯盟鏈

建構於多個互相已知身分的組織間，需要嚴格的身分認證及許可權管理，在一段時間內的節點數量是確定的，適用於組織間需達成共識的業務，其代表為Hyperledger Fabric系統。

聯盟鏈之特點如下：

- ①效率提升：定義參與者身分及驗證管理規則，在一定時間內參與方個數確定且節點數量小於公有鏈，對於共同實現之業務已具有一致理解。
- ②較佳隱私保護：資料僅在聯盟成員內開放，即使在同一聯盟內，不同業務之資料也會區隔。如華為公有雲端的區塊鏈服務提供同態加密，對交易金額資訊進行保護，透過零知識證明，對身分進行保護。
- ③無需激勵制度：參與者為了共同的利益而進行配合，因此自願貢獻運算能力、儲存，不需額外的獎勵機制。

(C) 私有鏈

指不對外開放，僅在組織內部使用，具備完善許可權管理系統，並對使用者進行身分認證，屬部分去中心化。因此，參與者的數量與節點狀態通常為確定的、可掌握的，且節點數量小於公有鏈。相較於資料庫，私有鏈的最大好處是加密審計與自證清白能力，無人可輕易竄改資料，即使遭竄改也能追溯到責任方。

私有鏈之特點如下：

- ①效能更高：同一組織內已具備信任機制，可採用非拜占庭容錯，即時進行確認的共識演算法，因此確認延遲時間及寫入速率提高，甚至與中心化資料庫的效能相當。
- ②更佳的隱私保護：私有鏈大多位於組織內部，可利用原有組織的資訊安全防護機制，能提供更佳的安全保護。

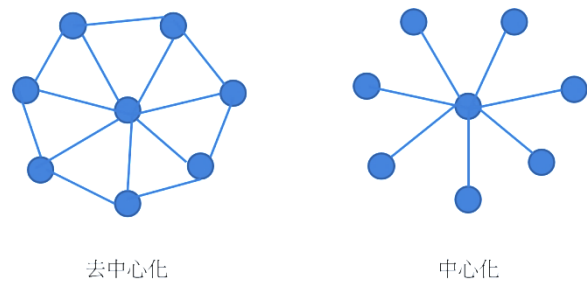
(7) 區塊鏈特性

由多種技術集合而成的創新技術區塊鏈，實現高效能合作與多方信任，具備以下四大特性[10]。

(A) 公開透明可信

去中心化系統中，所有節點均對等地發送與接收網路中所傳遞之消息。因此，每個節點皆可觀察系統中節點的所有行為，並在各節點進行記錄，共同維護帳簿，使系統對節點具有透明性。相對於中心化系統，節點間存有資訊不對稱之行為，中心節點具掌控權，恐導致黑

箱作業。去中心化及中心化網路之對比圖如圖二。



圖二：去中心化及中心化網路之對比圖

區塊鏈中，節點們會藉由共識演算法讓帳本保持一致性，整個系統皆透明、公平，使訊息具備可靠信。

(B) 防竄改，可追溯

防竄改，指交易在網路範圍內經過共識演算法驗證並增加至區塊鏈，就難以被修改或刪除。若要進行竄改，需要掌握系統大部分（51%）的運算能力，一旦發生攻擊，此區塊鏈系統將不再被相信且失去價值。防竄改，不等於區塊鏈上紀錄之內容不能被修改編輯，而是編輯過程將被完整記錄，如同日誌般，但此日誌是不能被修改。

可追溯，指區塊鏈上發生的交易皆有完整紀錄，保證寫入區塊鏈之交易難以被竄改。

(C) 匿名性，保障隱私安全

區塊鏈以公私鑰系統中之私鑰作為身分標示，用戶以私鑰參與區塊鏈上之交易，使節點間不須公開身分即可進行有效的交易，為用戶隱私提供安全保障。

密碼學為用戶提供更多保障，同態加密及零知識證明讓鏈上資料以加密形態存在，非相關用戶無法從密文中讀取訊息，只有相關交易用戶能在權限範圍內讀取密文訊息，為用戶隱私增加保障。

(D) 去中心化，系統高可靠

區塊鏈中每個節點都對等維護系統帳本並支持拜占庭容錯，即使部分節點故障依然能正常運作。嚴格來說，區塊鏈系統之可靠度非絕對，只是在滿足其錯誤模型的要求下，保證系統的可靠性，但因區塊鏈中節點數眾多，使錯誤模型要求能完全被滿足，因此認為區塊鏈具高可靠性。

三、 解決方案—交通事故數位證據區塊鏈

1. 交通事故數位證據及其處理流程

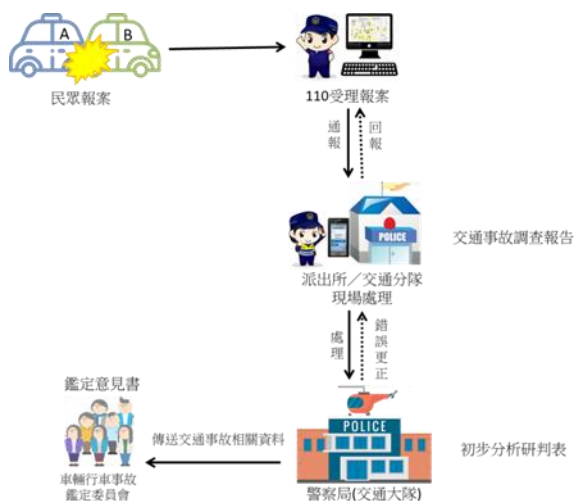
1.1 交通事故數位證據

數位證據指在電子設備中，以數位方式儲存而可用以佐證事實之資料，交通事故處理之數位證據有以下：

- (A) 交通事故現場照片。
- (B) 行車影像畫面。
- (C) 周遭監視錄影畫面。
- (D) 調查訪問表或筆錄訊問之錄音、錄影檔。
- (E) 道路交通事故現場圖。
- (F) 現場蒐證之錄音、錄影檔。

1.2 交通事故處理流程

交通事故發生時，由派出所或交通分隊員警至現場處理交通事故，將所蒐集或製作之相關資料(如現場照片、行車影像畫面、現場圖、道路交通事故調查報告表…)傳輸至警政知識聯網，再由交通大隊依所接收之資料製作初步分析研判表，並依民眾申請交付初判表。民眾如不服初判表內容，可於事發六個月內向車鑑委員會申請鑑定意見書(圖三)。



圖三：交通事故處理流程圖

傳統交通事故處理流程，現場員警傳輸交通事故相關資料至警政知識聯網後，如有內部員警遭受交通事故相關當事人賄賂，將不利當事人之證據刪除，或利用現今最流行技術Deepfake竄改數位影像資料，將嚴重影響交通事故肇責分析，關乎當事人民事、刑事、行政責任之歸屬，影響民眾權益甚鉅，為提升交通事故審核之正確性與品質，與警察機關之正面形象，應進行作業系統上更改。除此之外，傳統的交通事故紙本資料，隨著時間增加，累積的交通事故案件數量亦會增加，紙張數量龐

大，因紙張會受潮發霉或泛黃而有保存困難問題。

交通事故審核小組員警並未至交通事故現場，而是交通事故現場處理員警目睹整個交通事故現場，再透過現場處理員警傳送之交通事故相關數位證據分析肇事原因，製作初判表，因此對於交通事故相關數位證據之保全相當重要。

2. 區塊鏈在交通事故數位證據保全上的應用

將電子設備(行車影像紀錄器、手機)所錄影或拍攝之影像畫面、數位資料，藉由演算法取得雜湊值導入區塊鏈中，利用智能合約設定及管理使用者權限，且使用者在鏈上的所有行為皆會被記錄，使數位證據在保存、傳遞及檢驗過程更為便利，所花費的社會成本(人力、時間)將大幅下降，且能夠確保資料的完整性。藉由區塊鏈之分散式帳本，使數位證據於其他節點亦能被讀取，當數位證據被竄改破壞時，能於其他節點存取原始數位證據狀態。交通數位證據區塊鏈可以更方便、準確及迅速地儲存、檢索及瀏覽交通事故相關證據，透過網際網路可在遠端存取資料，不需花費人力及時間就能將資料即時送至車鑑委員會，更有效率及效能地釐清交通事故之肇事責任。

隨著科技的進步，使交通事故案件資料可存於區塊鏈上，其資料儲存空間相當大，但所需實際儲存裝置體積小，且區塊鏈之分散式帳本讓交通數位證據有異地備援之效，能有效保存及保全數位證據。

2.1 智能合約

在以太坊平台上，智能合約的程式碼在以太坊虛擬機上運作，每節點都含一個以太坊虛擬機，當節點打包驗證區塊時，便將相關交易可執行的程式碼送入以太坊虛擬機上執行，執行結果更新帳戶狀態並記錄於區塊鏈上。

透過Solidity語言進行智能合約撰寫，當發生觸發條件時，智能合約會依原先設定邏輯，執行相對應措施，並將結果保存於鏈上。

2.2 私有鏈

公有鏈因有效率問題及無法提供即時確定性，且參與者皆無法得知彼此身分，對於交通數位證據區塊鏈無法提供效率及安全上的保障。因此，採用私有鏈模式，不對外開放，參與者為各派出所/交通分隊現場處理員

警、交通大隊之員警及車鑑委員會委員，並對使用者進行身分認證。即使資料遭遇竄改或刪除，也能追溯到責任方，可追究其法律上之責任。

2.3 數位簽章

採用非對稱式加密法，每個使用者皆有一組公鑰及私鑰，簽名時使用私鑰，驗證時使用公鑰，將數位簽章附加在原交易中，用以證明交易發送者的身分。當現場處理員警發送交易（交通事故相關資料）時，先利用本身的私鑰對交易內容簽名，並將簽名附加在交易中。其他節點（交通大隊員警）收到廣播消息，先對數位簽章進行驗證，完成驗證並確認發送者身分，該交易才會觸發後續的流程。

3. 系統實作

系統架構中，透過Go語言開發之Go-Ethereum（簡稱為geth）來作為底層交通數位證據區塊鏈節點程式，而智能合約以Solidity程式語言實作，前端使用者介面由Java應用程式搭配web3j套件。透過特別編碼，將多筆交通事故相關資料雜湊值儲存於區塊結構中，每一區塊紀錄上一區塊位置，並串連在一起，形成交通數位證據區塊鏈，而為確保資料一致性，每一節點皆會保存相同資料副本。

交通數位證據區塊鏈平台作業流程分為四部分：註冊新節點、產生數位資料、傳送數位資料及接收數位資料，每份資料可執行多次的傳送與接收，說明如下。

(1) 註冊新節點

使用者先至Go Ethereum網站(<https://geth.ethereum.org/downloads/>)取得節點程式，下載安裝包（圖四）。



圖四：節點程式

使用者為派出所、交通分隊、交通大隊及行車鑑定委員會，每位使用者的電腦透過網路互相連接，共同維護資料，電腦中安裝geth節點程式，形成以太坊網路（圖五）。利用geth架設交通數位證據區塊鏈，架設四步驟為i.

設定創世區塊、ii. 建立Coinbase帳號、iii. 取得節點網路資訊、iv. 設定靜態網路設定檔。此區塊鏈具備較完善的許可權管理系統，能得知參與者數量及節點狀態，且節點數遠小於公有鏈，因此，具備更高的效能與更好的隱私安全。相對於資料庫，私有鏈中任何人皆無法輕易竄改資料，即使遭竄改也能追溯到惡意者。



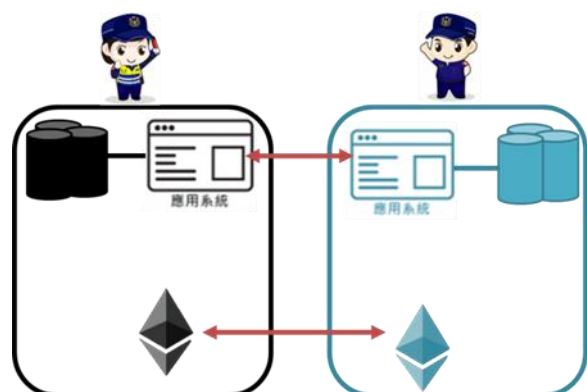
圖五：以太坊網路簡易圖

(2) 產生數位資料

將交通事故數位資料以SHA-256雜湊函數取其雜湊值，交通事故現場照片、行車影像畫面、周遭監視錄影畫面、交通事故現場圖及錄音（影）檔…將取得各自的雜湊值，因此鏈上資料為雜湊值的集合。

(3) 傳送數位資料

傳送方將交通事故相關資料以本身之私密金鑰加密上傳至交通數位證據區塊鏈平台，而傳送雙方具有各自以太坊節點、資料庫及應用系統（圖六），其他節點皆收到廣播消息則以傳送者之公開金鑰確認資料傳送者的身分。

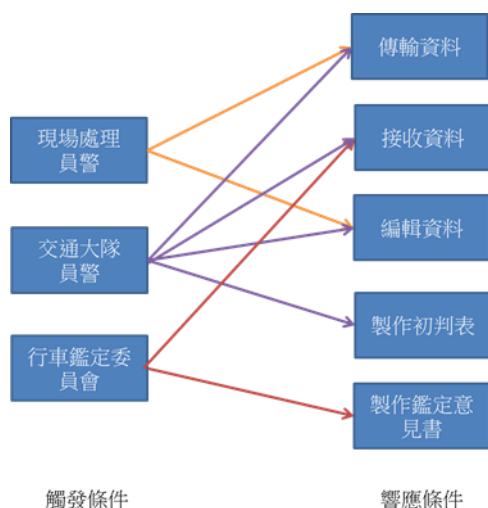


圖六：交通數位證據區塊鏈平台

(4) 接收數位資料

接收方透過區塊鏈平台驗證資料發送者身分，確認無誤後，透過智能合約設定進行瀏覽、編輯及製作交通事故相關資料。

智能合約設定角色與所對應之動作，角色分為各派出所／交通分隊現場處理員警、交通大隊員警及行車鑑定委員會委員等三種，所對應之動作共有傳輸資料、接收資料、編輯資料、製作初判表及製作鑑定意見書等五種，對應關係如圖七所示。交通事故現場處理員警（派出所／交通分隊）將所蒐集並製作之資料傳送至交通數位證據區塊鏈平台；交通大隊員警接收到資料後，如資料有誤可對資料進行編輯，或請現場處理員警編輯資料後並再上傳，如資料無誤則進行製作初判表，並將製作好之初判表上傳至區塊鏈平台，可供後續車鑑委員會使用；車鑑委員會委員依民眾申請交通事故鑑定，至區塊鏈上接收資料，並製作鑑定意見書。



圖七：智能合約之角色及對應動作

四、模擬案例探討

1. 模擬案例說明

大雄駕駛自小客車AC-1234，於2021年1月29日6時35分行駛於台中市清水區中山路及中華路口時，與小夫駕駛之自小客車DC-5678發生碰撞。由大雄以電話撥打110報警，由當地交通分隊派遣車禍處理小組A員警至現場進行交通事故處理，拍攝現場照片、繪製現場圖等。A員警向大雄及小夫要詢問行車紀錄器影像畫面，由雙方當事人親自交記憶卡給A員警釐清肇事原因。

2. 系統應用

2.1 現場處理員警上傳交通事故數位資料

A員警返回勤務處所後，將交通事故相關資料，現場照片、行車影像畫面…等傳輸至交通數位證據區塊鏈。

- (A) A員警至交通數位證據區塊鏈平台利用SHA-256對所蒐集到的資料進行雜湊運算，取得每個數位資料的專屬雜湊值。
- (B) 以A員警專屬之私密金鑰對欲傳送數位資料之雜湊值進行加密，並上傳至區塊鏈。因此，鏈上資料為多個雜湊值所組成的雜湊集。
- (C) 其他交通分隊、大隊或車鑑委員接收到廣播消息，利用A員警之公開金鑰進行確認，完成驗證並確認發送者身分，該交易才會觸發後續製作初判表的流程。

2.2 交通大隊員警接收資料並製作初判表

- (A) 透過智能合約設定，由隸屬於交通大隊之B員警負責製作初判表，藉由查看A員警所上傳之交通事故相關證據，如現場照片、行車影像畫面及現場圖，製作初判表記載雙方違規事實及肇事責任歸屬。
- (B) 如資料需修改，由B員警通知A員警將資料修改編輯後再上傳一次。
- (C) 初判表製作完成，利用SHA-256取其雜湊值，B員警將初判表雜湊值以本身私密金鑰加密上鏈，並廣播至各節點供驗證其正確性。
- (D) 大雄有申請提供初判表，因此B員警將所製作完成之初判表紙本送交給大雄。

2.3 車鑑委員會委員接收資料並製作鑑定意見書

大雄查看所收到之初判表，不服警方撰寫之可能肇事原因，並質疑現場照片及行車影像畫面有遭竄改之情形。B員警向其解釋對於交通事故相關證據之儲存、傳送皆以區塊鏈方式儲存資料，資料一旦上鏈，對資料之任何操作都經過所有成員共同驗證，具有防竄改與可追蹤之特性，因此能確保資料之一致性。經由B詳細解說，大雄對於警方交通事故相關證據保存及傳送流程，有一定程度之認識，相信資料保持原始狀態，具備證據力。但大雄對於警方撰寫之肇事原因仍有不服，因此自費3千元申請行車事故鑑定。

- 資訊工程系碩士班碩士學位論文，2020年，第4-7頁。

8. 華為區塊鏈技術開發團隊，「區塊鏈技術原理」，區塊鏈技術與應用，五南圖書出版股份有限公司，台北市，2020年，第36-38頁。

9. 華為區塊鏈技術開發團隊，「區塊鏈技術原理」，區塊鏈技術與應用，五南圖書出版股份有限公司，台北市，2020年，第73-81頁。

10. 陳柏仁，「基於區塊鏈技術之安全車載資訊系統」，南臺科技大學資訊工程系碩士班碩士學位論文，2018年，第5-6頁。

11. 翁嘉好，「基於區塊鏈之數位鑑識證據監管鏈」，國立政治大學資訊科學系碩士論文，2019年，第20-21頁。

12. 蔡馥璟、張躍瀚，「區塊鏈運用於跨境警務合作之研究」，執法新知論衡，第十六卷第二期，2020年，第71-72頁。

13. 賴寒彰,「區塊鏈探討與應用」,國立高雄第一科技大學資訊管理系企業電子化碩士班碩士論文,2017年,第11-16頁。

14. G. Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems", International Journal of Computer Science and Network Security, Vol. 11, No. 1, 2011, pp. 1-9.

15. M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, Blockchain, Business & Information Systems Engineering, Vol. 59, No. 3, 2017, pp.183-187.

- 16.M. Swan, Blockchain: Blueprint for a New Economy. " O'Reilly Media, Inc.", 2015.

17. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, Consulted. Vol. 1, 2008, p. 28.

18. 內政部警政署，刑案總數概況，網址：<https://ba.npa.gov.tw/npa/stmain.jsp?sys=220&ym=10900&yymt=10900&kind=21&type=1&funid=q01010101&cycle=41&outmode=0&compmode=0&html=q250x&out>

kind=1&fldlst=1111&cod00=1&rdm=pq5i
pVid，存取時間：2021-04-13。

19. 道安資訊查詢網，全國歷年事故總件數，
網址：<https://roadsafety.tw/motcgisDashboard/Dashboard/Custom?type=%E7%B5%B1%E8%A8%88%E5%BF%AB%E8%A6%BD%E5%9C%96%E8%A1%A8>，存取時間：2021-04-13。

我國不能安全駕駛之酒精濃度與肇事實證研究

吳國清

中央警察大學資訊管理學系教授

wkc@mail.cpu.edu.tw

摘要

當喝酒成為人類日常生活的一部分，加上車輛可快速行駛在道路以後，已衍生出公共危險、暴力（含家暴和性侵害）和公共衛生等問題。因酒後駕車致生車禍肇事所導致的後果，將使個人、家庭或社會付出相當大的成本。儘管世界各國（包括臺灣）透過各種方法（如制定與實施更嚴格的法令），試圖有效控制酒駕案件或預防犯罪的發生，但是仍然無法達到「零酒駕」目標，且不幸悲劇仍持續在發生。因此，本研究擬以我國各地方法院裁判書（檔案文件）高達 626,461 件作為樣本，透過大數據技術與統計分析後，並得到研究結果：（1）全國整體年均吐氣酒精濃度（BrAC）逐年遞減中；最高血液酒精濃度（BAC）為 0.794%，相當於 BrAC 值 3.97mg/L，發生於新竹縣市地區；全國年均 BrAC 以金門縣最高，臺灣本島以南投縣最高，六都以桃園市最高。（2）在酒精濃度與肇事率關係方面，BrAC 2.14mg/L（含）以下呈現直線關係，往後呈現多區段非線性的不規則變化。（3）當 BrAC 介於[2.77mg/L, 2.82mg/L]之間時，肇事率為 100%，即必會發生肇事。（4）推翻「酒精濃度愈高，肇事率就會愈高」的論點。（5）BrAC 達 2.25mg/L 以上時，未發生過量酒精中毒而死亡案件。（6）離島地區的金門、澎湖和連江等三個縣之年均 BrAC 和肇事率均高居全國之冠；雲林縣酒駕肇事率為本島最高。（7）就年均 BrAC 和肇事率交互作用分析，在六都中，以高雄市最為嚴重，其次是臺南市；新北市、桃園市和臺北市等北部三個直轄市，屬於全國酒駕嚴重等級最輕地區。（8）六都（直轄市）的駕駛行為人平均酒精濃度比其他類別縣市來得低。

關鍵字：大數據、不能安全駕駛、肇事、酒精濃度

一、前言

酒後駕車是個攸關公共健康和交通安全的核心問題（Stephens et al., 2017）。酒精（Alcohol）是在涉及到道路交通碰撞的駕駛行為人中最常被檢測到的物質。鑑於全球高達 35%的致命道路碰撞與酒精有關，確定酒精中毒對駕駛相關技能的影響非常重要。雖然大多數駕駛行為人承認醉酒後駕駛機動車的風險，但酒精仍然是與致命的道路交通碰撞有關的主要物質（Davey et al., 2020）。

1995 年，英國約有 24%的交通傷亡事故是在駕駛行為人血液中酒精含量大於 0.08%法定酒精標準值發生的（Clayton, 1997）。根據聯合國健康組織統計，全世界於 2016 年約有 135 萬人死於公路上，

其中高達 35%與酒精有關（World Health Organization, 2018），即約有 47 萬人死於與酒駕車禍肇事有關。

在臺灣，2013 年因酒駕致死事件頻繁，政府採取「治亂世用重典」的「嚇阻策略」（Deterrence Strategy），並於 2013 年 6 月 11 日修正《中華民國刑法》第 185-3 條。這條修正內容對酒駕犯罪具有「翹翹板式」雙重嚇阻效果的深遠意義，一是「降低」並明文規定酒精濃度法定標準值（吐氣酒精濃度由不明文 0.55mg/L 降至明文 0.25mg/L，血液酒精濃度由 0.11%降至 0.05%），行政罰標準下修到 0.15mg/L 和 0.03%；二是「提高」法定刑責。2019 年立法院司委會指出，2013 年 6 月修法後，酒駕致死案的一審地院判決有 63.7%低於

最低本刑3年，法官恐有輕判疑慮，與立法目的相違。高達近8成民眾不信任法官審理案件的公正性（劉玉秋，2019）。2019年過農曆新年前，在臺中市發生酒駕再犯陳姓男子（有犯罪前科）駕車當場撞死兩人肇事案件，引發社會憤怒和對司法不滿，並使政府不得不改採「特殊嚇阻策略」（Specific Deterrence Strategy）」進行修法，增加再犯（Recidivism）刑責規定與「罪責相當」原則。包括《道路交通管理處罰條例》分別於2019年4月17日、2019年5月22日和2019年6月19日修正公布相關酒駕加重處罰與保安政策之修正規定，包括提高酒駕罰鍰及拒絕酒測罰鍰、增訂沒入車輛、同車乘客連坐處罰、被害人懲罰性損害請求權和再犯安裝酒精鎖等，並分成兩個階段施行——2019年7月1日和2020年3月1日。同時2019年6月19日再度修正公布《中華民國刑法》第185-3條，增訂再犯刑責。由於我國刑法從2013年以前的法定「吐氣酒精濃度」（Breath Alcohol Concentration, BrAC）0.55mg/L，到了2013年以後修法降至0.25mg/L至今，顯示酒後肇事的嚴重性，希望藉由酒精濃度的大幅下降（差額0.30mg/L），來減少酒後車禍肇事。因此，如何設法達到「酒駕雙降目標」成為政府施政的重要指標，也是學者們長期以來所關注的探討議題。不過至今，國內外對於以系統性途徑和龐大法院裁判書案例，透過大數據分析，以了解酒精濃度與肇事之相關性研究，可說付之闕如。

鑑此，本研究擬從我國司法院法學資料檢索系統網站取得龐大法院裁判書案件（超過62萬筆JSON文字性資料），透過大數據技術，文字採礦、資料採礦與統計分析，及撰寫多種電腦語言和為數可觀的程式碼，來進行資料之洗清、處理、大數據分析和資料視覺化等，希望達到以下之研究目的：

- (1) 試圖了解各縣市酒駕行為人的酒精濃度與肇事為何？最大酒精濃度多少？在達到法定酒精濃度標準值情況下的肇事率為何？
- (2) 透過非監督式機器學習的分群法來得知各縣市肇事嚴重等級。

- (3) 以監督式機器學習的線性迴歸模型，了解酒精濃度對肇事率的解釋效果，及曲線變化為何？驗證是否「酒精濃度愈高，肇事率就會愈高」呢？當BrAC達2.25mg/L以上時，將會造成呼吸麻痺而死亡的高風險？

（FlightPhysical.com, 2005）

- (4) 試圖以變異數分析來檢定縣市地區的酒精濃度與肇事率是否具有交互效果，並以地理空間來呈現各縣市酒精濃度與肇事率交互強度與其嚴重等級。

二、文獻綜述

1. 相關名詞定義

1.1 不能安全駕駛

「不能安全駕駛」一詞並未在《中華民國刑法》第10條內加以定義。不能安全駕駛係指駕駛動力交通工具行為人，行駛在法定道路過程中，大部分無法在自由意志與理性選擇狀態下，可勝任操縱其交通工具與可預期其駕駛行為，而致生交通事故（肇事）風險機率增加。不能安全駕駛的結果，是大幅提升交通事故的風險，不確定性公共危險因子大增，造成個人或他人不可預期的生命與財產的威脅或損失。它自包括服用或飲用後在一段時間內可導致精準駕駛能力降低的（麻醉）藥物、違禁物、酒類，或在外在因素影響或干擾下，而致生不能安全駕駛。

如從因果關係論之，「交通工具行為人」為因，以「動力交通工具」和「飲用或服用酒類、毒品、麻醉藥品等」等為犯罪工具、「駕駛」為手段，致生抽象或具體「公共危險」為果。故《中華民國刑法》第185-3條的「不能安全駕駛」是一種風險機率（或然率）的概念，它會導致個人或多數人發生公共危險的可能性大增。它是工具性犯罪的一種，即當行為人駕駛交通工具且服用藥物、違禁物或飲用酒類、含酒精飲料後，已直接影響到駕駛能力或無法預期駕駛行為者，自構成刑事犯罪或交通違規。依駕駛汽車動力交通工具行為人所服飲物質不同而區分成酒駕（Driving Under the Influence of Alcohol）、毒駕

(Driving Under the Influence of Drug) 和藥駕 (Driving Under the Influence of Anaesthetics) 等三種，其中以酒駕之駕駛行為人數最多，所造成的有形與無形之生命、財產損失最大。

1.2 公共危險

所謂公共危險，係指犯罪行為足以危害不特定的多數人生命、身體、財產及一切之安全而言。就《中華民國刑法》第185-3條第一項規定，它可分成兩種：

- (1) 抽象公共危險，即預期可能發生不能安全駕駛交通工具者，包括：(酒精濃度達到法定標準值(如吐氣 $\geq 0.25\text{mg/L}$ 或血液 $\geq 0.05\%$)；(酒精濃度大於零值且未達法定標準值，但「致不能安全駕駛」者)；(服用毒品、麻醉藥品或其他相類之物，但「致不能安全駕駛」者)。
- (2) 具體公共危險，即駕駛交通工具行為已發生公共安全危害之事實者，如發生車禍肇事(事故)。

就法院裁判書之案由與主文觀點論之，當觸犯《中華民國刑法》第185-3條第一項規定之罪者，稱為「公共危險之不能安全駕駛動力交通工具罪」或「公共危險之不能安全駕駛動力交通工具而駕駛罪」。不論是否犯第185-3條第一項規定，只要因駕駛動力交通工具肇事致人死傷而逃逸者，自適用第185-4條之「肇事逃逸罪」。依據司法院大法官(民國108年5月31日)釋字第777號解釋，其中有關「肇事」(含酒駕)部分，非因駕駛人之故意或過失所致事故之情形(因不可抗力、被害人或第三人之故意或過失)是否構成「肇事」，尚非一般受規範者所得理解或預見，於此範圍內，其文義有違「法律明確性原則」，此違反部分，應自本解釋公布之日起失其效力。又根據《中華民國刑法》第14條規定「行為人雖非故意，但按其情節應注意，並能注意，而不注意者，為過失。行為人對於構成犯罪之事實，雖預見其能發生而確信其不發生者，以過失論。」前者為「無認識過失」，後者為「有認識過失」。同法第12條明定「行為非出於故意或過失者，不罰。過失行為之處罰，以有特別規定者，為限。」本研究認為大

法官第777號解釋令是有爭議的。因為刑事責任效力僅及於犯罪行為人之預謀或行為結果(既遂或未遂)，故第185-4條所稱「肇事」本已排除因不可抗力、被害人或第三人之故意或過失等情況之適用。另外，酒後駕駛之肇事行為乃非出於故意或過失，因為飲酒過量後將使其「預見」和「確信」因子變得更加模糊，自當排除正常人在理性判斷與自由意志下所為「故意或過失」之適用，但它卻對造成公共危險之風險(或然率)極大，涉及到公共健康和交通安全之嚴肅問題(Stephens et al., 2017)。故本研究建議修正第14條規定「行為人雖非故意，但按其情節應注意，並能注意，而不注意者，為過失。行為人對於構成犯罪之事實，雖預見其能發生而確信其不發生或因暫時失去判斷能力者，以過失論。」理由是飲用或服用酒精、毒品、麻醉藥品或其他相類之物，將導致人體神經認知過程受損，身體生理功能障礙(Impairment)，其功能障礙包括注意力、執行功能、感知、精神運動功能、反應時間和警覺性(Moskowitz et al., 2000; Ogden et al., 2004; Harrison et al., 2011; Martin et al., 2013)等暫時失去能力。行為人在「功能障礙」情況下所產生犯罪之事實，諉因於無法實施「理性判斷」，自不適用於「雖預見其能發生而確信其不發生」。

警察(機關及人員)對於「致不能安全駕駛」之實務操作上，包括命駕駛行為人在現場直線步行10公尺後迴轉走回原地，其腳離開測試的直線；又命其雙腳並攏，雙手向前平伸，閉眼、輪流使用左右手的食指指間觸摸鼻尖，其呈現無法以食指指觸碰到鼻尖；又命其閉雙眼，30秒內朗誦阿拉伯數字，由1,001至1,030之數值範圍，依其是否達到正常人行為表現、數錯數目或計秒過長等情事；或者命其用筆在兩個同心圓之間的0.5公分環狀帶內，畫另一個圓，其呈現畫圓不完整、不連續或畫在指定範圍外等情事，以決定是否為「致不能安全駕駛」。另一做法是警方在路邊攔停車輛之前，目視駕駛行為人反應遲緩、車身搖擺不定、蛇行，車身搖擺不定，轉彎半徑過大或過小等駕駛操控力欠佳；車輛行徑偏離常軌，時而加速，時而

突停等駕駛行為。

1.3 法定酒精濃度標準

現今世界各國對於法定酒精濃度標準 (Legal Alcohol Concentration Criteria) 或法定酒精限值 (Legal Alcohol Limit) 的容忍程度也不一致。不過各國法定血液酒精濃度 (Blood Alcohol Concentration, BAC) 標準大致介於 0.00% 至 0.08% 之間，其中以 0.05% 作為標準的國家占大多數。但仍然有少數國家嚴禁駕駛行為人喝了含有酒精、酒類飲品後開車的，如匈牙利、烏克蘭、古巴等國家之法定 BAC 值為 0.00%，只要 BAC 大於 0.00% 時，就觸犯國家法令規定；另一極端者，有極少數國家未明文規定的，如剛果、衣索比亞等國家毫無限限制 (維基百科，2007)。關於達到法定酒精濃度標準之處罰，我國將它分為行政罰和刑事罰。在酒駕行政處罰方面，根據《道路交通管理處罰條例》(修正日期：中華民國 108 年 6 月 19 日) 和《違反道路交通管理事件統一裁罰基準表》(修正日期：中華民國 108 年 6 月 28 日) 汽車駕駛人吐氣所含酒精濃度達每公升 0.15 毫克或血液中酒精濃度達百分之 0.03 以上者，可依酒精濃度比例原則和不同車種，科以行政裁罰之不同範圍的罰鍰處分。在酒駕刑事處罰方面，根據《中華民國刑法》第 185-3 條第一項規定駕駛人吐氣所含酒精濃度達每公升 0.25 毫克或血液中酒精濃度達百分之 0.05 以上者，處二年以下有期徒刑，得並科二十萬元以下罰金。

人體血液中都存在一種酒精水解酶 ADH (Alcohol dehydrogenase)，它是分解酒精的酵素。平日習慣飲酒或酒量較好的人，其體內 ADH 含量較多，分解酒精速度較快，故不易喝醉，酒後症狀也較輕微。此種人在喝完酒後，血液中的酒精濃度雖然很高，但也分解得很快，若代謝一段時間後才抽血，將可使血液酒精濃度低於法定 BAC 標準值。故血液酒精濃度高和累積飲酒酒精含量呈現正相關，但與代謝時間呈現負相關 (Yang et al., 2009)。酒精會從胃和小腸迅速吸收，並透過血液輸送到整個身體。其毒性作用因人而異，並受性別、體重、代謝率 (時間) (Rate of Consumption Time) 和消費酒精總量等變

數所影響。例如，體重較重者會比輕者在血液中含有酒精濃度較低些；空腹飲酒比飽餐飲酒較易達到酒醉狀態。由於酒精是一種鎮靜劑、催眠劑和成癮性藥物。它會迅速損害判斷力，並導致容易造成事故 (或交通肇事)，或行為失控。例如，酒後易於與他人發生口角、衝突、滋事或暴力；酒後駕 (騎) 車易發生肇事和傷亡等。理論上，血液酒精濃度在不同的 BAC 水平值所造成的肇事風險的或然率，兩者呈現線性關係。它從 0.05%BAC 值的 2% 相對肇事風險率，到了 0.20%BAC 值以上時，它的肇事風險率高達 30%。即提升 4 倍的 BAC 水平，但其肇事風險率卻增加 15 倍 (Wikipedia, 2007)。

在酒精濃度檢測上，常用體內酒精濃度測定方法大約有三種，血液測定法、呼氣測定法、尿液測定法 (單位：每 100 毫升尿液內含 X 毫克酒精)，其中尿液測定法較不常用，警方大部分採用呼氣測定法，當駕駛行為人無法進行吐氣檢測時，才會採用血液測定法。在酒精濃度檢測數據方面，(1) 時間無關，即不考慮人體酒精代謝率時，呼吸測醉器 (或稱呼氣酒精量測儀) (Breathalyzer) 所顯示的檢測數據，如果達法定酒精濃度標準值以上 ($\geq 0.25\text{mg/L}$) 時，警方則依此數據作為酒駕證據；(2) 當考慮人體酒精代謝率時，業據內政部警政署於民國 89 年 12 月 21 日 (89) 刑鑑字第 198913 號函，食後飲酒其呼氣酒精代謝率為每小時每公升 0.050 毫克 (最小值) 至 0.114 毫克 (最大值)，整體平均為每小時每公升 0.075 毫克，意即這個代謝率會因人而異。為簡化起見，我國法院採納呼氣酒精代謝率為每小時每公升 0.075 毫克。計算公式：飲酒後呼氣酒精平均估計值 (mg/L) = 警方攔停呼吸測醉器檢測值 (mg/L) + $0.075 \text{ mg/L} \cdot \text{HR} \times \Delta T \text{ HR}^1$ ，

¹ 臺灣彰化地方法院 105 年交簡字第 1328 號刑事判決 (民國 105 年 07 月 11 日)。本件被告於民國 105 年 6 月 18 日中午 12 時 12 分經施以吐氣酒精濃度測試，所測得之吐氣所含酒精濃度達每公升 0.18 毫克，依公式計算，則被告於同年月 17 日晚間 11 時許駕車上路時之體內呼氣酒精濃度平均估計值為每公升 1.17 毫克 (計算式： $0.18\text{mg/L} + 0.075 \text{ mg/L} \cdot \text{HR} \times$

作為酒駕呼氣酒精濃度是否達法定 0.25mg/L 之證據的證明方法。警方乃依呼氣酒精平均估計值作為酒駕證據。這種實施方式常用於警方深夜以後的路段或犯罪熱點攔停或發生肇事，但呼吸測醉器檢測值低於法定標準值 ($< 0.25\text{mg/L}$) 之時機。

酒精會抑制中樞神經系統，造成使用者的視覺、聽覺和反應障礙，降低注意力與判斷力，易使意識喪失和昏昏欲睡，其影響程度與生物體中的酒精濃度成正比。飲用含有酒精的提神飲料或酒類後，約 20% 的酒精量由胃吸收，80% 由小腸與大腸吸收，數分鐘後即分布在血液中。經由肝臟的脫氫酵素 (Dehydrogenase) 催化代謝，約 95% 的酒精會先變成乙醛，再氧化成醋酸，最後氧化形成二氧化碳與水，其餘約 5% 則由糞便、尿液、呼氣、皮膚汗液與唾液排出。想要測量人體內酒精的殘量，可由血液、尿液、唾液與呼氣進行測量，但因執法上不易採取血液、尿液、汗液、唾液等檢體，因此較可行的方法是以呼氣酒精濃度換算血液中酒精濃度來檢測。呼氣酒精濃度測量的原理，是基礎於血液中的酒精會遵循亨利定律 (Henry's Law) 而自由擴散於肺部中，所謂亨利定律是氣體在液體中的溶解度與氣體在氣相中的分壓成正比，因此在定溫定壓下，血液中的酒精濃度與肺部呼出的氣體酒精濃度會有一定的比例 (張維敦, 2004)。呼吸 (吐氣) 和血液中的酒精濃度是正比例的。然而，呼氣與血液的比例不僅在受試者之間，而且在同一受試者體內也可能時有不同。為了簡化起見，每個地區 (州、省) 或國家都有它們的法定「呼氣:血液」酒精濃度比例，中國香港採用的是 1:2300 (Yang et al., 2009)；美國為 1:2100；臺灣為 1:2000。

2. 酒精對人體的影響

酒精中毒 (Alcohol Intoxication) 的跡象 (Sign) 和症狀 (Symptom) 取決於一個人的血液酒精含量。當一個人因飲酒

與消耗酒精量產生行為或身體異常時，就可以說他或她患有酒精中毒。換句話說，這個人的精神和身體能力受到了損害或功能障礙 (Impairment)。除了觀察身體和精神受損的跡象外，還可以測量血液中的酒精含量。由於酒精 (乙醇) 對大腦的各個區域產生抑制作用，隨著人的酒精含量的增加 (人變得越來越醉)，會以漸進的方式造成身體和精神損害，從而產生中毒。長期飲酒、成癮或酒精濫用 (Alcohol Abuse)，將會導致神經系統疾病 (Neurologic Diseases) (American Addiction Centers, 2020)。

血液酒精含量 (Blood Alcohol Content, BAC)，也稱為血液酒精濃度 (Blood Alcohol Concentration, BAC) 或血液酒精值 (Blood Alcohol Level)，是一種用於法律或醫學目的之酒精中毒測量表示。酒精中毒造成的損害程度隨著 BAC 的不同而異。受損 (Impairment) 範圍從只有在 0.001-0.029% 之間水平值需透過特殊測試檢測到的輕微受損影響，一直到注意力、反射、運動控制等 BAC 連續頻譜 (Continuous Spectrum of BAC) 人的行為表現與其相對應功能受損情形。包括在 0.030%-0.059% 的大腦抑制力下降與集中度感覺變差，0.400%-0.500% 的死亡風險增加，及 0.50% 以上極高死亡可能性等。

3. 相關酒駕研究

3.1 警方執法嚇阻作用

根據臺灣《警察職權行使法》(修正日期：民國 100 年 04 月 27 日) 第 8 條第 1 項第 3 款明定「警察對於已發生危害或依客觀合理判斷易生危害之交通工具，得予以攔停並採行下列措施：……三、要求駕駛人接受酒精濃度測試之檢定。」根據 Caudill 等人 (1990) 一項研究顯示，警方對酒後駕駛 (Drinking and Driving) 行為的嚇阻作用偏低。超過半數 (59%) 的受訪者認為警察只是有點威懾力到完全沒有威懾力。在清醒的重度飲酒者 (Sober Heavy Drinkers) 中，55.8% 的人表示警察執行酒測威懾作用不太，甚至沒有作用的；另高達 71% 的醉酒重度飲酒者 (Intoxicated Heavy Drinkers) 也持同樣的

($13+12\div 60$) HR = 1.17mg/L)。 $\Delta T = 13.2$ 小時。

看法。這結果顯示，醉酒的重度飲酒者較有僥倖心理，自認為可避開警察指定之公共場所、路段和時段的車輛攔停與酒測，或者認為警察很少服勤執行路邊攔停與酒測。那些沒有酒後駕駛紀錄和飲酒低風險消費模式的駕駛人認為警察酒駕執法策略太過寬鬆 (Stephens et al., 2017)。

3.2 對酒駕安全認知

當被問及是否對自己在醉酒時的安全駕駛能力有信心時，整體上，有 62% 的受訪者覺得自己在醉酒時「可能」到「絕對可以」安全駕駛認知等級。在不同 BAC 水平值方面，有 73% 的醉酒重度飲酒者、66% 重度飲酒者和 63% 清醒的重度飲酒者，具有同樣的安全駕駛認知等級。醉酒重度飲酒者除了對安全駕駛的信心顯著高於清醒重度飲酒者外，且也對於酒後仍可駕車的知覺接受度較高 (Caudill et al., 1990)。有酒駕行為和有高風險飲酒態樣的駕駛行為人不認為酒後駕車會導致車禍風險增加，而且酒後駕車更可能同意他們在認為可以逃脫（躲避警察攔停酒測）的情況下喝酒和開車，尤其在警察執法不積極，固定路段和時段，或是較偏僻地區。酒醉後駕車次數越多的酒癮嚴重者，再犯率越高。再犯原因以「沒有交通工具可搭乘」最多；酒駕行為人決定酒駕之原因以自我認知之心理因素——自認神智清楚占大多數 (王邦安, 2008)。根據國內周文生等人 (2013) 針對酒駕行為安全認知研究顯示，被舉發次數多者比被舉發次數少者對酒駕安全認知較高，即對警察執法警覺性較高；有 75% (3/4) 的人不知道喝多少酒才會超過法定標準值，有 53.3% 的酒後駕車違規者在駕照吊扣（銷）期間仍會偶爾或如往常繼續駕駛車輛（無照駕駛）。

3.3 酒後肇事研究

根據張皓丞 (2011) 一項酒駕碰撞實驗結果顯示，酒精濃度對碰撞時間平均值、反應時間平均值、紅燈鬆油門距離平均值、車速標準差及反應時間標準差等變數達到統計顯著水準，證實飲酒確實會減弱駕駛績效。在歐洲地區，所有道路交通事故死亡人數中約有 25% 與酒精有關，且在歐洲所有公路里程數中，由血液中含有 0.5 克/升（即 BAC 為 0.05%）「酒駕行為人」

(Drunk Driver) 所駕駛車輛里程數也只有 1%。隨著酒駕行為人血液中酒精濃度 (BAC) 的增加，人、車或其他物之碰撞率 (Crash Rate) 也會上升。隨著 BAC 的增加，碰撞率的增加是漸進加劇的。如與「非酒駕行為人」(Sober Driver) 相比，體內含有 BAC 為 0.8 克/升 (0.08%) 酒駕行為人的碰撞率是非酒駕行為人的 2.7 倍。當 BAC 上升為 1.5 克/升 (0.15%) 時，酒駕行為人的碰撞率是非酒駕行為人的 22 倍。隨著 BAC 的增加，不僅碰撞率迅速增加，碰撞事故也變得更加嚴重。BAC 為 1.5 克/升 (0.15%) 時，「致命碰撞率」(Fatal Crash) (發生 A1 事故) 約為非酒駕行為人的 200 倍。因酒精而致生駕駛過程生理功能受損（如駕駛能力變差、反應遲鈍）且發生致命事故案件，約占歐洲所有致命事故的四分之一 (SafetyNet, 2009)。酒癮者易致生酒駕事故。吐氣時酒精濃度每公升達 0.25 毫克或血液中酒精濃度達 0.05% (50mg/dL) 時，其肇事率為非酒駕行為人的 2 倍 (蔡中志, 2001)。機車駕駛人涉及酒駕公共危險案件是其他駕駛人的 3 倍，再犯率將近一半 (49.53%) (陳高村等人, 2014)。

根據美國國家公路交通安全管理局 (National Highway Traffic Safety Administration, NHTSA) 統計，2012 年美國大約有 10,322 人死於與酒精有關的撞車事故，占所有交通事故死亡人數的 31%；到了 2017 年因酒駕車禍死亡人數高達 10,874 人，如以犯罪時鐘計算，每 48 分鐘有 1 人，或 1 天近 30 人，會因酒駕事故死亡。大約 25% 的致命傷亡 (A1、A2 類型) 事故與醉酒駕駛有關 (Babor et al., 2003)。在中國大陸，酒精相關事故占所有道路交通事故的 34.1% (Li et al., 2012)；根據大陸官方統計，在 2018 年因酒駕而死亡人數為 58,022 人，但 WHO 估計約 256,180 人，每 10 萬人口中約有 18.2 人死亡。在歐洲地區，酒駕占所有道路交通死亡事故的 25%，即每 4 件交通死亡案件中就會有 1 件涉及酒駕 (SafetyNet, 2009)。在日本地區，根據日本警察廳 (2010) 歷年來肇事統計分析顯示，酒醉 (吐氣 BrAC 達 0.25mg/L 或血液 BAC 達 0.05% 以上)

肇事死亡率約為未飲酒肇事死亡率的 30 倍；帶有酒味（吐氣 BrAC 達 0.15mg/L 或血液 BAC 達 0.03% 以上）肇事死亡率約為未飲酒肇事死亡率的 8 倍（蔡中志，2010）。

三、研究方法

1. 內容分析法

內容分析法是一種對文件（如歷史文獻、犯罪案件、刑事筆錄等）內容進行質性與量性的方法，其目的是經由文件內容本質的事實（Fact）、樣式（Pattern）或趨勢（Trend），試圖發現文件內容的隱性或潛藏價值，並透過內容分析來詮釋它們的價值意涵。基於此，本研究擬採內容分析法，結合大數據計算技術、文字採礦、資料採礦和專業統計等軟體來進行處理與分析。為便於進行本研究內容分析起見，研究人員撰寫甚多的軟體 Script 和電腦等語言程式碼，包括 DOS 批次處理指令、Word VBA、Excel VBA、（No SQL）MongoDB、STATA 和 R 語言等資料處理與分析，並行處理用個人電腦數計 3 部，在 Windows 10 作業系統，CPU 核心數為 4、邏輯處理器為 8，主記憶體 RAM 為 16GB，1TB 硬碟等環境為之。

2. 資料來源

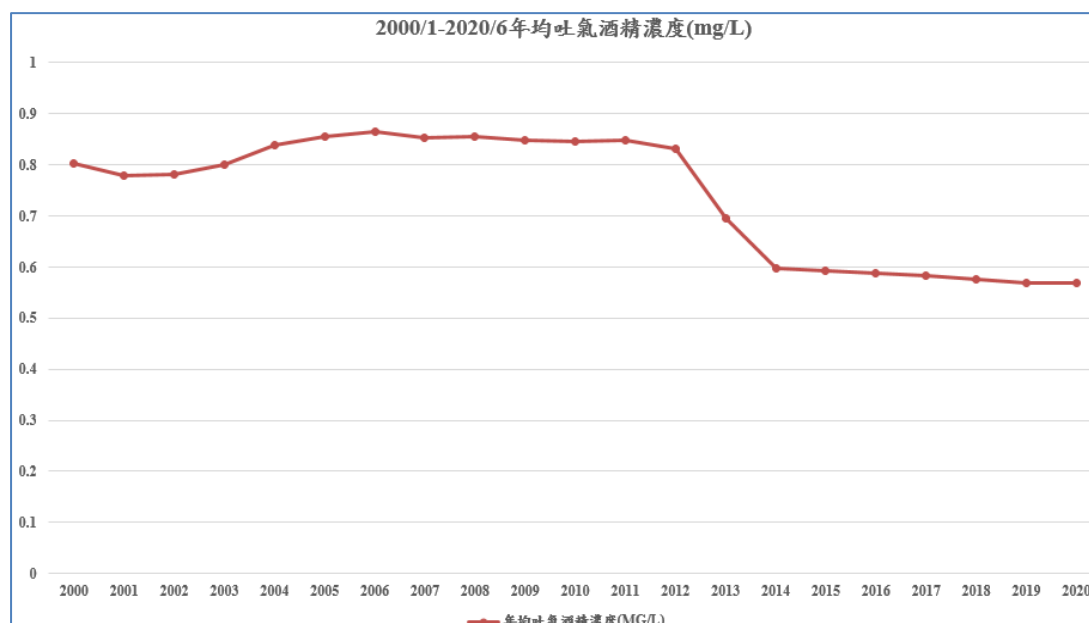
本研究從「政府資料開放平臺」（<http://210.69.124.88/>）所提供的國內各地方法院（含臺灣本島、澎湖，及福建金門、連江）以年月為單位進行下載壓縮檔案（RAR），內含民事、刑事和行政等裁判案件。下載壓縮檔案日期為 2000 年 1 月 1 日起至 2020 年 6 月 30 日止，取樣時間總計 20 年 6 月。經由 R 網路爬蟲程式下載，再經 DOS 指令對 246 個壓縮檔案進行解壓縮，總計所需硬碟容量超過 16GB，這個階段可說耗費相當多時間，故

藉由 3 部電腦來並行處理，以節省處理時間。最後透過 R、STATA ado 和 mata 物件導向程式碼篩選出與有關刑事公共危險案件裁判書之後，取得有效樣本數為 626,461 件裁判書（JSON 檔案類型）（超過 62 萬檔案），所需硬碟儲存空間仍高達 3.52GB，並且將它們透過 R 程式儲存至 MongoDB 資料庫內。其中視為無效而未納入本研究處理的裁判書，包括裁判案件屬於公共危險但非為酒駕、裁判內容重複、聲請上訴、上訴駁回、延長羈押、保證金、撤銷假釋、請求賠償損害、司法管轄錯誤或無罪判決等。

四、研究結果與討論

1. 酒精濃度敘述統計

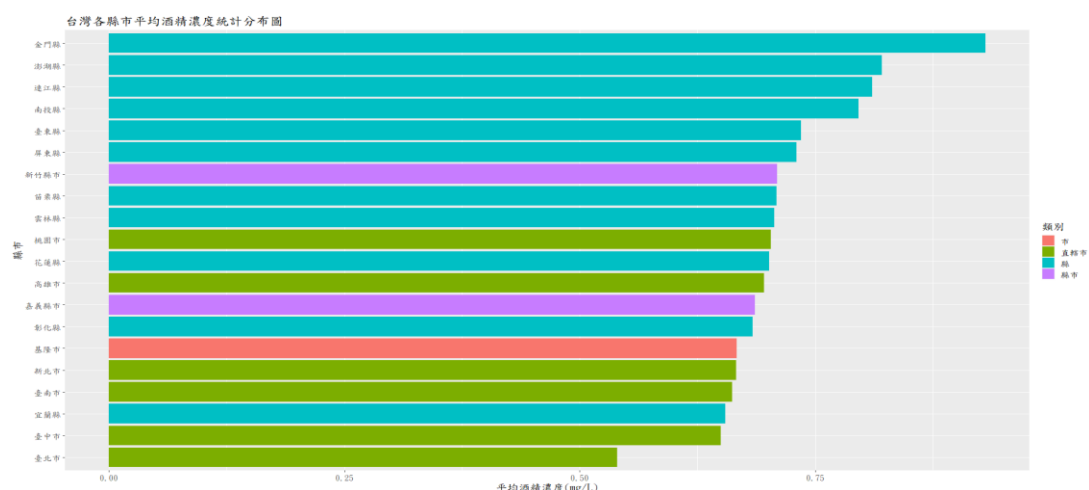
全國酒駕行為人酒精濃度最高者發生在新竹縣市，其 BAC 為 0.794%，換算成吐氣 BrAC 為 3.97mg/L。次高者發生在新北市，BAC 為 0.777%，換算成吐氣 BrAC 為 3.885mg/L。超出理論值 0.500%（2.5mg/L）高致死群甚多。意即在臺灣即使 BrAC 已達 3.97mg/L 也不會有酒精中毒致死發生。這個結果推翻過去學者們推論：「只要 $BAC \geq 0.450\%$ 或 $BrAC \geq 2.25mg/L$ 者，就會出現極高的致死率」。另從圖一得知，年均吐氣酒精濃度從 2000 年的 0.803mg/L，到了 2006 年達到最高峰的 0.865mg/L，而後逐年遞減，仍維持 0.832mg/L 以上，但受到 2013 年 6 月 11 日修正《中華民國刑法》第 185-3 條所採行的刑事嚇阻政策後，2013 年的年均吐氣酒精濃度大幅下降至 0.695mg/L，如與最大值相比，其降幅比率高達 24.46%。降幅另一主因是各縣市政府警察局配合內政部警政署推動酒駕大執法所致。到了 2020 年 6 月底止，年均吐氣酒精濃度已下降至 0.568 mg/L，降幅比率高達 52.29%。



圖一：我國 2000/1-2020/6 年均吐氣酒精濃度的時間變化

由圖二統計圖得知，各縣市從 2000 年 1 月起至 2020 年 6 月止，整體平均吐氣酒精濃度 (BrAC) 以金門縣最高，其次分別為澎湖縣、連江縣、南投縣、臺東縣和屏東縣等。顯然離島地區的駕駛行為人平均酒精濃度比本島地區來得高；在六都

中，以桃園市為最高，其次分別為高雄市、新北市、臺南市、臺中市和臺北市等。六都（直轄市）的駕駛行為人平均酒精濃度比其他類別縣市來得低。同時研究也發現，並非 BrAC 高（低）的縣市，其肇事率亦同步上升（降低）。



圖二：我國各縣市 2000/1-2020/6 平均酒精濃度統計圖

2. 不能安全駕駛肇事率分群分析

本研究經由資料探勘技術，以非監督式機器學習策略，Wards Linkage 分群演算法，透過 L2 相異度對不能安全駕駛肇事率進行分群探勘。經由分群參數設定六個

群和選定 $L2=11.11$ 的相異度量值後，獲得表一結果。結果顯示：(1) 離島地區（金門、澎湖、連江）肇事率最高。(2) 雲林縣是臺灣本島酒駕肇事率最高的縣市。(3) 位於中部地區的南投、彰化，為第 3 等級

嚴重區。(4) 位於南部地區之高雄市、屏東縣、臺南市，中部的臺中市，中北部的新竹縣市，東北部的宜蘭縣，列為第 4 等級嚴重區。其中臺南市為六都中酒駕肇事率最為嚴重的直轄市，其次是高雄市，但兩者差距不大。(5) 中低肇事群的第 5 等級者，包括苗栗縣、花蓮縣、基隆市、嘉義縣市。(6) 位於臺灣北部大城市的新北市、桃園市、臺北市等北部都會區，以及臺東縣，列為全國酒駕肇事嚴重等級最輕

的縣市。(7) 肇事率分群平均與吐氣酒精濃度分群平均兩者並非正向相關，例如，第 3 級肇事率群的平均 BrAC 就高於第 2 級肇事率群，同樣也發生在第 4 級和第 5 級。意即就分群分析而言，並不支持「酒精濃度愈高（低），肇事率必然就會愈高（低）」論點。本研究認為這可能與各縣市政府警察局的執法積極度有關，高見警率可能促使低肇事率。例如，新北市、桃園市、臺北市等北部大都會區。

表一：我國各縣市酒駕肇事率分群與其酒精濃度

輕重等級 肇事率分群	縣市名稱(肇事率)	肇事率 分群平均(%)	吐氣酒精濃度 分群平均(mg/L)
嚴重肇事群 (第 1 級)	澎湖(50.79%)、金門 (46.24%)、連江(45.45%)	47.49	0.854
高肇事群(第 2 級)	雲林(38.08%)	38.08	0.707
中高肇事區 (第 3 級)	南投(27.55%)、彰化 (27.22%)	27.38	0.74
中肇事群 (第 4 級)	新竹縣市(24.78%)、臺南 (23.76%)、高雄(23.49%)、 臺中(22.38%)、宜蘭 (21.8%)、屏東(21.6%)	22.97	0.684
中低肇事群 (第 5 級)	苗栗(18.1%)、花蓮 (17.61%)、基隆(17.00%)、 嘉義縣市(16.15%)	17.215	0.691
低肇事群 (第 6 級)	新北(14.77%)、桃園 (13.96%)、臺東(13.65%)、 臺北(9.88%)	13.07	0.661

3. 酒駕肇事率迴歸分析

本研究為能了解酒精濃度與肇事率之間相關與其解釋效果起見，乃從不能安全駕駛罪法定吐氣酒精濃度 0.25mg/L 標準值起²，以酒精濃度+0.01mg/L 作為遞增單位，分別計算酒駕案件數與其相對應的肇事件數，並求得酒駕肇事率。從表二線

性迴歸分析顯示，整體酒精濃度與肇事率是呈現強烈正相關的，其標準化後 Beta 係數=+0.91。

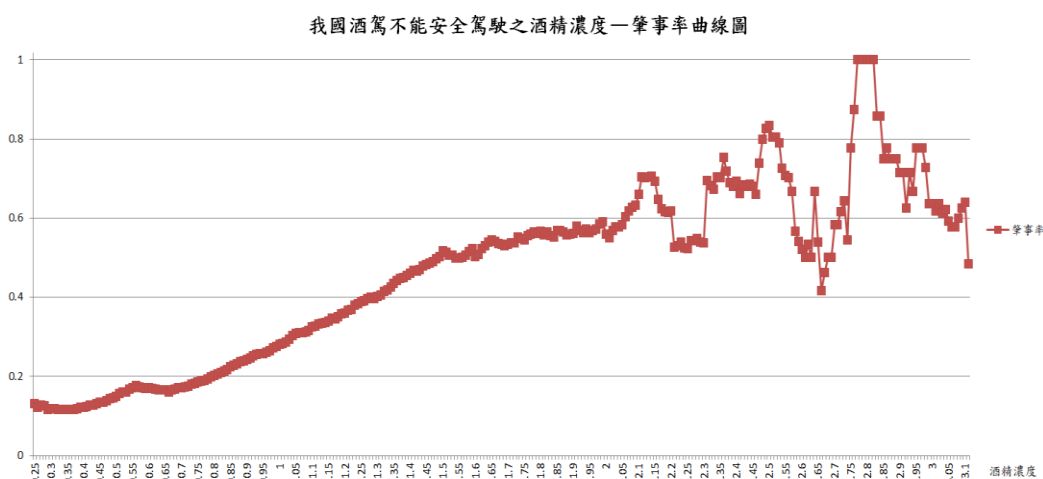
² 當警方或醫院是以血液測得駕駛行為人的酒精濃度時，本研究透過 1:2000 比例轉換公式，將它換算成吐氣酒精濃度值，以利統計分析。

表二：酒駕酒精濃度對肇事率線性迴歸分析

自變數	參數估計值	標準誤	t 值	Prob(t)	95%信賴區間	
					下限	上限
酒精濃度	.239911	.0063667	37.68	0.000	.2273792	.2524428
常數項	.0648743	.011926	5.44	0.000	.0414	.0883486
F 總檢定		F(1, 285)=1419.93；Prob > F = 0.0000； R-squared = 0.8328；Adj R-squared=0.8323； Root MSE=.08936； 標準化後 Beta 係數=0.912。				

從圖三曲線變化顯示，介於 [0.25mg/L, 2.14mg/L] 之間酒精濃度與肇事率幾乎呈現+45 度的線性關係，往後它們之間呈現高低交替之非線性變化。2.75mg/L 起肇事率就急速上升，到了 2.77mg/L 達到必然發生肇事。當酒精濃度介於 [2.77mg/L, 2.82mg/L] 之間時，酒駕肇事率達到最高峰 100%，意即我國駕駛行為人在此酒精濃度範圍內不安全駕駛最

為嚴重，必定會發生自摔、自撞或發生交通事故。然後 2.83mg/L 起肇事率又快速下降。當酒精濃度達 3.11mg/L 以上時，其肇事率就降至 48.48% 以下。這一重大發現顯然與過去相關研究有所差異。這也驗證了不支持「酒精濃度愈高，肇事率就會愈高」的論點；另由本研究結果顯示，BrAC 介於 [2.25mg/L, 3.97mg/L] 之間，並未發生呼吸麻痺而死亡。



圖三：酒精濃度與肇事率曲線圖

4. 酒精濃度與肇事率交互強度地理空間分析

由於酒駕酒精濃度對肇事率線性迴歸模型的解釋效果高達 91%。故當酒駕行為人的酒精濃度愈高（低），則可預測或

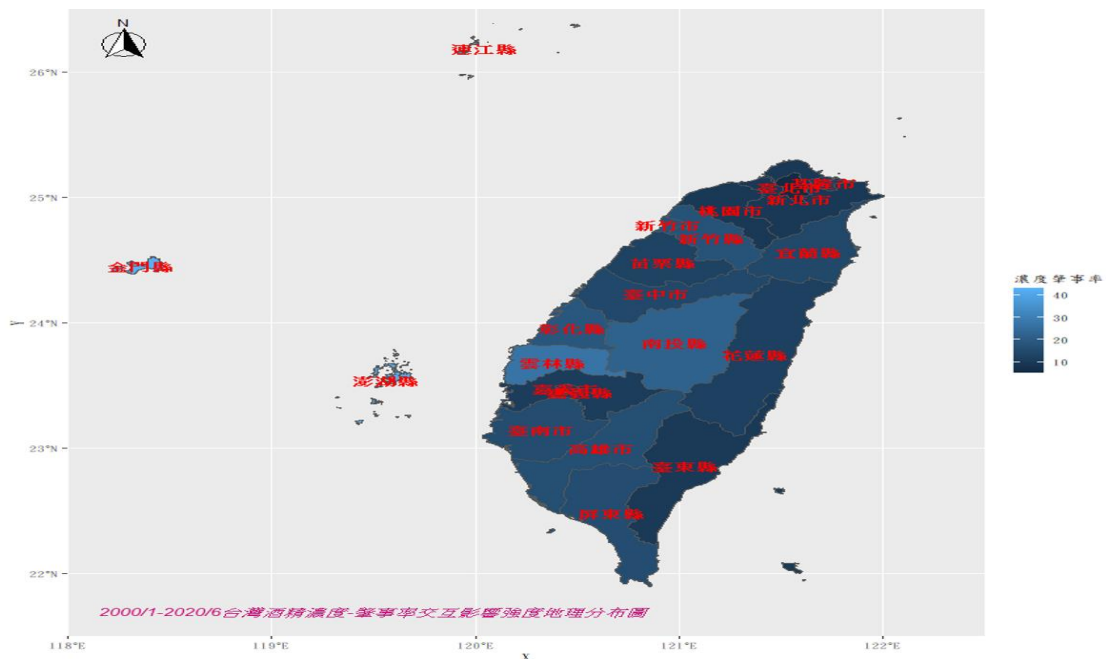
估計其肇事風險就會增加（減少）。意即酒精濃度對肇事風險具有強化效果。同樣地，就地理空間分析之，我國各縣市平均酒精濃度高低，將會正向影響到各縣市交通肇事率的高低。因此，本研究擬以各縣

市平均酒精濃度及其肇事率交互強度之相乘效果，來作為度量整體酒駕嚴重等級的指標。

經統計結果顯示，（1）離島地區（金門、澎湖、連江）的案件數雖然少，但因酒精濃度和肇事率均極高，形成全國酒駕最嚴重區。本研究認為，這可能與這三個縣市政府警察局採取「被動式酒駕執法」策略有關。意指當酒駕行為人發生車禍肇事後，警方才到案發現場對當事人進行吐氣或血液酒精濃度測試之檢定。此外，金門縣因盛產高酒精濃度的高粱酒，喝高粱酒人口相對較多，導致它的酒駕嚴重等級居全國之首。因此，建議離島地區的警察機關應採取「主動式或預警式酒駕執法」策略。（2）雲林縣是臺灣本島酒駕嚴重等級最高的地區。雲投彰等位於中部地區，可說是第二等級嚴重區。（3）新竹縣市為第三等級嚴重區。（4）位於南部地區之高雄市、屏東縣、臺南市，為第四等級嚴重區。其中高雄市為六都中酒駕最為嚴重的直轄市。如從米酒、保力達和高粱酒

等飲酒偏好統計量分析，高雄市均占全國第一位，這也反映出這個都市的人口結構，勞工之藍領階級數量較其他五都來得突出。（5）位於臺灣北部大城市的新北市、桃園市、臺北市等北部都會區為全國酒駕嚴重等級最低區。本研究認為它與這三個直轄市的警察機關採取「主動式或預警式酒駕執法」策略有關。

本研究以四種縣市類型（離島、縣市與市、縣、直轄市）對酒精濃度與肇事率交互作用強度值進行變異數分析（Analysis of Variable, ANOVA）後，得到 F 統計量為 26.86，機率值小於 0.0001，表示這四種區域之間的變異極為顯著。故即可進一步採用地理空間來呈現它們的酒駕嚴重等級，如圖五所示。圖內顏色愈深（淺）表示酒駕嚴重度愈低（高）。可以看出來離島地區酒精濃度伴隨肇事問題十分嚴重；新北市、桃園市和臺北市等北部地區直轄市問題最不嚴重區域。



圖四：我國各縣市酒精濃度與肇事率交互強度地理分布圖（2000/1-2020/6）

五、結論

本研究經由 626,461 件裁判書，及其大數據處理和分析後，得到下列結論：

- (1) 在全國酒駕行為人飲酒類別中，占 10% 以上共有四類，其中以啤酒類的 54.32% 居冠，其次分別為高粱酒類的 13.56%、提神酒精飲料保力達類的 11.56% 和米酒類的 10.57%。這 4 種占全部的 90.01%，即占了九成。
- (2) 全國整體年均酒精濃度值逐年遞減中。到了 2020 年 6 月底止，年均吐氣酒精濃度已降至 0.568 mg/L，降幅比率高達 52.29%。這與警察機關積極執法，2013 年和 2019 年的兩次修法，及法院受到強大民意壓力使判刑趨於重罰等三大因素有關。
- (3) 六都（直轄市）的駕駛行為人平均酒精濃度比其他類別縣市來得低。
- (4) 就酒精濃度與肇事率的關係，介於 [0.25mg/L, 2.14mg/L] 之間呈現正斜率直線關係，往後呈現非線性關係。當酒精濃度介於 [2.77mg/L, 2.82mg/L] 之間時，必定會發生自摔、自撞或發生交通事故。當酒精濃度達 3.11mg/L 以上時，其肇事率就降至 48.48% 以下。即不支持「酒精濃度愈高，肇事率就會愈高」的論點。另 BrAC 介於 [2.25mg/L, 3.97mg/L] 之間者，並未發生過量酒精中毒而死亡。
- (5) 離島地區的金門、澎湖和連江等三個縣之年均 BrAC 和肇事率均高居全國之冠；在六都中，以高雄市最為嚴重，其次是臺南市；新北市、桃園市和臺北市等北部三個直轄市，酒駕嚴重等級最輕地區。本研究認為這可能與當地百姓對酒後開車上

路知覺接受度和酒駕肇事案件容忍度，以及當地警察機關執法積極度等三大因素有關。

參考文獻

1. 王邦安，酒醉駕車決意歷程與預防對策之研究——以高雄地區為例，國立中正大學犯罪防治所碩士論文，2008。
2. 周文生、王玉玲，「酒後違規者對酒駕行為認知之研究」，中央警察大學，交通學報，第十三卷，第二期，2013，第 153~178 頁。
3. 張皓丞，車內酒氣偵測系統之研發與應用於市區酒駕行為之探討，國立中央大學機械工程研究所碩士論文，2011。
4. 張維敦，「呼氣酒測器如何測出我喝了多少酒呢？」科學人雜誌 (24) 2004，<https://sa.ylib.com/MagArticle.aspx?Unit=colums&id=385>。
5. 陳高村、郭佩霞，「酒駕處罰加重立法前後執法與判決結果特性分析」，2014 年道路交通安全與執法研討會，2014，第 527~542 頁。
6. 維基百科，「酒後駕駛」，2007，<https://zh.wikipedia.org/zh-tw/酒後駕駛>。
7. 劉玉秋，「酒駕致死逾半輕判——許宗力：研究讓量刑趨於一致」，中央廣播電臺，2019，<https://www.rti.org.tw/news/view/id/2012581>。
8. 蔡中志，「酒後駕車肇事防制對策之研究」，交通學報，第十卷，第一期，2010，第 39~58 頁。
9. 蔡中志，「國人酒精濃度與代謝率及對行為影響之實驗研究」，警光雜誌，第 538 期，2001。

10. American Addiction Centers, "Alcohol-Related Neurologic Disease," 2020, <https://www.alcohol.org/comorbid/neurologic-disease/>.
11. Babor, T., Caetano, R., Casswell, S., Alcohol: No Ordinary Commodity Research and Policy, Oxford: Oxford University Press, London, 2003.
12. Caudill, B.D., Kantor, G.K., Ungerleider, S., "Driving While Intoxicated: Increased Deterrence or Alternative Transportation for the Drunk Driver," *Journal of Substance Abuse* (2) 1990, pp: 51-67.
13. Clayton, A., "The End of the Decline in Drink Driving in Britain?" *Proceedings of the 14th International Conference on Alcohol, Drugs and Traffic Safety* (3) 1997, pp: 1227–1231.
14. Davey, J.D., Armstrong, K.A., Freeman, J.E., Parkes, A., "Alcohol and Illicit Substances Associated with Fatal Crashes in Queensland: An Examination of the 2011 to 2015 Coroner's Findings," *Forensic Science International* (312) 2020, 110190. <https://doi.org/10.1016/j.forsciint.2020.110190>.
15. Federal Aviation Regulation (CFR) 91.17, "Alcohol and its Effect on Pilots," *flightphysical.com* 2005, <http://flightphysical.com/pilot/alcohol.htm>.
16. Harrison, E.L.R., Fillmore, M.T., "Alcohol and Distraction Interact to Impair Driving Performance," *Drug and Alcohol Dependence* (117: 1) 2011, pp: 31-37.
17. Li, Y., Xie, D., Nie, G., Zhang, J., "The Drink Driving Situation in China," *Traffic Injury Prevention*, (13:2) 2012, pp: 101-108.
18. Martin, T.L., Solbeck, P.A.M., Mayers, D.J., Langille, R.M., Buczek, Y., Pelletier, M.R., "A review of Alcohol-impaired Driving: The Role of Blood Alcohol Concentration and Complexity of the Driving Task," *Journal of Forensic Sciences* (58: 5) 2013, pp: 1238-1250.
19. Moskowitz, H., Fiorentino, D., "A Review of the Literature on the Effects of Low Doses of Alcohol on Driving-related Skills," *National Highway Traffic Safety Administration, United States*, 2000, <https://one.nhtsa.gov/people/injury/research/pub/hs809028/Title.htm#Contents>.
20. NHTSA, "Drunk Driving," 2019, <https://www.nhtsa.gov/risky-driving/drun-driving>.
21. Ogden, E.J.D., Moskowitz, H., "Effects of Alcohol and Other Drugs on Driver Performance," *Traffic Injury Prevention* (5: 3) 2004, pp: 185-198.
22. SafetyNet, "Alcohol, European Commission, Directorate-General Transport and Energy," 2009, https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/specialist/knowledge/pdf/alcohol.pdf.
23. Stephens, A.N., Bishop, C.A., Liu, S., Fitzharris, M., "Alcohol Consumption Patterns and Attitudes toward Drink-Drive Behaviours and Road Safety Enforcement Strategies," *Accident Analysis & Prevention* (98) 2017, pp: 241-251.
24. Wikipedia, "Blood alcohol content,"

- 2007, https://en.wikipedia.org/wiki/Blood_alcohol_content#cite_note-3.
25. World Health Organization, "Global Status Report on Road Safety 2018," World Health Organization, Geneva 2018.
26. Yang, C.T., Fung, W.K., Tam, Thomas W.M., "Alcohol Study on Blood Concentration Estimation: Reliability and Applicability of Widmark Formula on Chinese Male Population," Legal Medicine (11) 2009, pp: 163-167.

能載舟亦能覆舟之文字隱碼研究

吳國清

中央警察大學資訊管理學系教授

wkc@mail.cpu.edu.tw

摘要

當人們透過手機、電腦或其他機器設備使用網際網路，並使之成為他們的日常活動的重要部分之時，象徵著科技工具已經影響到他們日常之生活、行為和思維模式了。不過，當人們遭受到資安事件所帶來的經濟損失或個資外洩與人格權受到侵害之時，就很快認知到資通安全保護的重要性。當一個國家將資安視成國安之戰略政策之時，那屬於國家層級資訊戰的重要一環了。用於資安目標（確保資訊之機密、完整和可用）之資訊或資料隱藏技術（Information or Data Hiding Technique）在全球網際網路盛行後得到快速發展與取得很好成就，如密碼學和加密工具。然而，這些技術很快成為惡力量的推手。如今，它們已成為世界各國資安主要威脅源、科技犯罪的主要工具和駭客場域試驗的保護傘（如暗網）。鑑此，本研究擬提出一個至今較少被國內外學術界所關注的資訊隱藏技術——文字隱碼術，它是一種利用檔案結構狀態的改變和編碼系統來達到資訊隱藏目的。本研究透過實驗法和撰寫程式碼，來實現它的可行性。經實際實驗結果顯示，文字隱碼確實可行，它的最大特點就是可以隱藏不同檔案類型和不受儲存空間限制的資訊隱藏量，並且不易被資安設備偵測到，也不易讓數位鑑識軟體所搜尋到資訊隱藏內容或它的詮釋資料。本研究期望這種技術不要成為資安威脅源或科技犯罪的主要工具。

關鍵字：資訊隱藏、文字隱碼術、圖像隱碼、密碼學

一、前言

2003 年 6 月，《中華民國刑法》增訂第 36 章之妨害電腦使用罪（第 358 條到第 363 條，計 6 條）；但隨著世界各國對非傳統戰爭型態——資訊戰的重視，及保護資通訊和網路安全的重要性，行政院於 2001 年 3 月成立「技術服務中心」，2016 年 8 月 1 日正式成立資通安全處。於 2018 年 6 月公布實施《資通安全管理法》。同時，政府積極推動「資安即國安」國家層級戰略政策，每年定期舉辦臺灣資安大會（CYBERSEC），投入可觀人力和龐大預算經費於產、官、學等資安領域的研

究和產品的研發。根據臺灣經濟部工業局的資安產值到了 2025 年估達 780 億元。未來國家將推動「資安即國安 2.0」戰略，也規劃行政院新設「數位發展部」，並且成立專責的「資通安全署」，提升對關鍵基礎設施及核心資料庫的防護韌性（馮建榮等人，2021）；與此同時，2006 年 4 月 6 日，內政部警政署刑事警察局成立「科技犯罪防制中心」，各縣市政府警察局在刑事警察大隊之下陸續成立新的「科技犯罪偵查隊」（簡稱科偵隊）單位（如 2016 年 12 月 9 日臺北市警局刑大成立科偵隊），藉以提升我國國民在資安治理能力，及預防和控制科技犯罪的發生，有效達成《警察法》

的警察四大任務——依法「維持公共秩序，保護社會安全，防止一切危害，促進人民福利」。現今，警察機關已將「資通安全」納入「社會安全」的重要一環。

儘管如此，由於這些相關法令規定大都屬於刑事告訴乃論或行政法令位階，加上網路犯罪無國界（如駭客入侵、勒索病毒、分散式阻斷服務等）和新型犯罪手法不斷出現，故可預期相關電腦（科技）犯罪案件一直存在著一定數量的犯罪黑數或無法在短期內偵破的冷案（Cold Case）。為了證實前面的假設，本研究從政府開放資料網站（<https://data.gov.tw>）透過網路爬蟲程式來蒐集我國 22 個地方法院相關電腦犯罪案件裁判書，期間自 2003 年 6 月起至 2020 年 4 月止，取得有效樣本數計 6,860 件。研究結果發現，以違反《著作權法》案件為最大宗，計 5,475 件，占全部的 79.81%（近 8 成）；其次是觸犯刑法妨害電腦使用罪，計 700 件，占全部的 10.20%；排名第 3 位是違反《個人資料保護法》的 449 件，占全部的 6.55%。三者合計占全部的 96.56%。為何妨害電腦使用罪案件在 18 年期間獲判有罪案件只有 700 件，年均將近 39 件，這象徵著刑法第 36 章的妨害電腦使用罪沒有預期發揮到應有的刑事政策和司法嚇阻力量。這結果與國內資安大廠所統計的高資安事件發生數有極大的落差，並也驗證了電腦（科技）犯罪存在一定數量的犯罪黑數。關於地方法院定罪妨害電腦使用案件數偏少原因，到底是涉及境外之司法管轄權或司法互助協議（條約）問題，或是因告訴乃論、偵查鑑識執法機關技術能量等因素所造成呢？還是我國政府因每年投入龐大資安預算經費於公務和非公務

機關之資通安全建設、資安治理和個資保護等頗有成效呢？值得深入研究。

不僅如此，更讓世界各國情治機關感到十分棘手難解的問題，就是深網（Deep Web or Deep Net）或暗網（Dark Web or Dark Net）的非法活動。暗網原創目的是提供網路使用者在公共網路（如 Internet）上，可以自由上網而不受審查，並保護個人隱私和資訊隱藏（如隱藏身分、訊息加密）之理念而設計的，以確保網路傳輸過程的訊息安全。然而，這種極為高度仰賴密碼學加解密技術的暗網，卻出現了「水能載舟，亦能覆舟」的困境。用於惡力量的加密直接關係到當今的三大威脅層面：好戰的恐怖（極端）主義、妨害電腦網路的使用和喪失證據資格（Evidence Admissibility）。文件透過加密後，其密文將無法表示用意之證明，即不得作為證據資格。

暗網非但已成為犯罪行為避風港和試驗場，也嚴重衝擊到明網和暗網的資訊安全、網路犯罪與數位鑑識等三個層面。例如，製作網路攻擊用程式，如惡名昭彰的勒索軟體，並在暗網網站進行實際試驗。由於它難以讓執法人員或專家追蹤，令資安設備（如入侵偵測[防禦]系統）難以偵測到異常與告警，當一旦試驗成功後便可移植到明網網站上，使得更多設備遭受損害，更多人參與犯罪或更多被害人和經濟的損失。

21 世紀，加密政策（Encryption Policy）正對自由民主價值觀形成重大考驗。觸發因素是一個兩難窘局的問題：

- (1) 善：密碼力量保護每一個公民在網上閱讀、個資或機敏資料、銀行和購物交易等安全和自由。

- (2) 惡：密碼力量也保護了外國間諜、恐怖分子、駭客和罪犯等犯罪的安全。

資訊隱藏猶如水，水能載舟（用於善），但亦能覆舟（用於惡）。其實早年最先出於善意的美國政府所推動的暗網，對這種窘局結果：往惡傾斜，可能是預想不到的和違背當初創建宗旨。

除了加密方法外，另一個資訊隱藏方法，就是隱寫術（亦稱隱碼術）（Steganography）。其中以「圖像隱碼」最為大家所熟知的。它主要以圖片（Picture）或圖示（Icon）作為隱藏資訊的載體，但這種方法無法承載大量隱藏資訊，技術水平高。基於此，本研究嘗試採用「文字隱碼」方法，從文字性檔案結構狀態改變和編碼，以實驗法和撰寫程式碼，來達到下列之研究目的：

- (1) 試圖以大家常用微軟的 Office 軟體之 Winword 文字檔案來隱藏可執行檔案（.EXE），以證明這種方法是否可承載大量隱藏資訊，而不被發現或異常示警？
- (2) 試圖為大家熟知的 PDF 文字檔案，透過合併途徑成另一個 PDF 文字檔案，是否可達到承載大量隱藏資訊目的和隱藏資訊效果？
- (3) 透過現今警察機關所採用的專業數位鑑識軟體 EnCase 和 Magnet AXIOM，透過 Search 或 Find 功能，是否可找到被隱藏起來的資訊（含 Metadata）呢？

二、文獻探討

1. 資訊安全

資訊安全之三大目的：機密性、完

整性和可用性（Confidentiality-Integrity-Availability, CIA）。它們是一種資訊安全基準模型，用於評估一個組織的資訊安全，以及實現並確保與資訊系統有關之機密、完整和可用等三大關鍵領域之安全。同時，它們也與法院呈堂表示內容用意之證據息息相關的。加密（如 DES 或 AES）可確保資訊的機密性和可用性；雜湊（如 128 位元的 MD5 Checksum 或 160 位元的 SHA-1 Checksum）所得的訊息摘要可驗證（Verification）資訊或映像檔案分段（Image File Segment）組合的完整性。

完整性對數位證據是否具有法定證據資格相當重要。現今，我國各級法院已接受 MD5 的證據完整性法律效力。國外有些國家則要求數位證據鑑定必須呈現 MD5 和 SHA-1。加密與雜湊的最大差別，在於前者可逆性（明文 A→密文 B（資訊狀態改變）→明文 A），後者不可逆性（明文 A→訊息摘要）。

當資訊涉及到網路通訊時，就會考慮到資訊與通訊（含網路）之保護、安全和網路犯罪等議題。根據我國《資通安全管理法》（2018 年 06 月 06 日公布）第 3 條第三款定義資通安全：「指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。」威脅資通安全或從事電腦網路犯罪等活動，其先決條件是必須由人去下達指令，親自或教唆他人或組織團體（3 人以上集體行動——犯意聯絡、行為分擔）加以實現。當透過通訊網路途徑或在網路上從事不法活動，乃由人去啟動欲達到特定目的之軟體和設備（發動端：起始點），經過通訊路由選擇（傳輸端：中繼點），最後抵達犯罪

目的地之受害設備或資料（目的端：終止點）。

根據法國鑑識兼犯罪學家艾德蒙·羅卡（Edmond Locard）交換定律（Locard Exchange Principle）之論點，「凡接觸過或走過，必留下痕跡」。因此，從事威脅資通安全或從事犯罪用的設備（如電腦、手機或其他行動裝置），都可能留下證據（跡證）。然而這些潛在數位跡證，存在著證據揮發性或揮發度（Volatility of Evidence）和資訊隱藏等問題。其中電介質（如 RAM 記憶體）的揮發度比磁介質或光介質來得高許多。當設備關機或沒電力時，電介質資料就會消失掉。還原資訊隱藏內容對於執法機關和人員來說是個極大挑戰。例如，透過加密法或隱碼法所製成檔案的還原，如何可呈現足以為表示意思之證明方法與其真實內容。

現今，許多政府機關或私人企業採用資訊委外，資料委外託管，資料放在公有雲的伺服器內，另個人對網際網路使用的高依存度與不當瀏覽或下載不明軟體，員工公私不分的電腦、手機混合使用，資訊科技產品和網路資源的濫用等，在資安治理（Governance of Information Security）不當或不遵守「資訊安全管理系統」（Information Security Management System, ISMS）資安管理規範等情況下，都會成為資訊安全的主要威脅來源、弱點，造成機敏資訊外洩，或違反資訊保密或營業秘密規定。

2. 資訊隱藏方法

在當今時代，由於網際網路的廣泛存在，人們彼此之間的溝通和分享多媒體內容變得極為容易。然而，與此同時，個人和受版權保護的材料或著作物的

安全傳輸已成為一個關鍵問題（Rehman et al., 2018）。隨著技術的進步和全球資訊網通信的廣泛使用，網路安全的挑戰也隨之增加。然而，這些挑戰可以透過先進的安全網路技術來應對，但每次這些技術對於長距離的秘密資訊通信來說可能不可靠，因此需要額外的安全機制來保護秘密資訊。在這種情況下，為了提供安全，有兩種技術被廣泛使用，即密碼學和隱寫術（Kumar et al., 2014）。因此，安全的資料傳輸方式是當前最迫切的需求。在密碼學方法中，資訊以加密的形式轉換，竊聽者無法理解；而隱寫術技術將隱藏的內容嵌入到不起眼的封面媒體中，以便在某些情況下不引起竊聽者的懷疑，發送加密的資訊可能會引起更大的注意，而不可見的資訊則否。

隱寫術是一種欲受保護秘密資料不被未經授權存取的隱藏資訊科學和藝術。隱寫術的方法是將秘密或機敏資料隱藏在一個音訊、視頻、文字或圖像等類型的文件中。隱寫術的實際挑戰是在不影響覆蓋文件的不可知情況下可實現高穩健性和容量。它是為了掩蓋嵌入資訊的存在，也是一種比密碼學更好保護資訊的方法，密碼學只隱瞞資訊的內容，而不隱瞞資訊的存在。原始資訊被隱藏在一個載體（Carrier）發生的變化就無法被觀察到。利用數位圖像作為載體來隱藏資訊，允許在通信方式上秘密地傳輸資訊。將秘密圖像與載體圖像相結合，就得到了隱藏的圖像。隱藏的圖像在沒有檢索的情況下很難被發現（Kumar et al., 2010）。

然而，能夠主動躲避資安軟硬設備偵測或人為監控的威脅，仍是資安所面臨的最大威脅和風險。例如「進階持續

性滲透攻擊」(Advanced Persistent Threat, APT)和零時差漏洞攻擊。駭客只要能不斷透過各種[資訊]隱藏方法不被發現或偵測到的話,就能持續對資安構成嚴重威脅和重大損失。

資訊隱藏 (Information Hiding) 係指不讓特定接收者以外的任何人知曉資訊的傳遞事件與資訊內容的意思表示,後來延伸為將秘密訊息或資訊暗藏在特別地方、無法接近或內容依習慣或特約無法表示其用意者。就法律層面來說,資訊隱藏是與證據資格有關的。若無法將資訊或訊息對外(如法庭或公眾)揭露並依習慣或特約足以為表示意思者,自不能作為證據資格。例如,加密過的密文檔案就不具法定證據資格。

資訊隱藏是一種將原有資訊狀態變更為另一狀態,但是經由反轉換後又會還原到原始狀態,故具有可逆特性。資訊抹除 (Wipe) 非為資訊隱藏,它是一種無法被還原回來的不可逆方法,它主要用於防止資訊再利用或不同證據受到交互污染。資訊隱藏主要目的有三種,第一種是讓資訊無法直接被存取(如無法開啟檔案);第二種是無法接近(根據檔案系統找不到檔案);第三種是內容無法表示用意(如訊息或檔案之攪亂、編碼、映像或壓縮等)。

資訊隱藏方法大致可分成五大類型:加密類、隱碼類、不可接近類、無法存取類和其他類等。其中不可接近類,包括(1)檔案隱藏法;(2)檔案刪除法;(3)媒體快速格式法;(4)RAM隱藏法等。而隱碼類則以隱寫術或隱碼術 (Steganography) 最具代表性。它原意指以秘密編碼 (Secret Code) 書寫方式來達到隱藏目的之活動總稱。它的主要特點是被隱藏資訊用的載體不會被破

壞,故不像加密類會引人注意或為搜索標的。隱碼術主要目的是為了隱瞞和欺騙。它是一種秘密通信的形式,可以涉及使用任何儲存媒體或主記憶體來隱藏資訊。它不是一種密碼學形式,因為它不涉及攪亂資料或訊息 (Scramble Message) 和使用金鑰,即不具混淆性 (Confusion) 與擴散性 (Diffusion)。相反地,它是一種資料隱藏的形式,並以巧妙方式執行,達到隱藏效果。密碼學是一門在很大程度上實現隱私的科學,而隱寫術則是一種實現保密和欺騙的做法,讓人易於產生錯覺。

資訊隱碼途徑可分為圖像(圖示或影像)、聲音和文字等三種。圖像隱碼已成功應用於數位浮水印 (Digital Watermarking) 與數位版權管理 (Digital Rights Management) 等(潘天佑,2012)。另一方面,駭客可經由隱碼途徑來達到資訊隱藏目的。例如,BEBLOH (趨勢科技,2018)或VAWTRAK(資訊保安,2015)等金融界木馬程式¹,就是利用「圖像隱碼術」在影像中使用最低有效位元 (Least Significant Bits, LSB) 的技巧來隱藏訊息²,又不會影響到載體的正常使用

¹ BEBLOH 會從命令及控制 (C&C) 伺服器擷取 URSNIF 惡意軟體。先前的垃圾郵件攻擊行動顯示,同時散佈 BEBLOH 和 URSNIF 是常見的手法。據 CrowdStrike 報導,攻擊行動是由 NARWHAL SPIDER 發動(Cutwail 殭屍網站),使用了圖像隱碼術,把惡意代碼隱藏在意想不到的圖像媒體中,藉此躲避特徵碼比對偵測。參見:[4]。

² Vawtrak 將含有銀行木馬程式的設定檔案暗藏在一個遠端的網站圖示 (Icon) 中,這個網站圖示 (favicon.ico) 是瀏覽器顯示在網址左邊的一個小圖。幾乎每個網站都會提供一個 favicon.ico 影像檔,因此,資安軟體看到這個檔案絕對不會懷疑它的真實性。除此之外,散布 Vawtrak 的網站還架設在 Tor 洋蔥路由器網路當中,難以追查和偵測。Vawtrak 擁有複雜的結構與攻擊模式,主要

用或降低原有資訊品質，故易於作為攻擊或竊取機敏資料之預備工作。這種平日可看得到的影像圖片，如美女或情色圖片，較易引誘他人點閱它；或者是隱藏在[迷人]風景圖片內，人們較不會去關注它或產生懷疑，而刪除它。現市面上有一些軟體工具可協助檢測與識別是否含有圖像隱碼存在，並加以移除或讓它失效，如 Guidance Software 公司的 EnCase (ILook Investigator)。不過不論使用「圖像、Video 影像或聲音」隱碼術的主要限制是，無法隱藏大量資訊，且需要較深的學理和技術。

3. 文字隱碼術

2010 年，Morran 等人使用自然語言技術作為文字替換的基礎，以便文字性隱藏資料可被嵌入到文件內容中。它的前提假設是，現有的語言處理技術可以提供足夠的豐富性和靈活性，以提供文字編碼設施所需的可靠性和複雜性。然而這種方法採用了語音索引標籤、詞義歧義和同義詞替換等技術，使一個語篇標記器來標記一個給予的封面文字，然後根據其語篇和詞義消歧來選擇特定的目標詞進行替換。但是因為除了在不同文字編碼系統外，文件內容存在語義的複雜性，處理效能較低，使得它的成效十分有限。2012 年，Por 等人提出在 Microsoft Word 文件內利用 Unicode 空白字元嵌入外部資料，以達到文字性資料隱藏效果，稱為 UniSpaCh 文字資

料隱藏法 (Text-Based Data Hiding Method)，然而這種方法，仍和 DASH 法一樣，都會受到嵌入資訊量效能 (Embedding Efficiency) 和編碼等限制之問題。

本研究將選擇另一種方法，稱為「文字隱碼術」(Text Steganography)，意指將文字編碼或機器碼隱藏在文字性質的檔案內，而且與原始文件內容無關，即與 UniSpaCh 和 DASH 之文件內容相依不同。本質上，它是屬於一種利用某些(並非全部)編輯或瀏覽文字(含編碼系統)用軟體本身的特有檔案結構之狀態改變，或者利用 DOS 指令迫使檔案結構狀態的改變，來達到資訊隱藏目的。它的特點是 (1) 可以隱藏大量資訊；(2) 隱藏對象可為任何檔案類型，如病毒程式(.EXE)或文字檔案(.TXT)；(3) 隱藏用載體為大家所常用的軟體，如預估 2010 年全球約有 80% 使用微軟的 WinWord (Montalbano, 2009)，或者 PDF 等，所製成的文件用載體，可以正常開啟它與瀏覽內容，故不易引人注意或被懷疑；(4) 難以被數位鑑識軟體工具發現；(5) 不易被資安軟體(如防毒軟體)，或違反機關內部資安政策而被告警、阻絕；(6) 可用於機敏資料的保護，即使設備(檔案)遺失或被攔截，也不會擔心資料外洩；(7) 它也可能成為駭客或不法之徒製造資安威脅或電腦網路犯罪的手段之一。

三、研究方法

由於文字隱碼術所採行方法有許多，受限於文章篇幅，本研究擬以 Word 和 PDF 等兩種檔案類型來實驗與實現本研究之目的。有關實驗用的軟硬體設備和程式設計用電腦語言，包括 64 位

為竊取各種金融資料與在受感染的裝置上無痕選擇進行遠端遙控交易；其攻擊模式則包括受感染裝置的螢幕擷取、發動中間人攻擊 (Man-in-the-Middle) 等。Vawtrak 以三種方式散播：以垃圾郵件誘導目標下載惡意軟體、各種植入式惡意軟體下載器、漏洞發掘器 (Exploit Kit) 等。Vawtrak 攻擊對象為銀行、遊戲、社交網路用戶。參見：[2]。

元個人電腦 (Windows 10 和 DOS 等作業系統環境)，Microsoft Office 2010 版以上 WinWord.exe、7Z.exe、Love.exe (模擬病毒程式用)、Adobe、DOS 指令、STATA ADO 語言、EnCase Forensic、Magnet AXIOM 等。

四、研究結果與討論

1. 惡力量的文字隱碼

1.1 演算法

在製作原理上，由於 Microsoft Office WinWord.exe 2010 版以上所編輯製作的文字檔案，乃是透過循環冗餘校驗 32 (Cyclic Redundancy Check, CRC32) 針對電腦檔案資料產生簡短固定 32 位元驗證碼的一種雜湊函式與非破壞型壓縮格式，其編碼系統為 UTF-16 LE，並以多個「可延伸標記式語言」(Extensible Markup Language, XML)

組織成一種複合檔案 (Compound File) 儲存之。因此，本研究藉由這些特性，可將「執行機器碼」(Executable Machine Code) (.EXE) 隱藏於任何由人為編輯的 WinWord 文字檔案內，檔案類型為.docx。

當這些可執行機器碼如為惡意程式 (Malicious Programs) 時，這個惡的力量將構成資安上的極大威脅。因為它被隱藏在文字檔案 (.docx) 內部，外部又是 CRC32 的壓縮格式，故不易被防毒軟體或入侵偵測系統所偵測到與告警，且可正常開啟該文字檔案而不會出現異常示警。更可怕的是，這種隱藏技術可以不受被隱藏檔案大小的限制，不會如圖像隱碼術 (Steganography) 那樣，每一個圖像檔案只能隱藏極少訊息量的限制，同時也不易被數位鑑識軟體工具找到。有關隱碼演算法如下：

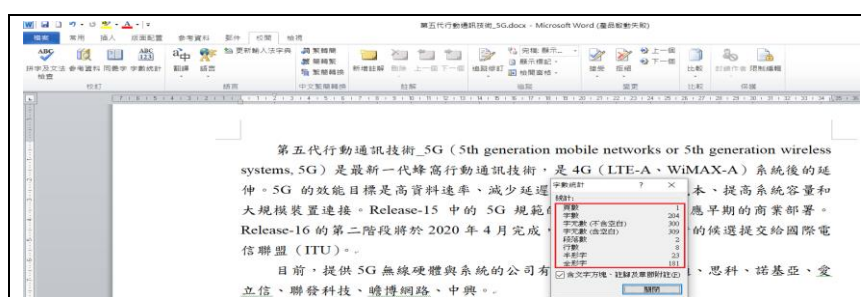
Step	Algorithm 1 HiddenExeCode algorithm
1:	Procedure HiddenExeCode()
2:	Rename($\Omega.exe$, $\Omega.xml$) //Virus File: $\Omega.exe$
3:	Rename($\Phi.docx$, $\Phi.zip$) //Carrier File: $\Phi.docx$
4:	IF Exist(temporary_folder_ Λ) THEN Remove(temporary_folder_ Λ) ENDIF Make(temporary_folder_ Λ)
5:	Move($\Phi.zip$, temporary_folder_ Λ)
6:	Decompress($\Phi.zip$)
7:	Move($\Omega.xml$, Subdirectory_of_decompressed_ Φ)
8:	Rename($\Phi.zip$, $\Phi.docx$)
9:	Remove(temporary_folder_ Λ)
10:	Send(Email_Address, $\Phi.docx$)
11:	Receive($\Phi.docx$) //Carrier file with Virus file: $\Phi.docx$
12:	Rename($\Phi.docx$, $\Phi.zip$)
13:	Decompress($\Phi.zip$)

- 14: Move(Ω.xml) //move out from Zip environment
- 15: Rename(Ω.xml, Ω.exe)
- 16: Attack(Ω.exe) //Virus file(Ω.exe) launches attack to a comprised computer
- 17: END

1.2 範例

本研究以 Microsoft Office 產品 WinWord.exe、7Z.exe 和模擬病毒程式用的 Lover.exe（容量大小：196 KB）等軟體作為實驗工具。有關文字隱碼實施過程如下：

- (1) 利用 MS Office WinWord.exe 2010 版以上建立一個文書檔案，檔名為第五代行動通訊技術_5G.docx。從選擇【校閱 > 字數統計】中記錄統計數據，及檔案內容與編排形式，如圖一所示。

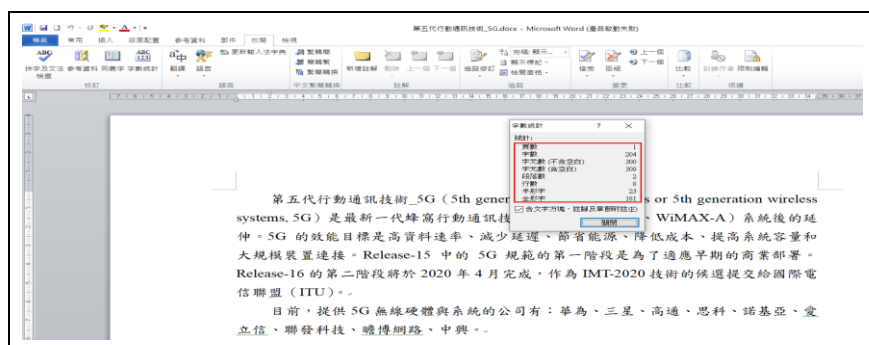


圖一：「第五代行動通訊技術_5G.docx」內容及其字數統計

- (2) 將「第五代行動通訊技術_5G.docx」變更為「第五代行動通訊技術_5G.zip」。
- (3) 建立一個暫存資料夾：TEMP，並將「第五代行動通訊技術_5G.zip」移入。
- (4) 以 7Z.EXE 壓縮/解壓縮軟體，開啟「第五代行動通訊技術_5G.zip」檔案。
- (5) 將「Lover.exe」病毒程式變更為「Lover.xml」（壓縮後為 105KB 大小，壓縮比= $(196-105)/196*100\% = 46\%$ ，CRC32 為 39C54D53），然後將它隱藏在已被開啟的「第五代行動通訊技術_5G.zip」檔案內，如圖二所示。
- (6) 將「第五代行動通訊技術_5G.zip」變更為「第五代行動通訊技術_5G.docx」。
- (7) 將「第五代行動通訊技術_5G.docx」透過電子郵件寄給對方。
- (8) 對方收到信件後，確認是否可正常開啟「第五代行動通訊技術_5G.docx」檔案？並選擇【校閱 > 字數統計】。然後比較前後之內容、字數和版面是否有被改變。
- (9) 從圖三結果發現：(A) 它可以正常開啟文字隱碼後的 Word 檔案，且無任何警語；(B) 在字數統計之各項數據與圖一比較結果完全相同；(C) 內容並未出現「資訊隱藏」用 Lover.exe 相關資訊；(D) 內容版面編排格式前後一樣。



圖二：Lover.xml 被隱藏在文字檔案內（CRC32: 39C54D53）



圖三：當隱藏 Lover.exe 後「第五代行動通訊技術_5G.docx」內容

(10) 利用 EnCase Forensic 或 Magnet AXIOM 等數位鑑識軟體找不到資訊隱藏 Lover.exe，並且正確顯示「第五代行動通訊技術_5G.docx」內容，

如圖四所示。在「詳細資料」(跡證資訊)欄位找不到與 Lover.exe 有關的詮釋資料 (Metadata)。



圖四：Magnet AXIOM 載入「第五代行動通訊技術_5G.docx」所呈現內容

1.3 程式碼

將上述實驗過程透過 DOS 指令來

達到自動隱藏目的；如要還原 Lover.exe，則解壓縮與更名。有關程式碼如下：

Step	DOS 指令
1:	C:
2:	CD \
3:	IF EXIST "TEMP" RMDIR /S /Q TEMP MD TEMP

```

4:      ren Lover.exe Lover.xml
      ren 第五代行動通訊技術_5G.docx 第五代行動通訊技術_5G.zip
5:      MOVE 第五代行動通訊技術_5G.zip TEMP
6:      CD TEMP
7:      "C:\Program Files\7-Zip\7z.exe" x 第五代行動通訊技術_5G.zip
8:      DEL 第五代行動通訊技術_5G.zip
9:      REM 隱藏 Lover.exe 病毒程式
      MOVE Lover.xml doc Props
10:     "C:\Program Files\7-Zip\7z.exe" a -tzip 第五代行動通訊技術
      _5G.ZIP .
11:     copy 第五代行動通訊技術_5G.ZIP ..\第五代行動通訊技術
      _5G.ZIP
12:     CD..
      ren 第五代行動通訊技術_5G.ZIP 第五代行動通訊技術_5G.docx
13:     RMDIR /s /Q TEMP

```

2. 善力量的文字隱碼

本研究透過文字檔案之編碼系統，如 ANSI、BIG5、Little-Endian Unicode (UTF-16LE)、Big-Endian Unicode (UTF-16BE)、Without BOM UTF-8 和 With BOM UTF-8 等，檔案結構，檔案簽章 (File Signature) (含檔頭和檔尾)，及數字系統轉換等概念，來達到有關機敏性檔案內容之文字隱碼目的。為了達到隱碼目的，本研究採用微軟 Office WinWord.exe、Adobe、STATA ado 語言和 EnCase Forensic 數位鑑識軟體等作為實驗用工具。有關資訊隱藏實驗程序如下：

- (1) 透過 WinWord.exe 編輯兩個機敏性檔案中文或全形字元 (Fully Formed Character) 內容，並分別儲存成兩個 PDF 檔案類型的文字檔案。並以 Adobe Acrobat Reader DC 瀏覽其檔案全文與資料格式。
- (2) 在 STATA 環境撰寫與執行 ADO 程式碼，主動匯入 PDF 檔案，並將這

兩個檔案內容串接 (String Concatenation)，然後將字串合併結果匯出到另一個 PDF。

- (3) 以 Adobe Acrobat Reader DC 瀏覽輸出 PDF 檔案，檢查是否已全部被隱藏起來。
- (4) 使用 EnCase Forensic 搜尋 (Search/Find) 功能及關鍵字，來檢視輸出 PDF 檔案內容是否可被找到。

2.1 演算法

本研究透過檔案結構變更狀態技巧，讓用來隱藏資訊的載體 (檔案) 開啟後內容呈現空白，但內容實際存在的，只是被隱藏起來，故不易被資安或鑑識用軟硬體設備的自動檢測或人為所識別。由於它為大家所熟知的 PDF 文字檔案，不含惡意程式碼，自不易被防毒軟體視成是一種病毒或惡意程式，而發出警告或刪除。同時在網路傳輸過程中，即使被他人利用設備攔截、竊取，也不易發覺它的真實內容。有關機敏性 PDF 檔案文字隱藏演算法如下：

Step	Algorithm 2 HiddenConfidentialCode algorithm
1:	Procedure HiddenConfidentialCode ()
2:	Import($\Omega 1$.PDF) //Confidential file: $\Omega 1$.PDF
3:	Import($\Omega 2$.PDF) //Confidential file: $\Omega 2$.PDF
4:	Merge $\leftarrow$ Concat($\Omega 1$.PDF, $\Omega 2$.PDF) // Merge = $\Omega 1$.PDF + $\Omega 2$.PDF
5:	Export(Merge, Φ .PDF) //Hidden Content File: Φ .PDF
6:	End

經由授權存取者接收到該文字隱碼檔案後，就可將該檔案拆解回來原始的兩個檔案與可用性，即可正常開啟

PDF 檔案，其瀏覽內容、編輯格式等完全相同。有關檔案還原 (File Recovery) 過程的演算法如下：

Step	Algorithm 3 FileRecovery algorithm
1:	Procedure FileRecovery ()
2:	Import(Φ .PDF) //Hidden Content File: Φ .PDF
3:	PositionHead $\leftarrow$ GetFileSignature(FileHead, Φ .PDF)
4:	PositionTail $\leftarrow$ GetFileSignature(FileTail, Φ .PDF)
5:	$\Omega 2 \leftarrow$ SubStr(Φ .PDF, PositionHead, PositionTail-PositionHead+n)
6:	$\Omega 1 \leftarrow$ Remove(Φ .PDF, $\Omega 2$.PDF)
7:	Export($\Omega 1$, $\Omega 1$.PDF)
8:	Export($\Omega 2$, $\Omega 2$.PDF)
9:	End

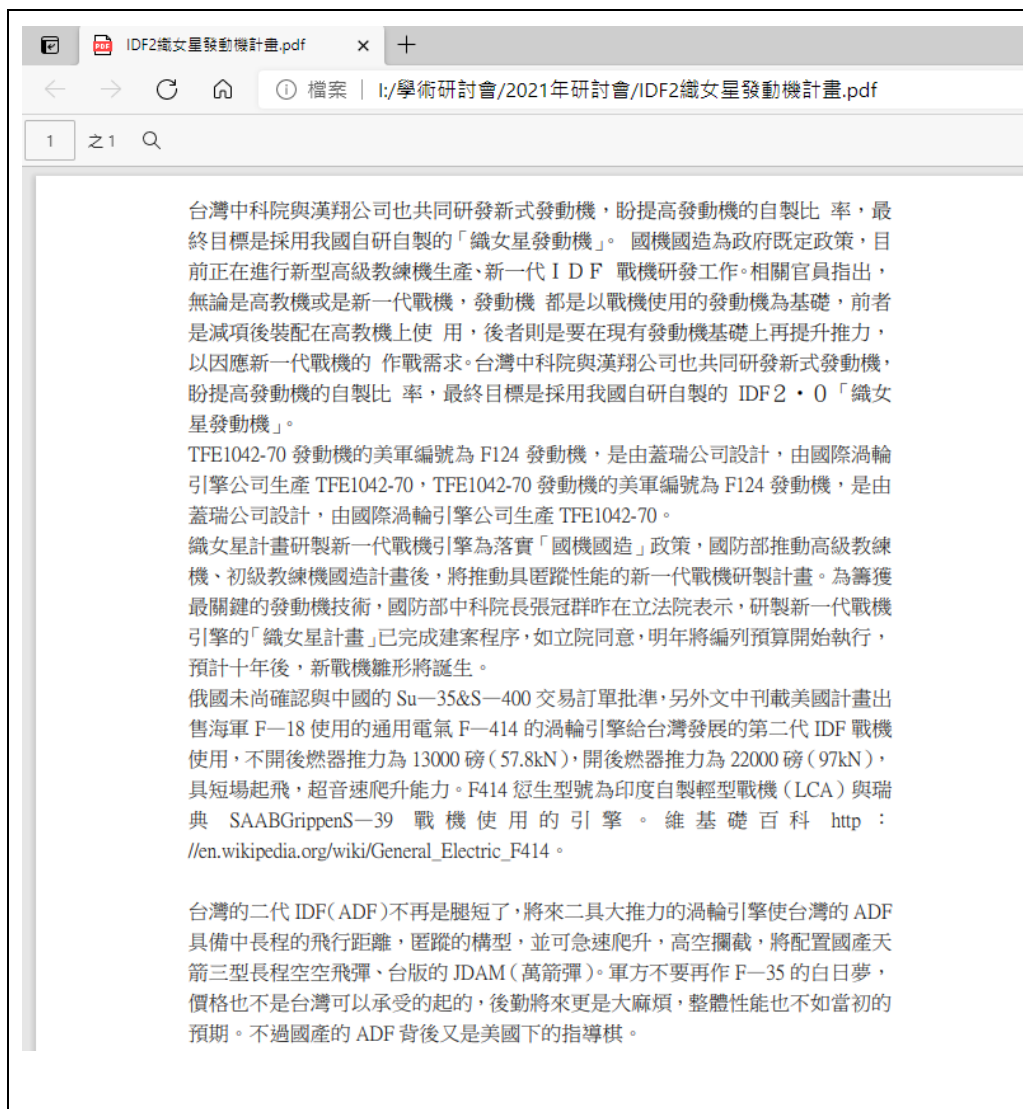
2.2 範例

本研究將以 Microsoft Office WinWord.exe、Adobe、STATA ADO 語言和 EnCase Forensic 數位鑑識軟體等作為實驗用工具。有關文字隱碼實施過程如下：

- (1) 利用 MS Office WinWord.exe 2010 版以上建立兩個機敏性文件，並分別儲存為「IDF2 織女星發動機計畫.PDF」(#1_機密文件) (如圖五所示，儲存大小為 145KB)、「共機侵擾台灣西南 ADIZ.PDF」(#2_機密文件) (如圖六所示，儲存大小為

85KB)。

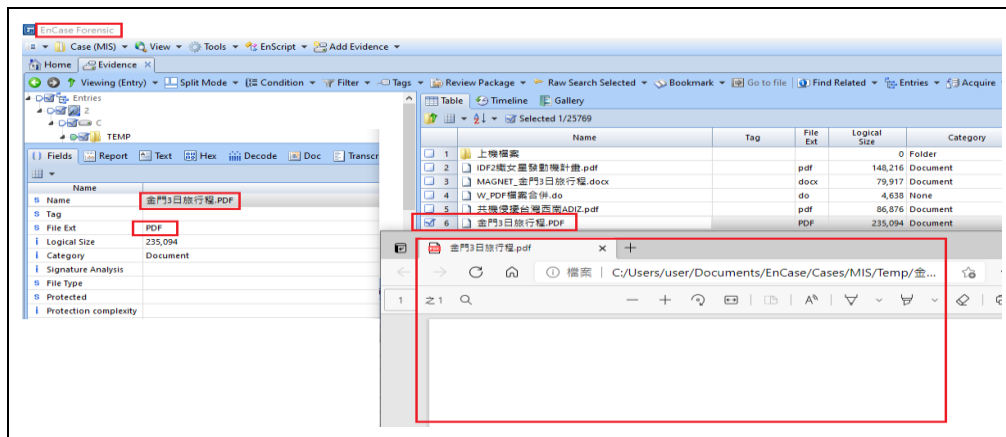
- (2) 撰寫 STATA ADO 程式碼，依序匯入這兩個 PDF 檔案，然後將它們合併 (Merge) 成一個字串，最後再儲存為「金門 3 日旅行程.PDF」。這個檔案即為文字隱碼後的檔案 (載體)。
- (3) 啟動 EnCase Forensic 數位鑑識軟體，發現「金門 3 日旅行程.PDF」內容是空白的，即無法以 Search/Find 功能和輸入關鍵字來找到匹配的內容，如圖七所示。



圖五：瀏覽「IDF2織女星發動機計畫.PDF」內容



圖六：瀏覽「共機侵擾台灣西南ADIZ.PDF」內容



圖七：「金門3日旅行程.PDF」檔案內容（呈現空白）

2.3 程式碼

有關「金門3日旅行程.PDF」檔案（載體）透過檔案還原技術，將它還原

回「IDF2 織女星發動機計畫.pdf」、「共機侵擾台灣西南 ADIZ.pdf」之 ADO 程式碼如下：

```
// STATA ado program  START

clear all

capture program drop DigitalCodeConversion

program define DigitalCodeConversion, rclass

    syntax, 輸入(string) 輸出(name) //call by name

    scalar HexCode = strupper("`輸入"')

    matrix M = J(200,1,,)

    local theLetter 0 1 2 3 4 5 6 7 8 9 A B C D E F

    scalar theLen = length(HexCode)/2

    scalar i = 1

    scalar theIndex = 1

    while theIndex <= theLen {

        scalar theFirst = substr(HexCode, i,1)

        forvalues k = 1/16{

            if word("`theLetter'", `k') == theFirst {

                matrix M[theIndex,1] = 16 * (`k' - 1)

                continue, break

            }

        }

        scalar theSecond = substr(HexCode, i+1,1)

        forvalues k = 1/16{

            if word("`theLetter'", `k') == theSecond {

                matrix M[theIndex,1] = M[theIndex,1] + (`k' - 1)

            }

        }

        scalar i = i + 2

        scalar theIndex = theIndex + 1

    }

end
```

```

        continue, break
    }
}

scalar i = i + 2

scalar theIndex = theIndex + 1
}

matlist M

scalar theCharList = ""

scalar i = 1

while M[i,1] != . {

    scalar theCharList = theCharList + "char(" + strofreal(M[i,1]) + ") + "

    scalar i = i + 1

}

scalar theCharList = substr(theCharList, 1, length(theCharList) - 2)

return local `輸出' = theCharList //輸出是 name

end

///// ado program  END //////////////////////////////////
////////////////////////////////////

// Call Procedure name: DigitalCodeConversion

Local PDF_file_signature_head

"255044462D312E350D0A25B5B5B50D0A312030206F626A0D0A"

DigitalCodeConversion, 輸入(`PDF_file_signature_head') 輸出(DecCode)

scalar theHiddenContentFile = fileread("E:\金門3日旅程.PDF") //import the hidden file

global Second_file_signature_head = strpos(theHiddenContentFile, r(DecCode))

display "The Second file signature head position = ", $Second_file_signature_head

////////// Save the second PDF file

clear

set obs 1

generate strL theSecondFileContent = substr(theHiddenContentFile, $Second_file_signature_head, .)

outfile using "E:\共機侵擾台灣西南 ADIZ.PDF", noquote replace

////////// Save the first PDF file

clear

set obs 1

generate strL theFirstFileContent = substr(theHiddenContentFile, 1, $Second_file_signature_head)

outfile using "E:\IDF2 織女星發動機計畫.PDF", noquote replace

```

當執行上述 STATA 的 ADO 程式碼後所產生的結果，如圖八所示。透過

Adobe 軟體開啟它們，發現與正本檔案內容、編輯格式等完全相同。



圖八：「金門3日旅程.PDF」還原回來的兩個 PDF 檔案內容

五、結論

資訊隱藏技術對資通安全帶來善的力量，也伴隨著惡的力量。文字隱碼術乃利用檔案結構狀態的改變，使得可隱藏大量資訊。如果用於惡，預期將給資安設備偵測能力帶來極大衝擊和提高科技犯罪執法難度。本研究透過實驗法和撰寫程式碼，讓文字隱碼術易於自動化實踐。有關本研究結論歸納如下：

- (1) Microsoft Office 2010 以上版本的各種軟體，均可作為文字隱碼很好的載體工具。它們對資安的最大威脅在於可承載不限容量大小的隱藏檔案、編碼與其各種檔案類型(如 txt、exe、docx、com、dll、xlsx 等)。
- (2) PDF 檔案結構具有文字隱碼特性。它可讓載體承載不限容量大小的全形文字。當由 Adobe 或其他軟體開啟 PDF 載體後，內容呈現空白。
- (3) 實驗結果，證明本研究所提出的文字隱碼術，將帶給現今數位鑑識工具和資安設備的技術上挑戰。
- (4) 總之，文字隱碼猶如水，水能載舟，亦能覆舟。

參考文獻

1. 馮建榮、彭煒琳，「資安大會登場台灣資安產值 2025 估達 780 億」，工商時報 2021/05/05，<https://www.chinatimes.com/newspapers/20210505000128—260202?chdtv>。
2. 資訊保安，「瑞士軍刀病毒：金融木馬程式 Vawtrak 正募集全球用戶密碼」，unwire.pro 2015，<https://unwire.pro/2015/03/26/banking-trojan-vawtrak-harvesting-passwords-worldwide/security/>。
3. 潘天佑，資訊安全概論與實務，第二版，臺北：碁峰資訊 2012，第 7 章第 9 頁。
4. 趨勢科技全球技術支援與研發中心，「垃圾郵件攻擊鎖定日本，使用圖像隱碼術散佈，BEBLOH 金融木馬程式」，2018，<https://blog.trendmicro.com.tw/?p=57932>。
5. AVG Signal Team, “Analysis of Banking Trojan Vawtrak,” 2015, <https://www.avg.com/en/signal/analysis>

- is-of-banking-trojan-vawtrak.
6. Kumar, A., Pooja, Km., “Steganography- A Data Hiding Technique,” International Journal of Computer Applications (0975-8887) (9: 7) 2010, pp: 19-23.
 7. Kumar, P., Sharma, V.K., “Information Security Based on Steganography & Cryptography Techniques: A Review,” International Journal of Advanced Research in Computer Science and Software Engineering (4: 10) 2014, pp: 246-250.
 8. Montalbano, E., “Forrester: Microsoft Office in no danger from competitors,” IDG News Service 2009, <https://www.computerworld.com/article/2523017/forrester--microsoft-office-in-no-danger-from-competitors.html>.
 9. Morran, M., Weir, George R.S., “An Approach to Textual Steganography,” Tenreiro, S. de Magalhães, Jahankhani, H., Hessami, A.G. (Eds.): ICGS3 2010, CCIS 92, pp: 48-54.
 10. Por, L.Y. , Wong, K., Chee, K.O., “UniSpaCh: a text-based data hiding method using Unicode space characters,” Journal of Systems and Software (85: 5) 2012, pp: 1075-1082.
 11. Rehman, A., Saba, T., Mahmood, T., “Data hiding technique in steganography for information security using number theory,” Journal of Information Science 2018, <https://doi.org/10.1177/0165551518816303>.

疫情下的 VDI 替代方案

范修維

世新大學資訊管理學系講師

fan@mail.shu.edu.tw

郭明煌

世新大學資訊管理學系副教授

mhguo@mail.shu.edu.tw

摘要

疫情期間如何停課不停學，讓無法到校學習的學子可以得到優質的遠距學習環境，是教育界的重要課題。在電腦相關課程的教學上，VDI (Virtual Desktop Infrastructure) 系統提供了莫大的助益，學生即使在家學習，也能使用校內的軟體資源，讓學習上無障礙。但是 VDI 系統需要長時間的規劃與建置，也需要投入高昂的預算經費，並非一蹴可幾。本文提出一個 VDI 替代方案，透過簡易的系統開發，搭配 Twice NAT (Network Address Translation) 的操作，就可以將學校電腦教室的個人電腦轉換為雲端電腦，在課餘時段提供師生遠距使用，達到 VDI 同樣的效果。此外，若將 Twice NAT 機制加以運用，還可以免除 KMS (Key Management Service) 驗證程序中的 VPN (Virtual Private Network) 連線需求，甚至改善部份網路間頻寬不足所造成的傳輸壅塞問題。

關鍵字: Twice NAT、VDI、Connection Broker。

一、簡介

雲端服務為資訊發展趨勢，舉凡虛擬機器、儲存空間、資料庫、數據分析、機器學習、乃至各類型的應用，都在雲端服務的提供範圍。它可以讓用戶透過網際網路選擇自己所需要的服務，並且隨選即用、依量計價，提供便利與彈性。這些服務中，雲端桌面為後起之秀，各大公有雲紛紛開始提供這類型服務，例如：AWS 的 WorkSpaces[1]、Azure 的 Windows Virtual Desktop[2]、GCP 的 Virtual Desktops[3]，透過這些服務，組織企業的員工可以在任何地點、任何時間存取雲端桌面，即使下班後需要回家繼續工作，也可以輕鬆連上雲端桌面，接續辦公室未完成的工作。

過去員工如果希望下班後可以在家把尚未完成的工作接續完成，就必須透過 VPN (Virtual Private Network) 服務連線回到組織內部，再用遠端桌面功能連上自己工作崗位的個人電腦，這種使用方式常因為 VPN 連線問題而造成困擾。此外員工為了隨時可連回工作崗位的個人電腦，下班時就不能將電腦關閉，這也造成了電力浪費。如果採用雲端桌面服務，員工不僅可以免除 VPN 連線的困擾，也可以在需要使用時才開啟雲端桌面服務，既環保節能，又可節省租賃費用。

公有雲提供雲端桌面服務的確可以為組織企業帶來彈性與便利，但如果在高度使用率的情形下，公有雲的租賃費用可能大於自行建置的費用，再加上資料存放的安全性及適法性議題，讓部分組織企業選擇自建方案。組織企業可自建私有雲並提供雲端桌面服務，這種方式通稱為 VDI (Virtual Desktop Infrastructure)，目前業界常見的 VDI 解決方案有 VMware Horizon、Citrix XenDesktop 以及 Microsoft VDI Suites。這些方案雖然是成熟的產品，但建置的技術門檻偏高，通常需要專業廠商協助規劃、建置與維護，組織企業才得以擁有 VDI 服務。

因為 VDI 建置的複雜性，從需求訪談、方案規劃、驗證測試、經費估算，再到預算編列、招商採購、組裝設定、運轉測試、細部調校，最後才能正式上線，提供穩定服務。整個過程數以月計，甚至超過一年，非常費事耗時。在建置成本方面，除了需要採購符合 VDI 產品規格的伺服器主機、GPU (Graphics Processing Unit) 加速卡、儲存裝置、網路交換器等硬體設備，還需付出 VDI 軟體授權、GPU 虛擬化授權、作業系統與資料庫授權等費用。雖然建置 VDI 需要付出許多人力、物力，但是其所帶來的效益讓部分學校投入 VDI 建置。學校在擁有 VDI 系統後，不僅可以提供

軟體共享服務，節省軟體授權費用，也可以快速佈署電腦桌面以更新教學環境，更能讓師生於課後、家中使用與上課相同的桌面環境，增加學習便利性。

在疫情期間，已擁有 VDI 環境的學校可以提供被隔離或滯留海外的學生更方便的學習管道，這些學生只要使用學校的 VDI 服務，就可以使用學校的授權軟體，存取校內網路資源，在學習、互動等各方面，都與在校學生無異。只是疫情爆發極為突然，在疫情爆發後才開始規畫 VDI 已緩不濟急，加上境外學生的流失造成學校收入短缺，學校不一定能投入足夠的經費建置 VDI 環境。但是各校普遍擁有電腦教室，如果可將這些電腦教室的個人電腦轉變成雲端電腦，就可以提供與VDI相同的服務。

讓學校的電腦可以遠端使用，並非單純開啟遠端桌面就能完成。它的重點不在於連線方式，而在於電腦的借用、歸還程序，以及保障使用期間不被其他用戶搶奪使用權。這些機制才是雲端桌面服務的管理核心工作。

本文後續將提出一個實作機制，可以將實體電腦轉換為雲端電腦。該建置方式不僅快速，更重要的是，它的建置成本極低，幾乎無需額外的費用支出。即使在疫情過後，對於經費較為拮据的學校，也可參考本文的方法，建置出VDI替代方案。

二、VDI分類

VDI 類型可以分為 Persistent 與 Non-Persistent 兩種，說明如下：

第一種 Persistent 類型為專屬式，特定用戶配置特定桌面，桌面可保留用戶的資料與環境設定，斷線後再行借用，仍然得到相同的桌面，可以接續先前的工作環境，這種方式適合長期固定工作的員工使用。

第二種 Non-Persistent 類型為共享式，用戶所取得的桌面並非固定，桌面資料或環境設定會隨著用戶歸還而消失，重新借用後會得到新的桌面及初始環境，這種方式適合不固定人員的共享使用，例如：輪班或客服人員使用。

本文所提出的方式可以將實體電腦轉換為雲端電腦，供用戶遠距使用。一般而言，電腦教室的個人電腦大部分具有防護措施（例如：還原系統，電腦重開機之後就還原為管理預設環境），這類型的電腦在雲端化之後，就

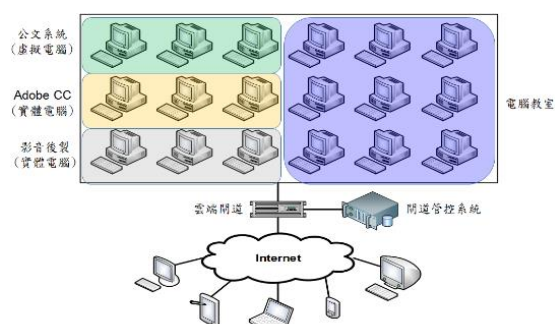
成為第二種 Non-Persistent 模式。如果將員工工作專屬的個人電腦雲端化，就要配置為第一種 Persistent 類型，讓該電腦只能由所屬員工使用。

三、VDI替代方案

本節將介紹VDI替代方案之佈建環境及使用技術、系統佈建流程、系統佈建成果。

1. 佈建環境及使用技術

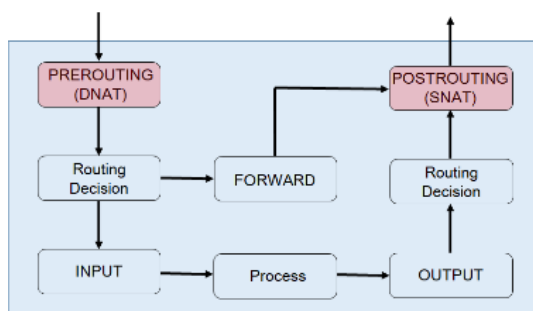
將實體電腦雲端化的重要工作，就是將校內個人電腦提供給用戶遠距使用，並且進行借還管制，避免未經授權使用以及借期屆滿時強制歸還。圖一為本文實作的架構圖，透過一台雲端開道伺服器將後端電腦（可為實體電腦、亦可為虛擬電腦）提供給用戶連線使用，並利用開道管控系統提供借用/歸還等操作，並對雲端開道進行連線管控。在雲端開道部分，利用 Twice NAT (Network Address Translation) 技術，將後端電腦提供給前端用戶連線使用。所謂 Twice NAT 就是在進行位址轉換時，同時將來源 IP、Port 號及目的 IP、Port 號同時進行轉換。也就是將「用戶裝置→雲端開道」的傳輸轉換為「雲端開道→後端電腦」的傳輸，使得後端電腦在回應時，可將「後端電腦→雲端開道」的傳輸轉回「雲端開道→用戶裝置」，如此便完成了用戶裝置與後端電腦的連線代理功能。事實上，業界常見的 VDI 解決方案也會有類似的裝置，並稱之為 Connection Broker。



圖一：實體/虛擬電腦雲端化架構圖

圖二為 Linux 系統的 iptables 架構圖，利用 PREROUTING 的 DNAT 機制進行目的 IP、Port 號轉換，再利用 POSTROUTING 的 SNAT 機制進行來源的 IP、Port 號轉換，就能

達成 Twice NAT 的實作。當用戶端向雲端開道發出連線請求時(不同埠號對應到不同的後台電腦)如表一所示，經過雲端開道的 Twice NAT 轉換之後，連線請求內容更改如表二所示。此 Twice NAT 可在 Linux 作業系統以 iptables 指令實作如表三所示，其中 \$ip1 為用戶端裝置位址，\$port1 為雲端開道所指派的埠號，\$ip2 為後台所對應的雲端電腦，\$port2 為連線通訊協定的埠號。



圖二：Linux 系統的 iptables 架構圖

表一：用戶端向雲端開道發出連線請求的內容

項目	內容
來源位址	用戶裝置
來源埠號	用戶裝置隨機產生的埠號
目的位址	雲端開道
目的埠號	雲端開道所指派的埠號

表二：連線請求經過雲端開道 Twice NAT 轉換後的內容

項目	內容
來源位址	雲端開道
來源埠號	雲端開道隨機產生的埠號
目的位址	所對應的後台電腦
目的埠號	連線通訊協定的埠號 (RDP 連線：3389，RGS 連線：42966)

表三：Twice NAT 在 Linux 作業系統實作的 iptables 指令

項目	指令
設定 MASQUERADE (SNAT)	<pre> /sbin/iptables -t nat -A POSTROUTING -p tcp --dport 3389 -j MASQUERADE </pre>
	<pre> /sbin/iptables -t nat -A </pre>

	<pre> POSTROUTING -p tcp --dport 42966 -j MASQUERADE </pre>
開放用戶端連線 (DNAT)	<pre> /sbin/iptables -t nat -A PREROUTING -p tcp -s \$ip1 --dport \$port1 -j DNAT --to \$ip2:\$port2 </pre>

雲端開道只要允放或拒絕用戶裝置的連線，就可以達到連線管控的目的。

在開道管控系統部分，需要學校自行撰寫程式，以提供師生借用/歸還後台電腦，並將借用/歸還的程序透過 Web Services 轉發至雲端開道，以設定 Twice NAT 轉換規則，來達到管控用戶裝置對後台電腦的連線。開道管控系統可依學校政策需求，來實作連線時間、是否得以展延、每位使用者同時借用數量上限等，甚至與教務系統的課表結合，達到更精細的管控。除了傳統的網頁界面程式提供借還服務外，還需要執行定期排程或背景監控程式，以偵測後台電腦狀態，並且執行關機或預熱等節能需求。

在後台電腦的控制部分，用戶歸還所借用的電腦後，後台電腦應予以重新開機以確保所有資料及環境變更皆已清除，並將電腦回復成預設狀態。前者可以透過 Windows 作業系統的 net rpc 呼叫 (或安裝 sshd 或同質性程式來接受遠端重開機操控) 來實作，後者可以透過電腦的硬體還原卡或軟體還原系統來完成。後台電腦應限制 RDP、RGS 的連線，只允放來自雲端開道的連線請求，以避免用戶裝置或其他電腦以未受管控的方式對後台電腦進行連線。此外，其他通訊埠 (如網路芳鄰) 亦應予以限制，以避免後台電腦的資訊被不當揭露。

在連線工具部分，用戶裝置可採用 Windows 系統內建的遠端桌面連線程式 mstsc.exe 進行連線。或者，當需要高流暢度或 3D 繪圖需求時，可採用 HP RGS 連線軟體進行連線。HP RGS 軟體可採用網路最大同時連線數的授權方式，這樣就可以在所有後台電腦上安裝 HP RGS 軟體，只要同時連線數未超過授權數量，皆可正常使用。

在雲端電腦節能及預熱部分，後台電腦應開啟網路喚醒 (Wake On Lan，簡稱 WOL) 的功能，它必須在 BIOS 與 Windows 作業系統同時設定，並且網路路由器啟用直接廣播 (Direct Broadcast) 功能，讓 WOL 封包可從遠

方發送並喚醒後台電腦。在離峰時段，後台電腦可被 net rpc 等遠程呼叫的管控方式予以關機，以達到節能省電的目的。後台電腦只需開啟一定數量的機器，每當用戶借用電腦，就利用 WOL 喚醒其他電腦預熱備用，讓後續借用可即時連線。當用戶歸還電腦後，可將該電腦重開機或直接關機，以達到資訊安全及節能省電的目的。

2. 系統佈建流程

將後台電腦雲端化的建置驟如下：

- (1) 建立雲端開道：雲端開道主要工作為 Twice NAT 轉換，可採用 Linux 作業系統及 iptables 進行實作，另需製作 Web Services 來接受開道管控系統所派發的指令。
- (2) 建立後台電腦環境：這部分主要工作是在現有電腦教室的個人電腦增加管控機制，例如：設定 net rpc 呼叫（或 sshd 遠程操控）、設定防火牆限制、啟用遠端桌面功能、安裝 HP RGS 連線軟體、設定 WOL 遠端喚醒等事項。初期建置可以只提供 RDP 連線服務，待有 3D 或影音流暢度需求後，再評估是否增購 HP RGS 連線軟體。

(3) 開發開道管控系統：開道管控系統並不需要建立獨立伺服器，可在學校現有的校務資訊系統新增功能，例如：電腦狀態列表、電腦借用/展延/歸還等。這部分可考量學校系統開發的人力資源來評估系統功能的規模，如果人力資源不足，可以只建立核心部分（借還系統），其餘附加項目（如：能源管理、狀態監控、故障維修、假日彈性開放等）可暫不開發。

3. 系統佈建成果

本案已在國內某學校完成實作，在該校機房內設置數台實體個人電腦及數台虛擬電腦，固定 7x24 全天候開放供師生隨時借用。另選定一間電腦教室進行設定，在夜間及假日時段加入支援，提供師生借用。圖三為某校的實際建置畫面，全校師生可透過學校行政資訊系統查詢後台電腦的可借用狀態，再依用戶喜好選定所欲借用的電腦，按下「借用」按鈕後，即可進到個人借用的畫面（如圖四所示），並進行後台電腦的連線、展延、歸還或重開機等操作。



圖三：雲端電腦列表



圖四：個人借用列表

4. 分析與討論

本節將討論技術分析與成本分析，與本研究系統佈建方法之限制。

1. 技術差異分析

在架構上，本文所提出的建置方法與一般業界 VDI 解決方案大致相同，差別僅在於實作方法。業界 VDI 解決方案為封閉式系統，其實作方式並未公開，學校必須付費購買其軟體；而本文所提出的方式為開放式架構，只要能提供 Twice NAT 機制的系統，皆可完成雲端開道的實作。

在開道管控系統方面，因為得以與學校資訊系統緊密結合，可以提供比業界 VDI 解決方案更符合學校生態的管理方式，例如：配合教室閒置時段開放遠端連線使用。

在後台電腦方面，業界 VDI 解決方案需要建置專屬伺服器並以伺服器虛擬化的方式動態建立虛擬桌面，並在歸還時刪除虛擬桌面以確保使用者的資訊安全。本文所提供的方式則不限制是否使用虛擬機器，即使實體電腦一樣能納入提供雲端桌面的服務。使用者在歸還電腦後，利用電腦上的還原系統及重開機程序，就能確保使用者的資料不被外洩。

在雲端電腦的軟體安裝與派送方面，業界 VDI 解決方案採用虛擬機器原始母檔的鏈結或複製方式來佈署雲端桌面，使用者登入雲端桌面時，以個人帳戶進行登入，可擁有個人的環境設定。這種方式佈署雖然方便快捷，但受限於只能使用虛擬機器，不能套用在實體電腦。對於某些特殊軟體在安裝時會綁定安裝者的帳戶，甚至會綁定電腦的特定機碼(如主機板的 UUID、網路卡的卡號)，這類特殊軟體在業界 VDI 解決方案就會無法使用。

本文所提供的建置方式可同時使用虛擬機器或實體機器作為雲端桌面。在虛擬機器方面，可比照業界 VDI 解決方案，先製作原始母檔，再以鏈結或複製的方式來佈署雲端桌面；在實體機器方面，可以按照電腦教室既有的管理機制進行軟體安裝與派送(例如：採用網路軟體複製、採用硬碟複製機複製、採用逐台電腦進行軟體安裝與設定等)。實體電腦教室軟體安裝的方式具有多樣性且有彈性，對於特殊軟體的安裝都能找到對應的解決方法，在安裝後只要套用本文所提出的雲端化機制後，這些電腦就可以轉換成為雲端桌面，提供

師生遠端使用，克服了業界 VDI 解決方案所無法解決的問題。

2. 成本差異分析

在建置成本上，本文所提出的方式是將已存在的電腦雲端化，不管是實體電腦或虛擬電腦皆可，只要利用這些電腦的閒置時段即可提供服務；換言之，無需額外費用建置後台電腦。當然，如果希望提供全天候的雲端桌面服務，就必須配置專屬機器，不管是實體電腦或虛擬電腦。但這類機器不必使用高階伺服器主機，可以使用一般個人電腦，大幅降低硬體成本。

在雲端開道部分，因其工作負荷極低，可使用電腦教室汰換下來的良品電腦來實作；或者，在豎有的伺服器虛擬化主機上切割些許資源(例如：1 vCPU、4G vRAM、30G vHD)以安裝 Linux 系統。這部分的建置成本亦近乎零。

在開道管控系統部分，如果學校的校務資訊系統為學校自行開發，則只要加掛新開發的程式即可；或者，比照雲端開道，使用電腦教室汰換下來的良品電腦擴充記憶體、加裝固態硬碟，一樣可以提供足夠的效能以因應所需服務。

在軟體部分，業界 VDI 解決方案需要高昂的授權費用，不僅連線代理伺服器要依據連線數量來計費，而且需要多台管理伺服器，這些伺服器又需要額外的作業系統及資料庫授權費用。反觀本文所提出的方案，雲端開道可安裝免費版本的 Linux 系統，開道管控系統可依附在豎有的校務資訊系統，完全無需額外軟體費用。

若考量 GPU 的提供，業界 VDI 解決方案需要在伺服器加裝專用的顯示卡，每張顯示卡動輒數十萬元，伺服器主機也必須符合指定規格的機種，另外還需要額外的 GPU 虛擬化授權租賃費用。反觀本文所提出的方案，只需購置 HP RGS 軟體，視所欲提供同時連線數採購即可，大幅降低所需建置成本。

在管理上，業界 VDI 解決方案需要該產品的專業技術人員，才能解決系統維運所面臨的各種狀況。學校人員若欲自行維運，其學習門檻極高，學習時間極長，同時必須從各種問題中逐步累積經驗。反觀本文所提出的方案，

僅有一台雲端開道及開道管控系統，相對單純，且皆為學校自行建置，只要系統能上線運行，日後的維護幾乎無需額外學習。

3. 佈建方法限制

然而，本文的方法所面臨的最大挑戰，就是學校是否有自行開發資訊系統的能力，以及足夠的 Linux 及網路系統管理能力。以學校生態而言，前者屬於統開發組，後者屬於網路管理組，二組之間能否有效溝通與良好合作，亦是成功與否的關鍵。

除了雲端開道及開道管控系統的建置與維運外，實體電腦教室的管理也需注意，在夜間或假日節能時段，電腦教室的散熱，以及電腦使用時數的增加所帶來的電力消耗也應予以評估。

對於課間空堂的動態時段開放，需留意實體電腦的人員接觸，當實體電腦開放為雲端桌面提供服務的同時，實體電腦若被人員由本機登入，遠端桌面連線將被本機人員搶走，造成資訊或隱私被不當揭露。基本上，實體電腦不應同時開放本機使用及遠端連線使用，在開放遠端連線使用時，應對實體電腦進行管制(例如：電腦教室的門禁管制)。

對於電腦當機所造成的不受控問題，若無額外配套措施，只能人工處理，開道管控系統可實作偵測電腦狀態，若出現不受控情形，則以適當方式(如 E-Mail、Line Notify 等)通知管理人員。當然，如果加裝網控型電力排插，就可以在電腦不受控時，強制予以斷電再復電，讓電腦回復正常。

另外，日前 Adobe 公司發布新授權政策[4]：裝置授權只能用於實體電腦，對於虛擬電腦的用戶，都必須具有實名授權。換言之，如果學校欲提供全校師生透過業界 VDI 解決方案使用 Adobe 軟體，就必須為全校師生每人配發一個實名授權。基本上，這費用對學校幾乎是天文數字，學校只能被迫從雲端桌面移除 Adobe 軟體，但這也變成全校師生只能到學校單機操作才能使用 Adobe 軟體。這對各校先前透過 VDI 雲端桌面所建置的軟體雲服務而言，無疑是一大打擊。反觀本文所提出的建置方式，將實體電腦雲端化，仍可使用裝置授權提供 Adobe 遠端使用的服務，完全不受 Adobe 授權政策改變的衝擊。

本文所提出的方式若稍作修改，還可以支援學校解決更多問題。例如：在疫情封鎖時期，一些滯留在境外無法回台的師生，若其電腦需要執行 Windows 或 Office 的 KMS (Key Management Service) 驗證，傳統作法須使用 VPN 連回學校，再執行 KMS 驗證程序。但 VPN 連線常因為 IP 分享器或 NAT 等網路裝置影響其連線，造成師生在驗證過程中的困難。利用本文所提供的 Twice NAT 機制，只要將 KMS 驗證請求轉發至校內 KMS 伺服器，就可以完成 KMS 驗證。當然，為避免 KMS 驗證被校外人士所濫用，可運用開道管控系統加以管制。圖五為本案在某校的 KMS 服務實作畫面。

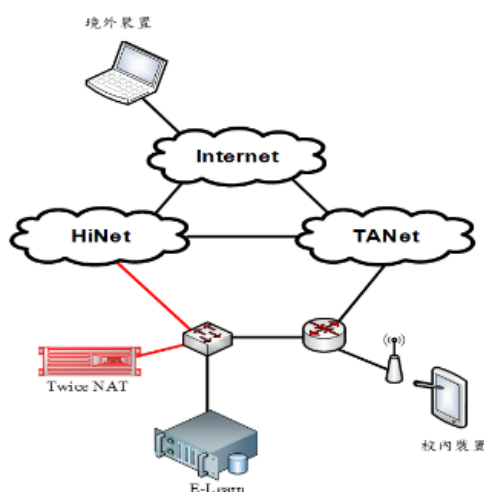


圖五：雲端KMS服務

在疫情期間，一些滯留境外的學子採用遠距學習的方式繼續修讀課程，但因為大陸地區對 TANet 的頻寬過於壅塞，導致對岸學子在使用校內遠距教學系統的連線品質過差，不僅畫面會破圖，聲音也卡頓，學習品質大幅下降。部分學校租用了 HiNet FTTB 線路避開了 TANet 的壅塞瓶頸，但校內的遠距教學系統卻被迫更換 IP 位址，將原來對外走 TANet 的線路改走 HiNet 線路。這種方式雖然可行，但學校網路必須配合調整，否則校內師生存取遠距教學系統時，會出現由原先的「校內裝置→校內路由器→遠距教學系統」路徑變成「校內裝置→校內路由器→TANet→HiNet→遠距教學系統」的繞路現象，反而增加校內師生使用上的延遲。

如果以本文所提出的機制，比照雲端開道，建置 Twice NAT 轉換系統，一端接 HiNet FTTB 線路，另一端接校園網路，這樣境外學子就可以走「用戶裝置→Internet→HiNet→遠

距教學系統」避開 TANet 壅塞線路，而校內師生存取時亦不會出現繞路現象，並且遠距教學系統亦無需更換 IP 位址，將所有影響降至最低。當 FTTB 線路退租時，校內主機及網路設定完全無需任何變更，只需將 Twice NAT 轉換系統一併回收即可。圖六為兩岸傳輸瓶頸的解決方案架構圖。



圖六：利用 HiNet FTTB 解決兩岸傳輸瓶頸 (紅色為增建部分)

表四是由大陸某地區學生對國內某學校進行傳輸測試，測試時段是在傍晚網路流量尖峰時期，若走 TANet 線路，傳輸速率僅 2.5 KB/s，若改走 HiNet FTTB 線路，傳輸速率提高至 32 KB/s，二者相差 12.8 倍。若以此數據估算，走 TANet 線路一小時僅可傳輸 9MB 的資料量，幾乎改無法傳送影音訊息；改走 HiNet 線路則可傳輸 115MB 的資料量，不僅音訊傳輸不成問題，甚至可傳送低畫質的影音教學資料。在非尖峰時段，大陸地區對該校傳輸甚至可超過 100 KB/s，對遠距學習幾乎已無影響。

表四：由大陸某地區學生對國內某學校進行傳輸測試

傳輸路徑	傳輸速率
大陸→TANet (1G/1G)→ 國內學校	2.5 KB/s
大陸→HiNet (1G/600M)→ 國內學校	32 KB/s

5. 結論

本文提出了一個傳統 VDI 的替代方案，可將學校電腦教室的實體電腦在課餘時段雲端化，轉換成雲端電腦供師生遠端連線使用。建置成本極低，僅需二台電腦，無額外軟體授權需求。在建置時程上，僅需些許程式開發時間，相較於重新規劃傳統 VDI 的解決方案，可大幅縮短建置時程，並省下鉅額建置經費。

在疫情期間缺乏人力、物力的情形下，本文所提出的方式可讓學校快速提供雲端桌面服務，以及免去 VPN 連線進行 KMS 驗證，並提供克服大陸地區對 TANet 傳輸瓶頸的解決方案，讓滯留於海外的學子得以提高遠距學習的品質。

參考文獻

1. Amazon, "Amazon WorkSpaces," <https://aws.amazon.com/tw/workspaces/>, Last Retrieved April 2, 2021.
2. Microsoft, "Windows Virtual Desktop," <https://azure.microsoft.com/zh-tw/services/virtual-desktop/>, Last Retrieved April 2, 2021.
3. Google, "Virtual Desktops," <https://cloud.google.com/solutions/virtual-desktops>, Last Retrieved April 2, 2021.
4. Adobe, "Technical support boundaries for virtualized or server-based environments," <https://helpx.adobe.com/enterprise/kb/technical-support-boundaries-virtualized-server-based.html>, Last Retrieved April 2, 2021.

惡意程式分析流程之研究

郭明煌

世新大學資訊管理學系副教授

mhguo@mail.shu.edu.tw

廖鴻圖

世新大學資訊管理學系教授

htliaw@mail.shu.edu.tw

林翔哲

世新大學資訊管理學系研究所碩士生

im12905@gmail.com

摘要

在現今網路蓬勃發展下，隨著使用網路的頻繁隨之而來的惡意程式也越來越猖獗，若沒有對惡意程式有深度的了解，不容易防範惡意程式的為害，導致資安事件發生的狀況。目前對惡意程式的分析都較少討論系統化分析的方法，本研究將提出一個建議流程，讓資訊安全人員在分析惡意程式時可以依據一定的流程，並在最後產製分析報告，以成為後續執行資安防護措施時的參考依據。

關鍵字:資安事件、惡意程式、惡意程式流程分析。

一、簡介

近年來網際網路的發達以及電子商務蓬勃地發展，網路變成人們日常生活中重要服務之一，民眾可透過網際網路與外界溝通獲取新知；企業利用網路提供電子商務等服務網路帶給我們便利的生活，但同時也隱藏著重大的危機。根據 AV-Test 於 2019 年六月的統計報告指出[6]，近年來惡意程式的數量成長率高達約 92.97%，表示使用者即便已安裝相關防護軟體，仍需更加小心提防，以免遭受性能暫時優於防護系統的惡意程式入侵。企業面對不斷演變的資安威脅環境，駭客利用多種惡意軟體和反分析的技術來武裝自己，因此如何有效識別並且分析惡意程式的行為便成為資安人員最重要的任務之一。本研究將建立一套當企業發生資安事故時，所需要的惡意程式分析流程。

惡意程式分析的執行方式與執行效果的好壞，必須要建立一套系統化的流程及方法以便提高後續進行惡意程式分析結果的準確性，目前在市場上雖有一些較有權威性的機構提出一些分析方法如 SANS 及既有的研究資料，眾多方法中都存在著思考不周全的地方，例如分析流程並無系統化的流程而是零散的分析方式、執行分析完後無產製分析報告、分析環境無描述如何建立。

本研究將分析每種執行方法的優缺點，並綜合現今已經提出的執行方法，規劃出一套線下分析的系統化分析流程，讓所有惡意程式分析人員更好入手並改進以往因不同人的分析習慣而導致效益不佳的狀況，希望藉由此方法提升執行惡意程式分析時有一致性的結果，並在最後會產出一份惡意程式分析報告，以利後

續資安防護團隊再進行防護措施時的參考依據。

二、文獻探討

SANS(System Administration, Networking and Security)提出惡意程式分析方法[1]，其目的在提供資安從業人員執行惡意程式分析技術及流程的參考。此方法雖然未提出明確的系統流程、但可對惡意程式分析仍可提供若干幫助。SANS 提出的分析方法的優點，一開始詳細的指導如何建立安全的分析環境，接續的動靜態分析讓研究者明瞭知道自己該如何進行分析。然而該方法沒有明確的系統化的流程，也未產置最後的分析報告。如果一套分析方法沒有系統化的流程，會導致從業人員一開始不知道要應先進行靜態分析，還是先執行動態分析，或行為分析等。另外，最後缺少報告產製，減少駭客利用系統的何種弱點來進行攻擊或是否有惡意中繼站(C&C Server)的說明，對資安防護團隊提升系統的安全及防護的協助有限。

學者 Ilker Kara 提出一套執行惡意程式分析架構[2]，該架構可以幫助資安從業人員在進行惡意程式分析時，以系統化的方式作業。此篇是以數位鑑識的角度而建立的分析方法，一開始的建立環境是將受害主機當前的狀態導出為映像檔，接續的分析方法則與其他研究無太大差異。該方法提供一次性的分析，提供分析人員參考；然此方法沒有系統化的分析流程，分析後也未產製報告。

學者 Amit Kumar Bindal 與 Navroop Kaur 提出一個動態分析的方法[3]，並建立一套執行惡意程式分析的架構。該架構可以幫助資安從業人員在進行惡意程式分析時，有系統的進行作業，並詳盡地描述動態分析時的環境建立、分析過程。此分析方法依賴沙箱的自動化分析，但是此方法缺少靜態分析的明確說明，也沒有報告產製。

學者 Yudi Prayudi 和 Imam Riadi 提出動靜態分析惡意程式方法[4]，使用動態分析與靜態分析兩種方式建立惡意程式分析方法，希望可以分析惡意程式的行為。與其他方法不同

之處，此方法包含報告產製，對接續資安防護提供相當大助益。然此分析方法缺少系統化的流程描述，也未明確定義實驗環境，在不安全的環境下分析惡意程式將具有相當的風險。

學者 Dolly Uppal、Vishakha Mehra、Vinod Verma 整理惡意程式分析技術與惡意程式分析工具[5]。此研究提出相當多的比較分析方式，如啟發式的惡意行為分析，對偵測惡意程式的機率可以提高。然而此研究未說明環境建置的步驟，也缺少系統化的流程及報告產製。

前述相關研究包含之流程比較如表 1，由表 1 中可看出相關研究對惡意程式分析著重於分析技術或方法，對於流程的涵蓋範圍較有限，因此本研究於提出一套惡意程式分析流程，以作為惡意程式分析標準作業程序(Standard Operating Procedures)之參考建議。

表 1：相關研究比較表

相關研究 比較項目	[1]	[2]	[3]	[4]	[5]
環境建立	O	O	X	X	X
動態分析	O	O	O	O	O
靜態分析	O	O	X	O	O
行為分析	O	O	O	O	O
相似度分析	X	X	X	X	O
混淆判定	O	O	X	O	O
記憶體分析	X	O	X	X	O
報告彙整	X	X	X	O	X
系統化流程	X	X	X	X	X

註：O 表示方法有此流程，X 表示沒有。

三、研究設計

本研究參考相關研究，提出環境建立、混淆判定、靜態分析、動態分析、反調試分析、動態分析、行為分析、記憶體分析、報告彙整等八個步驟的惡意程式分析流程，各流程之內容說明如下：

1. 環境建立：進行惡意程式分析時，因無法確切知道惡意程式會有何功能，如不在隔離的分析環境中處理，則可能導致第二次資安事故的發生。
2. 混淆判定：進行惡意程式分析時，惡意程式有可能會經過混淆處理，以避免惡意程式在短時間內分析完成，所以如果未經過混淆判定的流程進行解混淆，則無法看到原始的程式碼。
3. 靜態分析：進行惡意程式分析時，如先經過靜態分析取得一些重要資訊，如 IP 位址、函式庫，則對後續動態分析及行為分析會有相當的幫助。
4. 反調試分析判定：現今惡意程式常有防止分析功能，在進行行為分析、動態分析、網路行為監測時，惡意程式會判定目前是否有監控軟體在進行監控；如果惡意程式發現監控軟體，可能會自行跳出或不繼續運行惡意行為。所以利用反調試分析判定，再以人工將惡意程式的防止分析功能移除。
5. 動態分析：靜態分析的結果僅能用來輔助後續其他流程的判斷，如未經過動態分析，則無法判定惡意程式實際的功能。
6. 行為分析：行為分析可以確認動態分析結果的正確性，並可透過快速行為分析軟體來幫忙整理惡意程式的行為，加快分析時間。
7. 記憶體分析：如果惡意程式執行後自行消失，則可使用記憶體分析工具將已被加載在記憶體中的程式進行還原，或進行一些基本的字串搜索。
8. 報告彙整：在前述分析步驟完畢後，會將各項分析結果彙整並產製報告，提供資安防護人員防護措施及修補建議。

三、範例說明

以下以某一個惡意程式的分析過程，說明本研究流程之執行過程。

1. 環境建立：本研究利用 VMware 建立一個可以進行惡意程式分析的環境，該環境無法與實體網路進行連接，避免惡意程式在運行時連接到實體網路產生的風險[6][7]。
2. 混淆判定：本研究利用 PEiD 查殼軟體判定程式是否有被封裝或混淆[8]。在使用 PEiD 查殼軟體後發現，該惡意程式沒有被壓縮或混淆，如圖 1 所示該惡意程式並未經過混淆即壓縮處理。
3. 靜態分析：在不執行惡意程式的情況下進行分析[8][9]。

(1) 本研究使用逆向工程軟體分析後，發現到程式碼中有可疑字串 Back Door、sysWork.exe、tar zcvf test.tgz *.docx >1 nul 2>nul，如圖 2、圖 3。

(2) 使用 CEF Explorer 軟體進行分析後，發現到該惡意程式所使用的 dll 函式庫，KERNEL32、USER32、ADVAPI32、WS2_32、VCRUNTIME140D、ucrtbased。



圖 1：本研究範例之混淆判定圖

.rdata:00418...	00000009	C	BackDoor
.rdata:00418...	00000009	C	Autonuns
.rdata:00419...	00000034	C	A variable is being used without being initialized.
.rdata:00419...	00000036	C	A local variable was used before it was initialized.\n
.rdata:00419...	0000011D	C	A cast to a smaller data type has caused a loss of data. If this was intentional, you should ..
.rdata:00418...	00000041	C	<===== Welcome to Back Door > <=====>\n
.rdata:00418...	00000011	C	's was corrupted.
.rdata:00418...	00000028	C	's is being used without being initialized.
.rdata:00419...	0000001A	C	%s\n
.rdata:00419...	00000006	C	%2X

圖 2：本研究範例之靜態分析圖 1

Address	Length	Type	String
.text:0041211F	00000009	C	wMessage
.rdata:00418...	00000025	C	tar zcvf test.tgz *.docx 1>nul 2>nul
.text:00411D33	0000000D	C	szSystemPath
.text:00411D24	0000000F	C	szFileSelfPath
.text:00412AC0	00000008	C	svTable
.text:00411D40	00000010	C	ssServiceStatus
.text:00412117	00000008	C	sClient
.text:00412104	00000008	C	hThread
.text:0041210C	00000008	C	dwThreadId
.text:0041261C	00000008	C	cmdline
.rdata:00419...	00000008	C	\nSize:
.rdata:00419...	00000009	C	\nData: <
.rdata:00419...	0000002A	C	\nAllocation number within this function:
.rdata:00419...	0000000D	C	\nAddress: 0x
.rdata:00418...	0000000D	C	\\sysWork.exe
.rdata:00418...	00000009	C	\\cmd.exe
.rdata:00418...	0000001E	C	[*]Service Operation Success\n
.rdata:00418...	0000001C	C	[!]Service Operation Error\n
.rdata:00418...	0000001A	C	WSAStartup Process Error\n

圖 3：本研究範例之靜態分析圖 2

Output window	
75CB0000:	loaded C:\Windows\SysWOW64\advapi32.dll
76790000:	loaded C:\Windows\SysWOW64\msvcrt.dll
7720E230:	thread has started (tid=7408)
76310000:	loaded C:\Windows\SysWOW64\sechost.dll
770F0000:	loaded C:\Windows\SysWOW64\rpcrt4.dll
74820000:	loaded C:\Windows\SysWOW64\sspicli.dll
74810000:	loaded C:\Windows\SysWOW64\cryptbase.dll
76550000:	loaded C:\Windows\SysWOW64\bcryptprimitives.dll
76250000:	loaded C:\Windows\SysWOW64\ws2_32.dll
7720E230:	thread has started (tid=4064)
F3000000:	loaded C:\Windows\SysWOW64\ucrntime140d.dll
FC000000:	loaded C:\Windows\SysWOW64\ucrntime140d.dll
762E0000:	loaded C:\Windows\SysWOW64\imm32.dll
760B0000:	loaded C:\Windows\SysWOW64\kernel.appcore.dll
Debugger:	thread 4064 has exited (code 0)
Debugger:	thread 8456 has exited (code 0)
Debugger:	thread 7408 has exited (code 0)
Debugger:	process has exited (exit code 0)

圖 4：本研究範例之反調式分析圖 1

.text:00412A05	mov	[ebp+var_4], eax
.text:00412A08 ; 13:	sub	411294(&unk_41D034);
.text:00412A08	mov	ecx, offset unk_41D034
.text:00412A0D	call	sub_411294
.text:00412A12 ; 14: if (!sub_4110B9())		// anti_debug function
.text:00412A12	call	sub_4110B9
.text:00412A17	test	eax, eax
.text:00412A19	jz	short loc_412A1F
.text:00412A1B	xor	eax, eax
.text:00412A1D	jmp	short loc_412A7B

圖 5：本研究範例之反調式分析圖 2

4. 反調試分析判定：分析程式是否有防止行為分析的防護機制，如果有則需要手動將惡意程式進行修補，避免影響行為分析判斷[9]。

{1} 使用逆向工程軟體發現程式會立即跳出，故判定該程式可能有做反調式分析功能，如圖 4。

{2} 使用靜態分析方式分析發現惡意程式有反調試分析機制，需要手動進行修補程式，以利後續動態分析及行為分析。(如圖 5)

{3} 將反調試分析機制的關鍵邏輯判斷點 jz 改為 jnz，再重新編譯成可執行文件。(如圖 6、圖 7)

{4} 修改後發現，惡意程式可在開啟行為分析軟體的情況下正常運行。(如圖 8)

.text:004129FE	mov	eax, __security_cookie
.text:00412A03	xor	eax, ebp
.text:00412A05	mov	[ebp+var_4], eax
.text:00412A08 ; 12:	sub	411294(&unk_41D034);
.text:00412A08	mov	ecx, offset unk_41D034
.text:00412A0D	call	sub_411294
.text:00412A12 ; 13: if (!sub_4110B9())		
.text:00412A12	call	sub_4110B9
.text:00412A17	test	eax, eax
.text:00412A19	jz	short loc_412A1F
.text:00412A1B	xor	eax, eax
.text:00412A1D	jmp	short loc_412A7B

圖 6：本研究範例之反調式分析圖 3

.text:004129FE	mov	eax, __security_cookie
.text:00412A03	xor	eax, ebp
.text:00412A05	mov	[ebp+var_4], eax
.text:00412A08 ; 12:	sub	411294(&unk_41D034);
.text:00412A08	mov	ecx, offset unk_41D034
.text:00412A0D	call	sub_411294
.text:00412A12 ; 13: if (!sub_4110B9())		
.text:00412A12	call	sub_4110B9
.text:00412A17	test	eax, eax
.text:00412A19	jnz	short loc_412A1F
.text:00412A1B	xor	eax, eax
.text:00412A1D	jmp	short loc_412A7B

圖 7：本研究範例之反調式分析圖 4

```

C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.17763.1098]
(c) 2018 Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Users\user\Desktop\分析標的>
C:\Users\user\Desktop\分析標的>malware.exe
Can not Open the Service Manager
[!]Service Operation Error
C:\Users\user\Desktop\分析標的>

```

圖 8：本研究範例之反調式分析圖 5

5. 動態分析：在執行程式的情況下進行流程追蹤[9][10][11]。

- {1} 使用動態分析發現惡意程式會將當前目錄下附檔名為.docx 檔案封裝成 test.tgz，再將檔案移動到上層目錄並改名為 ss 檔案(如圖 9)。
- {2} 使用動態分析發現惡意程式會抹除當前目錄下的所有檔案
- {3} 使用動態分析發現惡意程式先取得 system32 的絕對路徑，再將惡意程式複製到 C:/windows/system32 下，名稱為 sysWork.exe 的檔案。
- {4} 使用動態分析發現惡意程式已將 BackDoor 後門建立為系統常駐服務。
- {5} 使用系監控工具查看後，發現系統被開啟了 port 45000 的後門(如圖 10)。

```

.text:0008288C      rep stasd
.text:0008288E      13: sub_D81294(unk_D80834);
.text:0008289E      mov     ecx, offset unk_D80834
.text:00082899      call   sub_D81294
.text:00082898      14: system("tar zcvf test.tgz *.docx 1>nul 2>nul");
.text:00082898      mov     esi, esp
.text:0008289A      push   offset Command ; "tar zcvf test.tgz *.docx 1>nul 2>nul"
.text:0008289F      call   ds:system
.text:000828A5      15: sub_D8129E(v1, 0);
.text:000828A5      add     esp, 4
.text:000828A8      cmp     esi, esp
.text:000828AA      call   sub_D8129E
.text:000828AF      16: system("mv -f test.tgz ../ss");
.text:000828AF      mov     esi, esp
.text:000828B1      push   offset ahhTest_tgz_$ ; "mv -f test.tgz ../ss"
.text:000828B6      call   ds:system
.text:000828BC      17: sub_D8129E(v3, 0);
.text:000828BC      add     esp, 4
.text:000828BF      cmp     esi, esp
.text:000828C1      call   sub_D8129E
.text:000828C6      18: system("del /Q *");
.text:000828C6      mov     esi, esp
.text:000828C8      push   offset aDelQ ; "del /Q *"
.text:000828CD      call   ds:system
.text:000828D3      19: sub_D8129E(v5, 0);
.text:000828D3      add     esp, 4

```

圖 9：本研究範例之動態分析圖 1

Process Name	PID	System File	Path	Port	Protocol	State
wininit.exe	550	System File	C:\Windows\System32\wininit.exe	TCP	0.0.0.0:48684	TS_Listen
wininit.exe	550	System File	C:\Windows\System32\wininit.exe	TCP	0.0.0.0:48684	TS_Listen
spoolsv.exe	1530	Unknown	C:\Windows\System32\spoolsv.exe	TCP	0.0.0.0:45000	TS_Listen
System	4	System File	System	TCP	0.0.0.0:445	TS_Listen
System	4	System File	System	TCP	0.0.0.0:5357	TS_Listen
System	4	System File	System	TCP	169.254.228.23:139	TS_Listen
System	4	System File	System	TCP	169.168.136.139:139	TS_Listen

圖 10：本研究範例之動態分析圖 2

6. 行為分析：分析惡意程式會產生的行為，例如連線到哪個 IP，或新增移除了哪些檔案[10]。

- {1} 使用行為分析工具分析發現惡意程式將當前目錄下的 docx 文件包裝成 test.tgz，再將 test.tgz 檔案移動到上層目錄(如圖 11、圖 12)。
- {2} 之後發現惡意程式刪除當前目錄下的所有文件(如圖 13)。
- {3} 使用行為分析工具進行分析發現惡意程式將自身程式複製到 C:/windows/SysWOW64 目錄下，且更名為 sysWork(如圖 14)。
- {4} 最後惡意程式將自身註冊成為 BackDoor 的後門，常駐在系統服務中，並在每次開機會自行啟動後門(如圖 15 和圖 16)。
- {5} 使用系統監控工具進行監控發現 sysWork 具有開啟本地的 port 45000 的行為，並成功建立後門(如圖 17)。

電腦\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BackDoor			
		名稱	資料
	amdsata	(預設值)	(數值未設定)
	amdsbs	DisplayName	BackDoor
	amdxata	ErrorControl	0x00000000 (0)
	AppHostSvc	ImagePath	C:\Windows\system32\sysWork.exe
	AppID	ObjectName	LocalSystem
	AppIDSvc	Start	0x00000002 (2)
	Appinfo	Type	0x00000010 (16)
	applockerfltr	WOW64	0x0000014c (332)
	AppMgmt		
	AppReadiness		

圖 16：本研究範例之行為分析圖 6

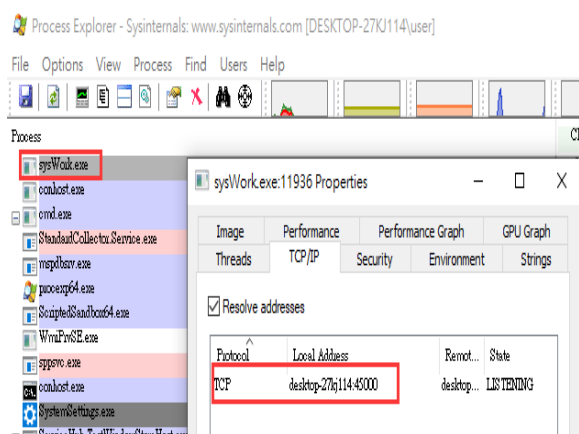


圖 17：本研究範例之行為分析圖 7

圖 18：本研究範例之記憶體分析圖 1

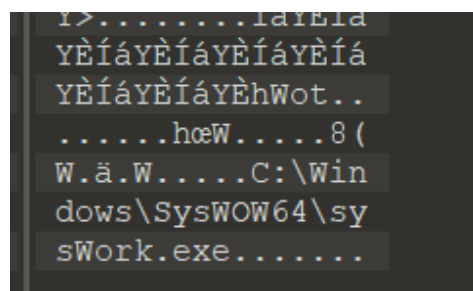


圖 19：本研究範例之記憶體分析圖 2

7. 記憶體分析：萃取在系統運作中的記憶體後進行分析[10][12]。

〔1〕 使用 Procdump 將惡意程式從記憶體中萃取出部分資料(如圖 18)。

〔2〕 使用十六進制編輯器查看萃取出的記憶體資料，發現惡意程式的部分內容(如圖 19)。

分析工具 > Procdump				
搜尋 Procdump				
名稱	修改日期	類型	大小	
Eula.txt	2017/3/13 上午 0...	文字文件	8 KB	
procdump.exe	2017/4/25 上午 0...	應用程式	637 KB	
procdump64.exe	2017/4/25 上午 0...	應用程式	334 KB	
sysWork.exe_200701_121522.dmp	2020/7/1 下午 12...	DMP 檔案	283 KB	

8. 報告彙整：彙整分析結果，以提供建議給資訊安全人員。本實驗之惡意程式分析結果如下：

- 〔1〕 該惡意程式對註冊表進行寫入；
- 〔2〕 將本地的 doc 文件進行打包後刪除原文件，有竊取文件之疑慮；
- 〔3〕 將程式自身註冊為常駐服務；
- 〔4〕 開啟常駐後門。

分析結果之修補建議：

- (1) 建議當程式需要對註冊表進行寫入時須嚴格管控權限；
- (2) 平時使用電腦要採取最小權限原則，勿使用最高管理員身分；
- (3) 需定期對系統常駐服務進行檢查，是否有可疑服務；

(4) 防火牆需進行內對外的端口進行控管。

四、分析討論

以下說明本研究方法與前相關研究[1][2]之比較，如表 2 所示。

1. SANS 惡意程式分析概述[1]：此方法於動靜態分析及行為分析時未檢出程式具有惡意行為，使用靜態分析時有搜查出該程式所使用的動態連結函式庫(DLL)及可疑字串，另外較為敏感的行為只有檢出有 powershell 會被執行，但無法判定惡意程式實際運行時會對系統造成的效果。
2. 惡意程式基礎分析方法[2]：此方法於動靜態分析及行為分析時未檢出程式具有惡意行為，使用靜態分析時有搜查出該程式所使用的動態連結函式庫(DLL)及可疑字串，另外較為敏感的行為只有檢出有 powershell 會被執行，但無法判定惡意程式實際運行時會對系統造成的效果。

本研究方法：此方法在進行靜態分析後，陸續進行反調試分析機制的判定與人工移除該機制，故後續可以使用動態分析及行為分析的方式進行分析，使用靜態分析時有搜查出該程式所使用的動態連結函式庫(DLL)及可疑字串，在進行動態分析時有檢出程式建立植入後門到系統中並寫入註冊表。最後將該惡意程式分析完成，並彙整惡意程式的分析結果。

表 2：分析結果比較表

比較項目	[1]	[2]	本研究流程
靜態分析	檢出疑似惡意字串	檢出疑似惡意字串	檢出疑似惡意字串
反調式分析	無此功能	無此功能	檢出惡意程式具有反調式分析機制
動態分析	未發現	未發現	檢出惡意行為

	惡意行為	惡意行為	為
報告彙整	無彙整	無彙整	檢出惡意行為並彙整惡意行為、提供修補建議
系統化流程	無	無	有

由上述分析可以發現，兩種分析方法[1][2]的分析結果相似，僅檢出有 powershell 會被執行，但無法判定惡意程式實際運行時會對系統造成的效果。本研究的方法可以檢出惡意程式的具體惡意行為。因此推斷前兩套惡意程式分析方法，可以成功分析未具有反調式分析機制的惡意程式，但如果惡意程式有反分析機制的話則無法完整分析出惡意程式的行為。表 3 整理三個分析方法可檢核的惡意程式類型。

表 3：分析方法差異比較表

比較項目	[1]	[2]	本研究流程
勒索病毒	可檢出	可檢出	可檢出
木馬程式	可檢出	可檢出	可檢出
無檔案型惡意程式	可檢出	可檢出	可檢出
具備反調式功能的惡意程式	無法檢出	無法檢出	可檢出
電腦蠕蟲	可檢出	可檢出	可檢出

五、結論

爲了要確實做好資訊安全防護，了解駭客的攻擊手法是必要事項，不僅要分析惡意程式的行為，更重要的是要確實的將分析結果回饋給資安防護團隊進行後續相關防護作業，以免後續遇到類似攻擊手法，或未知的惡意程式攻擊時無法防範。但如無對惡意程式做深度的剖

析就無法進行重點性的防護，因此一個惡意程式分析的流程就顯得特別重要，這樣的流程有助於了解惡意程式的行為，找出資安防護的破口並加以改進。

由於過往的惡意程式分析方法太過於零散，且無系統化的流程，所以經常造成在作業時造成對惡意程式的行為了解的不夠透徹。本研究提出一個惡意程式分析分析流程，並以範例證明可達一定成效，希望本研究之成果可以為資訊安全防護盡一份心力。

參考文獻

1. System Administration Networking and Security, “Malware Analysis: An Introduction,” Available: <https://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103>
2. Ilker Kara, “A basic malware analysis method,” Computer Fraud & Security, Volume 2019, Issue 6, Pages 11-19, 2019
3. Amit Kumar Bindal, Navroop Kaur, “A Complete Dynamic Malware Analysis,” International Journal of Computer Applications, Volume 135, No.4, Pages 11-19, 2016
4. Yudi Prayudi, Imam Riadi, “Implementation of Malware Analysis using Static and Dynamic Analysis Method,” International Journal of Computer Applications, Volume 117, No.6, Pages 11-15, 2015
5. Dolly Uppal, Vishakha Mehra, Vinod Verma, “Basic survey on Malware Analysis Tools and Techniques,” International Journal on Computational Sciences & Applications, Volume 4, No.1, Pages 103-112, 2014
6. HP 惠普科技股份有限公司, “2018 資安指南：駭客與資安專家競相設計與機器學習”， Available: <https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-3530ZHP.pdf>
7. vmware.com, VMware Workstation 15, Available: <https://www.vmware.com/tw/products/workstation-player/workstation-player-evaluation.html>
8. PEID, PEID, Available: <https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml>
9. hex-rays, IDA Pro, Available: <https://www.hex-rays.com/products/ida/>
10. Microsoft Sysinternals suite, Available: <https://docs.microsoft.com/en-us/sysinternals/>
11. x64dbg, x64dbg, <https://x64dbg.com>
12. Sweetscape, 010editor, <https://www.sweetscape.com/010editor/>

智慧型警車攔截圍捕輔助系統之研究

古淳寶

中央警察大學資訊管理所研究生

im1093061@mail.cpu.edu.tw

董正談

中央警察大學資訊管理所助理教授

tung@mail.cpu.edu.tw

鄧少華

中央警察大學資訊管理所教授，通訊作者

pdeng@mail.cpu.edu.tw

摘要

警察追捕逃逸車輛的過程非常危險，時常造成追車員警、被追緝者及第三人的傷亡，因此追車員警應與對方保持安全距離並持續尾隨在後，待支援警力到達後再進行攔截圍捕。然而，警車攔截圍捕實際上有著許多問題，如追車員警必須不斷使用無線電回報目前位置、支援警力對路況不熟悉、勤務指揮中心難以掌握現場狀況等情形，導致攔截圍捕效率低落，甚至造成警車相撞等意外。有鑑於此，本研究使用智慧型警車攔截圍捕輔助系統，以M-Police(警用行動電腦)連結警車行車記錄器，建立攔截圍捕群組，整合定位導航、即時影像、群組對話、車牌辨識、資料分析等功能，自動產生最短路徑導航、車輛及車主資訊等訊息，使所有加入攔截圍捕行動的警力及勤務指揮中心能夠互相配合，快速鎖定逃逸車輛位置，進而順利完成攔截圍捕任務。本研究透過智慧型警車攔截圍捕輔助系統協助警車追逐行動，改善現行攔截圍捕所遇到的問題，期望降低警車追逐造成的傷亡，提升員警執勤的效率及安全性。

關鍵字：執勤安全、定位導航、車牌辨識、資料分析

一、前言

警察依法盤查人車時，若發現犯罪事實、違禁品、危害情況、通緝犯、民眾呼救等情形，且該車駕駛駕車逃逸，即可發動警車追逐以追緝車輛。為了降低意外及傷亡的機率，使用優勢警力進行攔截圍捕是較為適當的做法。然而，想要呼叫支援警力進行攔截圍捕，追車員警必須不斷使用無線電通報目前位置，在高速追逐的過程中可能導致追車員警因分心造成意外；而支援警力僅依無線電所傳遞的訊息進行追捕，若不熟悉路況，便難以追上逃逸車輛；另外在勤務指揮中心方面，因無法掌握現場狀況，除了派遣支援警力之外，難以給予其它實質幫助。本研究為解決警車攔截圍捕行動的諸多難處，使用M-Police連結警車行車記錄器，建立一套結合定位導航、即時影像、群組對話、車牌辨識、

資料分析等功能之智慧型警車攔截圍捕輔助系統，以5G(第五代行動通訊技術)傳輸警車追逐現場的即時影像及位置至攔截圍捕群組，讓勤務指揮中心能夠觀察現場狀況進行指揮調度、支援警力可以依據輔助系統上的最短路徑導航快速跟上逃逸車輛，使追車員警再也無需不斷通報目前位置，加上車牌辨識及資料分析，全方面輔助警車攔截圍捕行動，改善攔截圍捕的效率並降低危險性。

二、研究動機

2018年6月22日警員李孟修駕駛警車支援圍捕機車竊賊，過程中不慎和民眾駕駛的休旅車發生碰撞，導致李員雙手擦傷、該位民眾胸口挫傷；2017年4月23日凌晨發生群眾鬥毆事件，在攔截圍捕逃竄車輛過程中有兩輛警車不慎相撞，導致警

員簡銘韋重傷陷入昏迷，於八十三天後不幸離世。

以上兩起事故均顯示警車攔截圍捕的危險性，在攔截圍捕過程中，支援警力僅依據無線電所通報的訊息行動，不但無法得知目標的確切位置，也不清楚現場狀況，若對路況不熟，極可能在攔截圍捕過程中發生意外，在不清楚自己與目標的距離時，甚至可能於轉角處與目標或友軍相撞，造成無法挽回的後果。

上述案例如能使用智慧型警車攔截圍捕輔助系統支援攔截圍捕行動，將現場的即時影像與定位導航位置傳輸至攔截圍捕群組，使支援警力及勤務指揮中心能夠清楚查看現場情況、目標位置、距離等資訊，並於群組中互相溝通，將能提升警車攔截圍捕的安全性。

三、研究目的

本研究期望改善警車攔截圍捕所遇到的問題，使用M-Police連結警車行車記錄器，以定位導航、即時影像、群組對話等功能強化攔截圍捕群組成員間的聯繫，讓追車員警能專心保持距離尾隨跟車、支援警力可以快速追上目標，並使勤務指揮中心能夠視情況進行指揮調度，加上車牌辨識系統查詢車主資訊、資料分析改善攔截圍捕戰術等功能，全方面強化警車攔截圍捕的效率及安全性。

四、相關文獻及背景知識

本研究之智慧型警車攔截圍捕輔助系統結合定位導航、即時影像、群組對話、車牌辨識、資料分析等功能，以5G傳輸警車追逐現場的即時影像及位置至攔截圍捕群組，以下就相關文獻及背景知識進行探討。

1、第五代行動通訊技術(5G)

作為4G網路的下一代通訊技術標準，5G網路的目標在於提供更高的傳輸速率、減少傳輸延遲、節省基地台能源消耗、降低運作成本、提高系統總容量以及提供更大量的裝置進行連線。相較於4G網路，5G將會透過使用更高頻率的頻段來

達成更高的資料傳輸速率，如30GHz到300GHz的毫米波頻段，透過使用更高頻的波段，比起前一代的通訊技術，資料傳輸速率高達近百倍 [3]。

5G不管在覆蓋率、頻譜效率、延遲優化、傳輸速率上都將比4G高出一個等級，其中連線速率將達到1Gbps。此外，5G網路還定義了萬物皆聯網的概念，智慧機械、自駕車、無人機等都可不必依靠傳統的有線網路，透過物聯網或車聯網以無線訊號進行通訊，相較於4G所運作的700MHz、900MHz、1800MHz、2600MHz等頻段，5G網路預計運作在28GHz及60GHz的極高頻(Extremely high frequency, EHF)電磁波上。由於其物理限制，訊號的穿透力較低，且具有更高的方向性，5G也將需要更密集的基地台佈建[11]。

在應用方面，5G網路將支援更多不同類型的需求，如自動駕駛汽車、無人機及人工智慧等，許多正在發展的技術都須仰賴5G網路的特點才能夠實現。本研究期望透過5G網路的高速資料傳輸速率傳輸警車追逐現場的即時影像及位置至攔截圍捕群組，使支援警力能夠快速並精準的鎖定逃逸車輛，進而在最短的時間內完成圍捕行動。

2、全球定位系統(GPS)

全球定位系統(Global Positioning System, GPS)為美國國防部所發展之涵蓋全球的衛星導航及定位系統，GPS利用接收衛星軌道資料進而解出衛星所在位置，再計算出接收器與衛星之間的距離，以求出接收器所在位置，因此全球定位系統是一套不受時間與天候影響的高精度定位系統，可供全天候24小時做連續位置、相對速度等的訊號輸出[6]。

GPS提供了使用者位置，速度及時間等資訊，其系統基本架構包括均勻散佈於軌道面與赤道成 55 度傾角，高度距地表約 2萬公里上的 24 顆衛星與 3 顆預備衛星，以及三個部門，分別為[4]:

(a) 使用者部門(User Segment):

這部門泛指的是般使用者的各種 GPS 接收機，其用途是用來接收衛星

之訊號並解碼成可提供定位之導航訊息。

(b) 太空部門(Space segment):

此部門指的分佈於太空中的定位衛星，GPS 系統的設計為 24 顆衛星分佈於六個軌道面，軌道平面與赤道夾角為 55 度，而軌道高度約為 20200 公里，因此衛星繞行地球一周約為 12 個小時，因此只要使用者在地球上任何時間、任何地點，能獲得四顆良好的衛星訊號，即可達到三度空間的定位。

(c) 控制部門(Control segment):

此部門由一系列監控站所構成，主要是對 GPS 衛星傳送訊號品質做監控，並適時地修正導航訊息乃至衛星軌道等。

GPS 可以正確提供使用者全球性的定位資訊，且對使用者不加收任何費用，因此全球定位系統已廣泛使用於各個領域，如軍事用途、飛機導航、車輛導航、手機定位等，均以 GPS 訊號作為導航定位。

3、Google 地圖(Google Maps)

Google 地圖(Google Maps)是 Google 公司向全球提供的電子地圖服務，地圖包含地標、線條、形狀等資訊，提供地圖模式、衛星模式、地形模式三種視圖。Google Maps 於 2005 年 6 月 20 日將覆蓋範圍從原先的美國、英國、加拿大擴大至全球。目前在全球多國開通了「街景」(Street View)服務，使用者可以透過由 Google 街景車在街道上拍到的影像檢視街景畫面[1]。

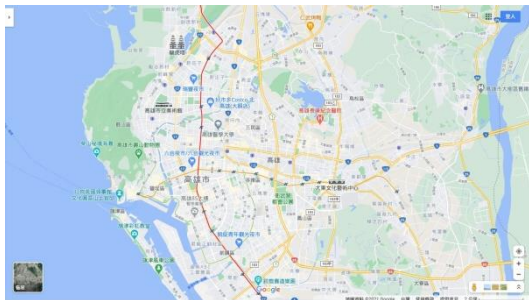


圖1：Google Maps地圖模式

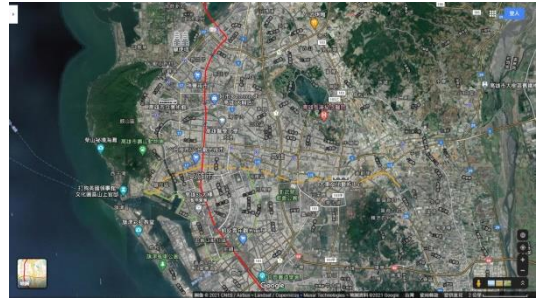


圖2：Google Maps衛星模式

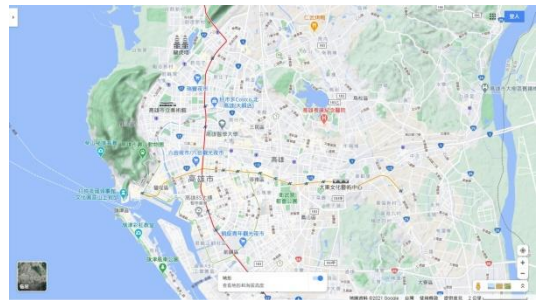


圖3：Google Maps地形模式

4、群組軟體

群組軟體原先稱作協同型軟體(Collaborative software)，為一種電腦軟體，目的在幫助人們完成共同的目標。群組軟體(groupware)一詞，在 1978 年，由 Peter and Trudy Johnson-Lenz 所創立出來，最初的定義為「有目的性質的團隊，運用額外的軟體來支援他們達成任務。」群組軟體所指的範圍相當廣大，與電腦輔助協同工作(Computer-supported cooperative work, CSCW)的定義有若干重疊。活用群組軟體已是現代企業必備的條件之一，在它所提供的協同工作環境中，組織裡獨立的員工可以相互溝通、討論、任務管理，如電子郵件、即時訊息、視訊會議、工作流程管理…等等，即使不是在相同的工作場所，也可以共同合作、相互支援[7]。

群組軟體的應用主要分為三大類[12]：

- (a) 以文件及表格為基礎的群組軟體(document & form-based groupware)：像是電子郵件(E-mail)、工作流程

(workflow)、文件管理(document management)等。

(b) 大量訊息交換的資訊管理群組軟體(transaction-based high-volume information management groupware)：組織成員在資料庫管理(document imaging)中，因溝通合作而有著大量資料交換的過程稱之。

(c) 組織通訊的群組軟體(organizational communications groupware)：此類應用強調組織的溝通和合作像是群體行事曆(group calendar)、視訊會議(video conferencing)、電子會議(electronic meeting)、組織記憶(organizational memory)以及群體創作(group authoring)等。

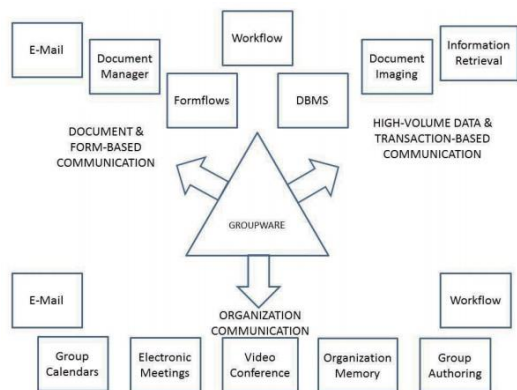


圖4：群組軟體應用的三個主要類別

5、推播技術(Push Technology)

推播技術(Push Technology)通常泛指透過伺服器端將訊息主動送到客戶端上的技術之一，其實是拉播技術(Pull Technology)的延伸，它改變了過去資訊是被動地讓使用者自己來取得這樣的模式，所採用的是主動性的做法，將資訊主動推給使用者。

拉播技術與推播技術兩者間的差異，前者主要是基於傳統「需求-回應」的框架下，它必須得是使用者們清楚知道何時何地要來找尋資訊，它才會從所要找尋的地方提供資料給使用者們；而至於後者，

它能允許使用者們在盡可能取得的情況下可以快速地取得資料，但對使用者們來講，他們並不需要任何有關於資訊從哪裡提供的知識[5]。

6、車牌辨識系統

車牌辨識系統之基本功能包括利用定點或是可移動之裝置，以擷取靜止或移動中車輛之車牌號碼，並針對車牌所包含之字元加以辨識，而且可以連結多功能之車牌資料庫進行各項的管理行為。一套完整的車牌辨識系統主要由兩大部分所組成，一是配合環境所搭配之硬體系統，另外則是有關字元辨識的軟體核心技術。擷取清晰的車牌是車牌辨識系統的重要關鍵，因此符合環境條件的硬體設備就變得十分講究。一般而言，一套車牌辨識系統硬體設備需具備以下功能[2]：

(a) 高解析度取像裝置：可擷取高畫質清晰的車牌影像。

(b) 輔助光源：依據環境光場的變化提供取像裝置足夠的光源。

(c) 無線網路的介面傳送影像，將使得車牌辨識系統無遠弗屆，並且使得交通或車輛管理所涵蓋的區域更加寬廣。

(d) 影像終端裝置：處理透過網路通訊介面所蒐集到的所有影像資訊，進行辨識、分析以及管理等各項必要的動作，並且可與資料庫建立聯結。

車牌辨識系統的核心是以字元辨識軟體為主。取得車牌的影像並完成字元切割之後，就可交給字元辨識軟體進行辨識的程序，除了數位影像的前處理技術之外，一般我們會針對其應用領域的不同，選擇辨識程式的核心技術，包括字元樣版比對、模糊類神經網路辨識技術以及字元特徵比較等方式，透過高效率的快速演算技術，將車牌辨識系統的準確率以及效率發揮到極致。

7、資料分析

資料分析是使用統計分析方法對收集來的資料進行分析，再加以處理及加工，以開發資料的功能、挖掘資料的價值，主要目的是為了找出有用的資訊並形成結

論。

資料分析程序可為以下步驟[10]：

- (a)採集：資料採集涉及到多個資料庫來源，NOSQL 經常用於資料管理及採集。
- (b)導入：為進行有效分析，對於前端所採集的資料導入分散式資料庫。
- (c)分析：資料分析技術包涵資料探勘、統計、人工智慧、數學分析、演算法…等。
- (d)呈現：分析結果視覺化或提出報告，以其論證或預測結果作為訂定策略之支援。

許多領域都需要資料分析技術，這項技術也廣泛應用於各種領域。例如工廠裡的異常偵測系統就使用資料分析技術，從工廠系統輸出機器的溫度變化與運轉次數後，根據這些資料預測是否會發生異常，這類技術也用於廣告效益預測或天氣預測。資料分析的技術可讓我們掌握趨勢，也能從中找出影響這些趨勢的原因，更可進一步預測未知的事物[8]。

8、警車攔截圍捕戰術

PIT(Precision Immobilization Technique)是美國執法部門開發的一種追車策略，使用警車的車頭側面去輕推逃逸車輛的車尾側面，造成逃逸車輛後輪打滑，進而使之失控而停止[9]。而在英國方面則是使用TPAC (Tactical Pursuit And Containment) 進行警車追逐，TPAC使用多輛警車包圍逃逸車輛以限制其速度，運用多數優勢將逃逸車輛框住，將其引導到不會影響他人的安全處再進行圍捕。

我國各警察機關尚無規範警車追逐使用的策略，本研究期望透過分析攔截圍捕影像並參考英、美等國家的警車追逐策略，以建立更有效率及安全性的攔截圍捕戰術。

五、警車攔截圍捕難處分析、解決方案及有無輔助系統協助攔截圍捕比較表

有鑑於警車攔截圍捕的各種難處，本研究將分析現行警車攔截圍捕所會遇到的各種問題並建立攔截圍捕輔助系統，以協助警方能夠快速並安全的逮捕逃逸目標，降低警車追逐的危險性。以下就警車攔截圍捕難處分析、解決方案及有無輔助系統協助攔截圍捕比較表分別敘述：

1、警車攔截圍捕難處分析

現行的警車攔截圍捕有著諸多難處，如追車員警必須不斷使用無線電回報目前位置、支援警力對路況不熟悉、勤務指揮中心難以掌握現場狀況等情形，導致許多警員寧願單一警車追逐也不願呼叫支援警力。然而，無論有無支援警力協助，現行的警車追逐方式始終無法有效的兼具效率及安全性。

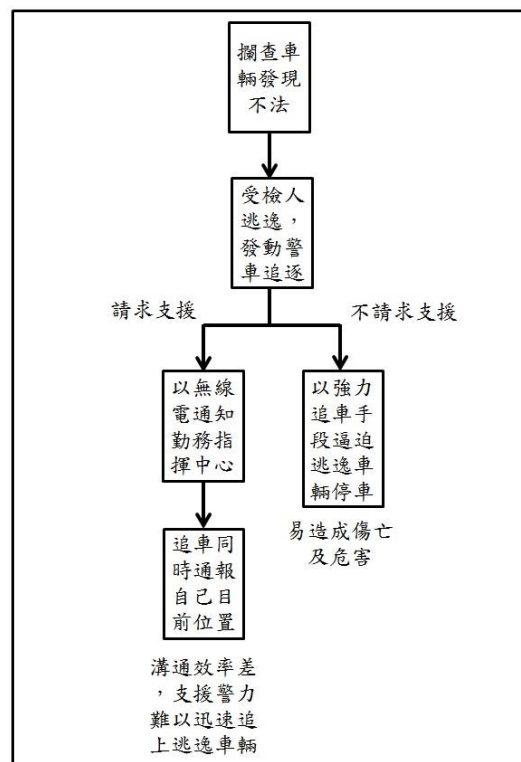


圖5：現行警車追逐流程

1.1、追車員警必須頻繁使用無線電通報

警察欲呼叫支援警力協助攔截圍捕時，會使用無線電通報自己目前所在位置。然而，警車追逐的過程會不斷的移動

位置，追車員警必須頻繁使用無線電通報自己目前所在位置，使追車員警無法專心跟車，甚至導致意外發生，而支援警力僅依據無線電所發出的訊息進行追捕，也難以精準鎖定目標位置，導致攔截圍捕行動效率低落，一旦圍捕時間拖長，便會提升警車追逐的危險性。

1.2、支援警力對路況不熟悉

由於支援警力可能來自各個不同的轄區，對於警車追逐所在位置不一定清楚，唯一的訊息來源只有追車員警使用無線電通報的位置訊息，造成支援警力難以快速跟上逃逸目標，甚至可能在找路的過程中發生意外。

1.3、勤務指揮中心僅有派遣支援的功能

當勤務指揮中心接收到警車追逐事件發生的通知時，便會派遣支援警力協助進行攔截圍捕。然而，勤務指揮中心僅能派遣支援警力，無法做出其它實質上的幫助。如能清楚掌握現場狀況，或許能夠提供不同的協助。

1.4、無線電頻道共用干擾訊息

警察使用的無線電可使同頻道的所有警力接收到訊息。然而，當警車追逐事件進行時，同頻道除了追車員警正在通報自己的位置外，可能還有其它與警車追逐事件無關的資訊如交通事故處理、民眾糾紛排解等訊息正在傳達，導致警車追逐的訊息被干擾，使支援警力必須花費更多心力才能正確鎖定逃逸車輛。

1.5、因情況緊急而未查證目標資料

警車追逐通常都是突然發生，追車員警並沒有時間去查詢逃逸駕駛及車輛的資料。然而，警車追逐的對象有可能是違反槍砲彈藥刀械管制條例、殺人罪通緝犯等的危險人物，若無準備可能在逮捕時發生意外。如能使用智慧型輔助系統自動查詢逃逸目標資料，使支援警力能夠有所準備，便可降低警方被危險人物攻擊的可能性。

1.6、沒有統一的攔截圍捕戰術

我國警察沒有如英、美等國家的執法單位有專門的攔截圍捕戰術，當警車追逐事件發生時，支援警力總是難以互相配合。如能分析各個警車追逐事件的影像畫面，研究出適合該地區警方的攔截圍捕戰術，並在常年訓練中教育員警以提升警車追逐的技巧及默契，便能夠提升警車攔截圍捕的效率及安全性。

2、解決方案 - 智慧型警車攔截圍捕輔助系統

本研究為解決警車攔截圍捕的各種難處，使用M-Police連結警車行車記錄器，建立一套結合定位導航、即時影像、群組對話、車牌辨識、資料分析等功能之智慧型警車攔截圍捕輔助系統，以5G傳輸警車追逐現場的即時影像及位置至攔截圍捕群組，加上車牌辨識及資料分析等功能，全面提升警車攔截圍捕的效率及安全性，相關系統架構如圖6。

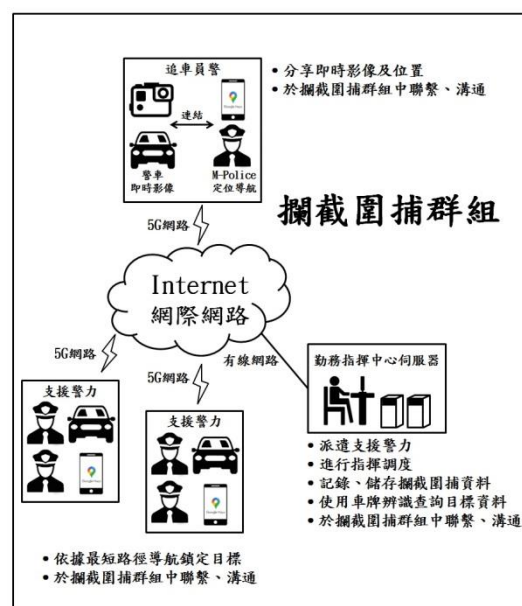


圖6：系統架構圖

2.1、即時影像及位置分享

將M-Police與警車行車記錄器使用Wi-Fi連結，如圖7，再把即時影像及定位畫面同步至攔截圍捕群組中，勤務指揮中心及支援警力便會接收到攔截圍捕正在進行的推播訊息，如圖8，點擊加入攔截

圍捕群組後將能查看追車員警的即時影像及位置，追車員警便無需不斷使用無線電通報自己目前所在位置，只要專心保持距離尾隨跟車，等待支援警力接近後再進行攔截圍捕即可。



圖7：M-Police連結警車行車記錄器畫面

員警的M-Police，持續不斷更新警車追逐的最新位置。導航地圖畫面讓支援警力了解自己目前與目標的相對位置，就算對路況不熟悉也能快速跟上逃逸車輛，並避免在轉角處發生與逃逸車輛或友軍發生碰撞的意外。



圖9：支援警力加入攔截圍捕群組所呈現的畫面



圖8：攔截圍捕之推播訊息

2.3、即時影像及位置呈現

勤務指揮中心能夠於攔截圍捕群組中查看警車追逐現場情況，加上即時地圖所呈現攔截圍捕群組各警力的位置，使勤務指揮中心人員除了派遣支援警力加入攔截圍捕外，還能夠觀察現場情況及地圖來進行指揮調度，提升警車攔截圍捕的效率。

2.2、使用最短路徑導航鎖定目標

支援警力加入攔截圍捕群組後，便能依據智慧型警車攔截圍捕輔助系統顯示之最短路徑導航行動，該導航目標為追車



圖10：勤務指揮中心加入攔截圍捕群組所呈現的畫面

2.4、攔截圍捕群組對話

攔截圍捕群組具有對話功能，追車員警及支援警力能夠使用M-Police直接進行群組對話，並可視情況使用外接式或藍牙耳機，而勤務指揮中心人員則是使用電腦連接耳機及麥克風，如此使用專屬於攔截圍捕群組成員的通訊群組進行溝通、聯繫，便能避免被其他不相關的訊息干擾之情形。

2.5、車牌辨識系統

當警車追逐事件發生時，車牌辨識系統能夠自動辨識追車員警所追蹤車輛的車牌號碼，並顯示於勤務指揮中心電腦畫面中，勤務指揮中心人員可點擊查詢該車的車籍資料，如果車主為違反槍砲彈藥刀械管制條例或是殺人罪通緝犯等危險人物，便能提前告知攔截圍捕成員注意自身安全，減少員警遭到攻擊的可能性。



圖11：車牌辨識查詢資料畫面

2.6、資料分析

當攔截圍捕行動結束後，智慧型警車攔截圍捕輔助系統將會自動記錄攔截圍捕的時間、地點、參與人員、成功與否等資料，並將其建檔儲存，而追車員警的行車記錄器影像也會自動存入資料庫中。上述資料將由系統分析產出各式報告，而報告中所呈現的資訊可用於攔截圍捕戰術研究、犯罪熱點地圖更新、績效評核參考依據等用途。

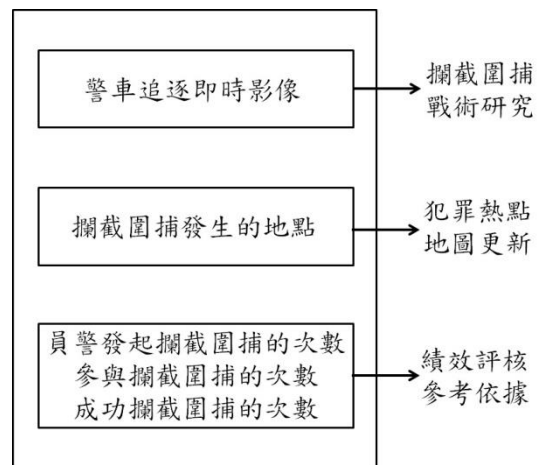


圖12：智慧型警車攔截圍捕輔助系統資料庫

3、有無輔助系統協助攔截圍捕比較表

本研究期望透過智慧型警車攔截圍捕輔助系統之定位導航、即時影像、群組對話、車牌辨識、資料分析等功能協助第一線員警以更有效率的方式進行攔截圍捕，改善現行攔截圍捕的諸多難處，降低警車追逐造成的傷亡。有無使用輔助系統協助攔截圍捕的差別如表1所示。

表1：有無輔助系統協助攔截圍捕比較表

	無輔助系統協助攔截圍捕	有輔助系統協助攔截圍捕
安全性	低	較高
效率	低	較高
成功率	低	較高
通訊品質	差(可能被無關訊息干擾)	優(具專屬通訊群組)
戰術選擇	少(勤務指揮中心能夠提供的幫助有限)	較多(勤務指揮中心可查看即時地圖及影像進行調度)

六、情境模擬

本研究針對智慧型警車攔截圍捕輔助系統的運用進行情境模擬，狀況如下：2021年2月11日12時30分許，高雄港務警察總隊六十三號碼頭中隊警員張三於高雄港66號碼頭管制站進行人車查驗，在查驗管制人車的過程中發現民眾李四車上藏有一級毒品古柯鹼(Cocaine)，李四見毒品被警方發現便立即駕車往豐漁三路逃逸，此時現場員警張三立刻拿出M-Police使用智慧型警車攔截圍捕輔助系統，將警車攔截圍捕事件發生的訊息推播給勤務指揮中心及支援警力，並將耳機接上M-Police後便騎乘警用機車ABC-123於逃逸車輛後保持安全距離持續尾隨跟車。

高雄港務警察總隊勤務指揮中心及支援警力接收到推播訊息後，便立即加入

攔截圍捕群組。勤務指揮中心人員透過車牌辨識系統發現車主有違反毒品危害防制條例、槍砲彈藥刀械管制條例等前科，如圖13，並於攔截圍捕群組中通知各成員注意自身安全。



圖13：查詢目標車輛及個人資料示意圖

支援警力藉由最短路徑導航快速接近逃逸車輛，當目標沿前鎮漁港逃逸至漁港南一路時，勤務指揮中心便調度支援警力在與漁港南一路交岔之興漁四路、興漁三路及興漁二路路口阻擋去路，迫使逃逸車輛駛入西岸碼頭，如圖14。當目標及攔截圍捕警力都進入西岸碼頭後，勤務指揮中心人員再聯絡保全人員將其入口柵欄門關閉，最後於西岸碼頭內成功逮捕違法民眾李四，如圖15。



圖14：攔阻逃逸路線示意圖



圖15：攔截圍捕成功示意圖

七、結論及後續研究

警車攔截圍捕具有許多不確定性因素，時常造成追逐員警、逃逸對象或是無關第三人的意外及傷亡。本研究期望透過智慧型警車攔截圍捕輔助系統改善現行警車攔截圍捕的問題，使追車員警無需不斷的通報自己的位置、支援警力可以依據定位導航最短路徑快速跟上目標，還有讓勤務指揮中心能夠掌握全局進行指揮調度，加上車牌辨識、資料分析等功能，全方面提升警車攔截圍捕的效率及安全性，達到安全圍捕人犯的成果。後續研究方面，如能將警車追逐時間、地點、路線、影像等資料的分析結果運用於攔截圍捕即時地圖中，預判逃逸車輛可能行駛的方向，使勤務指揮中心能夠事先調度支援警

力至指定地點攔阻去路，便能大幅度的縮短攔截圍捕所花費的時間，進而降低發生危害的機率，使警方更順利的完成攔截圍捕任務。

參考文獻

1. 李哲銘，「應用 Google 街景地圖的路線導覽系統——以長距離運動賽事為例」，國立雲林科技大學碩士論文，2015，第 11~12 頁。
2. 張正佳，「多視角車牌影像融合技術之評估」，國立交通大學碩士論文，2006，第 6~7 頁。
3. 張建明，「5G 超密集異質性網路下基於使用者服務品質滿足率提升之多層負載平衡機制」，國立中山大學碩士論文，2019，第 14 頁。
4. 莊智清、黃國興，電子導航，新北市：全華，2001。
5. 楊泓歷，「行動裝置之訊息推播雲端平台設計與實作」，義守大學碩士論文，2012，第 9 頁。
6. 鄧智允，「應用 GPS/INS 整合解決 GPS 定位脫鎖之研究」，明志科技大學碩士論文，2011，第 7 頁。
7. 賴俊佑，「整合心智圖與同步互動機制於網頁群組軟體之應用架構」，國立暨南國際大學碩士論文，2012，第 8 頁。
8. 寺田 学，辻 真吾，鈴木 たかのり，福島 真太郎，Python によるあたらしいデータ分析の教科書，2018.
9. David D. L. Mascareñas, Christopher J. Stull and Charles R. Farrar, Autonomous execution of the Precision Immobilization Technique, Mechanical Systems and Signal Processing, Volume 87, Part B, pp:153-168, 2017.
10. Nitin Sawant and Himanshu Shah, Big data Application Architecture Q&A-Problem-Solution Approach, pp:9-27, 2013.

11. P. K. Agyapong, M. Iwamura, D. Staehle, W. Kiess and A. Benjebbour, Design considerations for a 5G network architecture, IEEE Communications Magazine, vol. 52, no.11, pp:65-75, 2014.
12. Setrag Khoshafian and Marek Buckiewicz, Introduction to Groupware, Workflow, and Workgroup Computing, 1995.

人工智慧的發展對執法單位的影響與策略

The influence and strategy of the development of artificial intelligence on law enforcement agencies

鄭宇森

美國休士頓大學城中分校 刑事司法學系

1 Main St, Houston, TX 77002

jonson78962@gmail.com

Yu Sen, Cheng

Master of Science in Criminal Justice, University of Houston Downtown

1 Main St, Houston, TX 77002

jonson78962@gmail.com

摘要

科技的日新月異，使現行執法人員執勤方法改變，其中最吸引人但又令人懼怕的，就是人工智慧，現在人工智慧已開始用於機器人領域，以協助或替代各項工作，而執法人員，亦可以透過人工智慧與機器人更有效的打擊犯罪，但是，當我們在越多的領域使用人工智慧來協助我們執行任務並提供機器人更多的自主權時，可能會面臨法律與道德的問題。本文從介紹人工智能與機器人的特性開始，逐漸推衍至人工智能與刑事司法領域的交互影響，並提及人工智能在執法運用上的局限性、障礙與可能面臨的挑戰，並在最後提及未來執法機關面對人工智能與機器人的運用上，需要做出的規範與準備，以作為未來執法機關在司法實務上執行及運用人工智慧的參考。

關鍵詞: 人工智慧、科技執法、程序正義、法律規範、倫理道德

The influence and strategy of the development of artificial intelligence on law enforcement agencies

Yu Sen, Cheng

Master of Science in Criminal Justice, University of Houston Downtown

1 Main St, Houston, TX 77002

jonson78962@gmail.com

Abstract

The rapid development of science and technology has changed the existing methods of law enforcement officers. One of the most attractive is artificial intelligence. Artificial intelligence has begun to be used in robotics to assist or replace part of the work, and law enforcement officers, Artificial intelligence, and robots can also be used to combat crime more effectively. However, when we use artificial intelligence in more fields to assist us in performing tasks and provide robots with more autonomy, we may face legal and moral issues. This paper introduced artificial intelligence and robots' characteristics, gradually deducing the interactive influence of artificial intelligence and criminal justice. Second, the article further hints at the limitations, obstacles, and possible challenges of artificial intelligence in law enforcement applications. Finally, it proposes future law enforcement agencies in the face of applying artificial intelligence and robots. The standards that need to be made will serve as a reference for future law enforcement agencies to implement artificial intelligence in judicial practice.

Keywords: Artificial Intelligence, Science and Technology Enforcement, Procedural Justice, Legal Norms, Ethical and Morals.

1. Introduction

1.1 What is Robotics and Artificial Intelligence

People are always full of fantasies about robots. It is because of the blurring of robot definition and interpretation that it gives people the space to imagine and create. A robot is a machine that can perform work automatically. It doesn't have to be long like a person, but it must be a device that can operate on its own. It can accept human command, run pre-programmed procedures, or act on principles based on artificial intelligence. Its mission is to assist or replace the work of social work, such as production, construction, or dangerous work. Today's robots are already working in the industrial, commercial and service industries. The robot has moved from a single-function, goal-oriented machine to a multi-functional system. After decades of development, robots have been recognized for use in different tasks. (Savela, Turja, & Oksanen, 2018).

Artificial Intelligence (AI), a term that attracts people but teaches everyone to be afraid, draws us to be a smart robot that can think, help people with their work, and cook for our children. Artificial intelligence refers to the wisdom expressed by machines made by humans. The definition of artificial intelligence can be divided into two parts, namely "artificial" and "intelligent." "Artificial" is better understood and less controversial. Its definition is the things that humans created.

About what is "Intelligence" It involves other issues such as consciousnesses, self, mind and so on. We use our brain to create something automatic. However, humans have a minimal understanding of our intelligence, and we have a limited understanding of the necessary elements that constitute human intelligence, so it is difficult to define what is "intelligence" or "artificial."

Robots are tools for performing tasks, and Artificial intelligence is the brain that humans create for them. The overlap between robots and artificial intelligence is that we can apply

artificial intelligence to robots. That is, the robot is changed to a machine that can automatically perform motion without performing repeated work. This kind of used intelligent robot can perform relative and appropriate reactions and actions by sensing externally different environments and commands. (Savela, Turja, & Oksanen, 2018).

1.2 The Autonomy in Robotics and Artificial Intelligence

As robots become more complex, experts and scholars begin to pay attention to which ethics the robot's behavior needs to conform to, and which robot is eligible to have social, cultural, moral, or legal rights. Some scientific organizations claim that there may be robotic brains in 2019. Others predict that the robot's intelligence will have a breakthrough in 2050. Recent advances have made the behavior of robots more complicated.

Like all technology issues, automated robots bring about technological changes. The impact of smart robots on society cannot be ignored, and now police and law enforcement personnel are using robots to detect explosives or use robots for other criminal investigation purposes. In the future, we may provide more autonomy for robots because of advances in technology. However, we have to consider whether we can make these robots have autonomy. When robots can also be judges, human beings may face a day of trial by robots, because humans are always more likely to make mistakes than robots. Humans may think that they can avoid this legal and moral issue, but these problems may arise when we deliver autonomy to the robot. (Greeling, 2013).

1.3 What we have now in Robotics and Artificial Intelligence

We are now living in an era of artificial intelligence, and artificial intelligence has changed many of our way of life and has given us a lot of help. Now the phone can take pictures

with the AI function. The car can reach its destination by means of automatic navigation and automatic driving. Banks can control the funds in the form of AI and Robot. The doctor can use AI and Robot to find the medicine that is most suitable for the patient. The farmer can control the growth environment of the plant by AI and Robot to get the most fruits. The police can use the AI and Robot's assistance to know the crime hotspots or use the AI method to conduct face recognition to find the prisoner. The judges use the aid of the AI to consider the prisoner's sentence to make the final judgment. Robot and artificial intelligence are now in every corner of our lives. (Rigano, 2019)

2. Artificial Intelligence and Robotics policy in Criminal Justice

2.1 Human Interaction and consequence in Artificial Intelligence and Robotics

Nowadays, technology can connect the human brain with the robot arm, and use the electric wave provided by the human brain to command the robot arm, which is called the Brain-Computer Interface. The robot arm is built on the basis of the program, and it is based on our needs to cooperate with the instructions to perform the task. However, this technology is quite expensive. This technology can make people who are inconvenient or who have lost their arms to use the robot arm to eat. Perhaps this technology can be used in the future to allow law enforcement personnel to work with robots or robotic arms to make the law enforcement process safer.

2.2 Agency and law enforcement policies in Artificial Intelligence and Robotics

The rapid development of science and technology has made criminal techniques more oriented towards cross-type and cross-border expansion. In particular, the current crime characteristics are the most professional division of labor. Through the input of overseas information, it is difficult for police units to trace the source. These problems have brought significant threats and challenges to public

security. It is more feasible at this stage to use face recognition technology to conduct a criminal investigation. Face recognition means that the machine of AI will continuously learn from each other and analyze and understand each person's face. In the past, the police had to spend dozens of hours in front of the computer to find criminals through the monitor image. Now through artificial intelligence and face recognition, criminals can be located within a few minutes. At the same time with AI, we can also analyze the behavior of criminals before crimes and finding out the path of movement after the crimes. We can also use mathematical calculation formulas to introduce the location, time, land type, meteorological conditions, etc. Only through the use of innovative technology and emotional analysis and integration capabilities can we assist in the optimization of police duty performance. (Zachary, 2018).

On the other hand, the use of Artificial Reality (AR) policing has gradually matured. The AR is based on Artificial Intelligence's combination of virtual images and images seen by the human eye. The machine simulation allows the police to collect and display intelligence on the battlefield in real time. AR can improve the judgment of the police in dangerous situations. AR can increase the ability of police to collect clues and track. AR can provide a realistic training environment for police, and at the same time integrate real-life devices into the scene. The AR can be displayed in real time by monitoring police patrols and providing images of drone. With AR assistance, law enforcement officers can fight crime more effectively (Cowper, T., & Buerger, M. 2003).

2.3 How to create Public and Personal safety by Artificial Intelligence and Robotics

In recent years, the development and application of drones have been expanding. The police should develop towards the intelligent automatic take-off and charging direction of the drone, which can be applied patrol or large-scale rally, increase patrol range and frequency,

quickly deploy and construct 3D policing video and audio defense system.

It has become a common trend to use online customer service or chatbot to solve routine problems in various industries. Police can improve the quality of police services by using AI robot technology to answer common questions quickly, such as confirming whether providing a channel for immediate consultation of the public for fraudulent telephone calls. It not only can reduce the human burden of the policeman, but also improve the quality of service. On the other hand, police robots can also be used to add functions such as face recognition and license plate recognition to policing robots. In the initial stage, they can be applied to busy police stations and simple work. Besides, the police can use AI robot to transmitting images back to the police station. It can also confirm the identity of the people who need assistance. Therefore, law enforcements can use robots and AI to enhance public safety (Joh, 2017).

2.4 The problem in Criminal Justice which can be answered by Robotics and Artificial Intelligence

With a huge database, the introduction of AI will be the next step for the police to strengthen their combat power. Intersection surveillance images are the main tool for police handling at this stage. Therefore, we need to apply intelligent image analysis to provide intelligent monitoring such as video enrichment, license plate recognition, object detection, etc., and then combine artificial intelligence towards automatic processing and discrimination, to effectively save the human resources and the key to handling the case. On the other hand, the police should continue to strengthen the analysis of various types of situations and the use of tools, such as detecting cases of theft, clarifying which systems and associated tracking are used in the process of solving the case, identifying details that may be overlooked. In the future, the self-learning judgment of the machine can be used to further guide and assist the new investigators in the screening, collation, and

analysis of the sentiment, and enhance the effectiveness of the case through information technology.

3. Limitation in Artificial Intelligence and Robotics

3.1 Ethics and Law aspect in Artificial Intelligence and Robotics

The use of robots and AI will create many ethical and ethical issues because the robot is unpredictable. As we apply a large number of robots to various fields, we must ensure that the robots do not go wrong. On the other hand, whether the robot can replace the human decision is also a problem we need to discuss. Although human thinking is not as fast as robots, we usually consider more aspects. If the AI robot does not get enough information, it is likely to judge the error. On the other hand, whether we should give the robot the same status as the average human being in law is also a problem. If a robot sins because of a mistake, there is no way to deal with this result. Therefore, in the field of criminal justice, before using robots for law enforcement, we must consider whether we can solve the moral, ethical and legal problems of robots. (Pagallo, 2017).

3.2 What is our obstacle in Artificial Intelligence and Robotics

As technology becomes more developed, the development of artificial intelligence has begun to have some related problems. But because of these changes, artificial intelligence robot has done things beyond human resources, such as robotic arms, automated tools, etc., Human being will be afraid that their jobs will not be guaranteed.

Among these obstacles, I think the most important thing is the gap between unemployment and the rich and the poor. The rapid development of artificial intelligence has led to a gradual push for automation in many industries. Like manufacturing, it is about efficiency and standards. Robots are less likely to be fatigued than humans. They can work as a

standard for 24 hours, and customer service personnel and drivers are also easily replaced. The society is getting more and more self-driving. When it starts to spread, it can reduce the traffic accident rate. It can also calculate which route to take the least time. It will be the most significant advantage of self-driving, and it will also cause massive unemployment in the future. We should begin to think about how to combine the combination of industry and AI robot, and how to avoid people being eliminated in the future technology era. (Royakkers, & van Est, 2015)

3.3 Problems of Autonomous in Artificial Intelligence and Robotics

AI robots learn their prejudice based on the information instilled by the creators. They begin to have autonomy. It reflects how people perceive the world. Not only AI robot creators, but biases such as data can affect their judgment. The AI robot does not discern whether the received data is right or wrong. It is a problem that people are going to solve now.

To be more like human beings, the current AI robots will begin to instill emotions and humans will feel. If the robots really have feelings in the future, is it a human or a machine? On the other hand, it is a security issue. As mentioned in the previous article, when people instill the wrong ideas of AI robots, it will cause a lot of problems. Nowadays, drones and autonomous robots have already been used on the battlefield. More and more people are demanding international law to limit AI robotic weapons. It will become a sensational problem in the future. Therefore, we can know that the creators' infusion of misconceptions about robots may affect the safety of society. (McAllister, 2016)

4. Conclusion

4.1 Criminal Justice and AI Robotics Future Policy

In summary, what scares us is that this law enforcement robot will think for itself. What should he do if he is not obedient? Even worse,

when the boss found out that the law enforcement robot was better than the police, then the police would not be unemployed? Will AI robots make wrong judgments and infringe on the rights and interests of the people? These statements are concerned that machines may deprive law enforcement officials of their rights, but ignore the rewards we may receive, such as different types of better law enforcement tools, reducing labor, safer law enforcement environments, and a new learning and decision-making tools. These returns make law enforcement officers smarter and more sophisticated, making human society more stable. What we should do is to set the rules for the use of AI robots, so that AI robots can help law enforcement officers fight crimes to a limited extent. On the other hand, data collection is carried out for the use of AI robots in the field of Criminal Justice to correct the problem in the future. (Sharkey, Goodman & Ross, 2010).

4.2 What do we need to prepare for the future generation of AI and Robotics

The AI era has arrived, and the future will accelerate development. Whether we like it or not, these technologies will bring significant benefits and will inevitably reflect the weakness of our civilization. The government must indicate that they use AI robots to protect people. The government must ensure people's right to privacy, equality, and even the dangers that may arise in the future. The government must use sensible policies to deal with these dangers. They should let people feel relieved when the government use AI to assist the police in law enforcement. To achieve this goal, governments and law enforcement agencies need to build strong collaborative capabilities to manage the use of artificial intelligence. The results of this effort will determine whether humans will succeed in creating and using artificial intelligence technologies. If adequately managed, law enforcement officers will be able to get a lot of help from AI robots and gain the trust of the people.

From the era of artificial intelligence, we still need to continue to work hard even though we will encounter many difficulties. Each field will have different problems. As long as we can keep our enthusiasm for new ideas, we believe that robots and artificial intelligence will be able to have a significant contribution in the Criminal Justice area.

Reference

- [1] Cowper, T., & Buerger, M. (2003). Improving our view of the world: Police and augmented reality technology. *FBI Law Enforcement Bulletin*, 77(5). Robots and Cops: Connect the Dots.
- [2] Christopher Rigano, "Using Artificial Intelligence to Address Criminal Justice Needs," *NIJ Journal* 280, January 2019,
- [3] Greeling, K. Y. (2013). Autonomous robots in law enforcement: future legal and ethical issues. Carbondale: Southern Illinois University.
- [4] Joh, E. E. (2017). Artificial Intelligence and Policing: First Questions. *Seattle UL Rev.*, 41, 1139.
- [5] McAllister, A. (2016). Stranger than Science Fiction: The Rise of AI Interrogation in the Dawn of Autonomous Robots and the Need for an Additional Protocol to the UN Convention Against Torture. *Minn. L. Rev.*, 101, 2527.
- [6] Pagallo, U. (2017). When morals ain't enough: Robots, ethics, and the rules of the law. *Minds and Machines*, 27(4), 625-638.
- [7] Royakkers, L., & van Est, R. (2015). A literature review on new robotics: automation from love to war. *International journal of social robotics*, 7(5), 549-570.
- [8] Savela, N., Turja, T., & Oksanen, A. (2018). Social acceptance of robots in different occupational fields: A systematic literature review. *International Journal of Social Robotics*, 10(4), 493-502.
- [9] Sharkey, N., Goodman, M., & Ross, N. (2010). The coming robot crime wave. *Computer*, 43(8), 115-116.
- [10] Kaplan, Z. A. (2018). R2D2 OR IROBOT: CAN ARMED ROBOTS BE A FRIEND TO POLICE WITHOUT BEING A FOE TO THE PUBLIC?. *Notre Dame Journal of Law, Ethics & Public Policy*, 32(2).

國家圖書館出版品預行編目（CIP）資料

2021 年第 24 屆資訊管理學術暨警政資訊實務研討會：「運用智慧科技創新警政服務」論文集 / 廖有祿編輯 -- 初版. -- 桃園市：中央警察大學資管系, 2021.05

面；公分

ISBN 978-986-98280-7-9 (平裝) NT\$: 150

1.警政 2.警政資訊系統 3.文集

575.807

110009023

2021 年第 24 屆資訊管理學術暨警政資訊實務研討會-「運用智慧科技創新警政服務」論文集

發行者：陳擇文

編輯者：廖有祿

出版者：中央警察大學資訊管理學系

作者：王逸嵐、董正談、鄧少華等著

地址：33304 桃園市龜山區大崗里樹人路 56 號

電話：(03)328-5189

印刷者：尚曄文化事業有限公司

地址：22066 新北市板橋區板新路 103 號 4 樓之 1

電話：(02)2958-6010

定價：新台幣一百五十元

二〇二一年五月初版

版權所有，翻印必究