特稿

應用犯罪偵查知識工程化於刑案偵查實務之探討
——以F銀行ATM跨國盜領案為例

林宜隆*、吳昆霖**

要　目

DOI：10.6460/CPCP.202208_(32).04

* 大同大學資訊工程學系暨研究所教授、台灣數位鑑識發展協會（ACFD）創會理事長，中央警察大學退休教授。

** 宜蘭縣警察局刑警大隊偵查佐，國立宜蘭大學資訊工程研究所碩士。

摘　要

臺灣刑案犯罪偵查，係以刑事訴訟法之檢察官為犯罪偵查主體，司法警察（官）僅定位為偵查輔助機關，然而，資通訊科技（ICT）進步所帶來現今之犯罪手法多變且日新月異，偵查人員無時無刻接受著最新的挑戰及思維（即所謂：犯罪科技化與科技犯罪化）；因此，導入「犯罪偵查知識工程化」（ICNIV modelling）方式，提升犯罪偵查技能與效能、法律素養及人權等觀念，實有其必要性與急迫性。

2016年7月11日，臺灣金融史上首件ATM盜領案，F銀行20家分行、51台ATM，在7月9日至11日期間，遭多名外籍人士盜領新臺幣83,277,600萬元；警方於案發後第7天宣布破案，分別在宜蘭縣及臺北市共逮捕3名犯嫌，並掌握來臺外籍嫌犯共有19人，其中16人已潛逃出境（已發布通緝），迄今本案已追回贓款新臺幣77,481,100萬餘元，前警政署長陳國恩說：「國際犯罪集團在臺灣踢到鐵板。」

回歸檢視本案偵辦過程，從F銀行報案、逮捕主嫌、追溯共犯及取贓等偵辦過程，運用「犯罪偵查知識工程化」之方式，逐一檢視及檢討案件偵查手法、技巧及程序之優劣，作為日後刑事人員偵處案件之依據。因此本文試以，建立「合理化」、「科學化」、「系統化」、「知識化」之犯罪偵查基本原則（ICNIV modelling）。

因此本文以「F銀行ATM跨國盜領案」為案例，自案發後，F銀行通報警方起，至查獲主嫌、共犯及起出贓款，再

導入國內學者林宜隆教授所提出「犯罪偵查知識工程化」之方法與架構，剖析多元化且先進之新興犯罪型態與手法。

關鍵詞：犯罪偵查、知識工程化、犯罪偵查技術及推理法則、駭客、ATM跨國盜領

A Study on Application of Knowledge Engineering to Criminal Investigation – ATM Hacking Theft Steal Case from F Bank as Example

I-Long Lin* & Kun-Lin Wu**

Abstract

The criminal investigation of Taiwan's criminal case is based on the prosecutors of the Criminal Procedure Law as the main body of criminal investigation, and the judicial police (officials) are only positioned as auxiliary investigation agencies. However, the current criminal methods brought about by the advancement of information and communication technology (ICT) are changeable and changeable. With the rapid changes, investigators are always accepting the latest challenges and thinking (the so-called: criminal technology and technology criminalization); therefore, the "ICNIV modelling" approach is

* Professor, Department of Computer Science and Engineering, Tatung University (TTU); Founder, Association of Cyber Forensics Development in Taiwan (ACFD); Retired Professor of Central Police University (CPU).

** Investigation Assistant, Criminal Police Brigade, Yilan County Police Station; Master of Computer Science and Engineering, National Ilan University.

introduced to improve criminal investigation skills, effectiveness, and legal literacy and the concepts of human rights, etc., have their necessity and urgency.

On July 11, 2016, the first ATM theft in Taiwan's financial history, F Bank's 20 branches and 51 ATMs were stolen by many foreigners from July 9th to 11th. NT$832.776 million was stolen. On the 7th day after the incident, the police announced that they had solved the case. They arrested 3 suspects in Yilan County and Taipei City respectively, and knew that there were 19 foreign suspects who came to Taiwan, 16 of whom have absconded and left the country (wanted). So far this case More than NT$77,481,100 in stolen money has been recovered. Former Commissioner of Police Chen Guoen said: "International criminal syndicates have kicked the iron plate in Taiwan."

Return to review the investigation process of this case, from the investigation process of F Bank reporting, arresting the main suspect, tracing accomplices, and taking stolen goods, using the method of "ICNIV modelling' to review and review the investigation methods, techniques and procedures of the case one by one the pros and cons will be used as the basis for criminal investigation and handling of cases in the future. Therefore, this article tries to establish the basic principles of criminal investigation (ICNIV modelling) of "rationalization", "scientization", "systematization" and "intellectualization".

Therefore, this article uses the "Transnational theft of ATMs in Bank F" as a case. After the incident, Bank F notified the

police, until the main suspect, accomplices, and stolen money were found, and then introduced the "Crime Investigation Knowledge Project" proposed by the domestic scholar Professor Lin I-long. The method and framework of ICNIV modelling analyzes diversified and advanced emerging crime patterns and methods.

Keywords: Crime Investigation, Knowledge Engineering, ICNIV modelling, Hacker, ATM Transnational Theft

壹、前　言

所謂「知識工程化」，意旨將集成化的思維，去組織欲分析之目標個案，讓刑案偵查呈現一體之綜合且具體之面貌；犯罪偵查含括發生刑事案件後，警察受理民眾報案，啟動偵查作為之案發現場及書面資料的證據保全，追緝犯嫌及執行拘提或搜索，最後到案件移送等，需具備各方面的專業知識及偵查技巧，刑事犯罪偵查工作始能發揮最大之效益（林宜隆，1998）。

我國刑案偵查，係以刑事訴訟法之檢察官為犯罪偵查主體，司法警察（官）僅定位為偵查輔助機關，然而，科技進步所帶來現今之犯罪手法多變且日新月異，偵查人員無時無刻接受著最新的挑戰及思維；故導入「犯罪偵查知識工程化」，提升偵查技能、法律素養及人權等觀念，實有其必要（林宜隆，2009）。

近10年來，內政部警政署致力建構一系列查察刑案之知識平臺，讓戶役政、刑案素行紀錄、查捕逃犯、失蹤人口、查贓、在監在所、親等關聯式架構表，但對於刑案破獲後之資料庫，僅止於移送書、起訴書及判決書等靜態資料，尚未建立「合理化」、「科學化」、「系統化」、「規則化」之資料庫查詢方式（林宜隆，2009）。

因此本文以「F銀行ATM盜領案」為案例，自案發後F銀行通報警方起，至查獲主嫌、共犯及起出贓款，再導入國內學者林宜隆教授所提「犯罪偵查知識工程化」（ICNIV modelling）之架構，剖析多元化且先進之犯罪型

態與方法（林宜隆，2011；林宜隆，2016）。

貳、犯罪偵查知識工程化之探究

犯罪偵查係在發掘犯罪行為在心理上、物理上、社會上殘存的表徵，並依據一定的犯罪痕跡所能顯現的片段表徵來推理犯罪事實和犯罪人，進而收集證據等基本的技術及推理法則，以應付變化多端的犯罪型態。犯罪偵查走向合理化（不被合理懷疑）、科學化（刑事鑑識）、系統化（組織現場蒐證系統化）及規則化（知識化犯罪事實）等目標及願景，具備程序性之原理、原則，作為偵查實務工作之參考，避免故事性或英雄化渲染，讓犯罪偵查工作日益精進，並提升犯罪偵查知識工程化正確性，其詳細步驟如下（林宜隆，1998；林宜隆，2009）：

一、犯罪偵查與實務工作

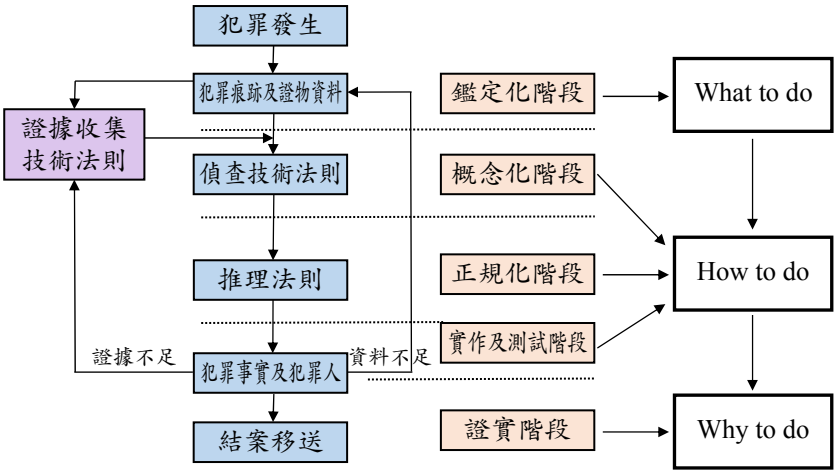
依目前我國刑事訴訟法規定，偵查主體為檢察官，檢察官有指揮警察偵查犯罪之職權。然而，就實務工作經驗而言，案件能否破案之關鍵卻在於承辦警察之專業能力，不論是犯罪現場保全、蒐證、鑑識、查訪、拘提、逮捕、搜索、扣押、通訊監察等工作都需仰賴F線從事偵查工作之員警，因此建立警察應有的犯罪偵查專業素養、能力及法學素養，應是作為犯罪偵查工作的前提及目標（林宜隆、吳昆霖、施凱鐫，2016）。

二、犯罪偵查知識工程化五大階段

國內學者林宜隆教授提出犯罪偵查知識工程化方法係為：欲使犯罪偵查走向合理化、科學化、系統化及規則化（知識化犯罪事實）等專業職能，應具備下列五項基本原則（如圖1）（林宜隆，2009；林宜隆，2017）：

圖1

犯罪偵查技術及推理法則運用（ICNIV modelling）之流程圖



(一)鑑定化階段（Identification, I）：蒐集所有現場犯罪痕跡及證物資料，找出問題

犯罪偵查工作乃是一種解決問題的過程，首先要明確瞭解問題所在，才能確定偵查手段和方法。進而蒐集所有關鍵資料，以便供應判斷推理案情的證據與參考。

如本案民眾發現F銀行ATM吐鈔異常後報案、F銀行

通報特定ATM遭盜領、領鈔車手身分、共犯及交通工具。

(二)概念化階段（Conceptualization, C）：從事鑑識、檢討，以發現新的價值或認定問題

將所蒐集之資料加以鑑識或檢討，往往又可以發現資料價值，進而使其個化，如調閱監視器可發現車手樣貌，反求交通工具可得知住處及身分、將異常吐鈔ATM進行數位鑑識可追溯駭客來源及入侵點。

如本案案發地相關監視器調閱小組、同一型號遭駭ATM數位鑑識、如何同步鎖定同一型號ATM地點並自動吐鈔及聯絡領鈔車手取款、車手取款後之作為。

(三)正規化階段（Normalization, N）：多方假設，進而演繹歸納案情

以現場狀況和搜索所得痕跡、證物等資料為基礎，運用智慧、經驗予以推測種種可能性，多方假設並加以演繹歸納案情。

如本案模擬嫌犯各別入境時間、聯絡方式、如何分工、如何同步聽從指揮並至指定ATM進行取款犯案、犯案後逃逸、集合、交付贓款及路線。

(四)實作及測試階段（Implementation, I）：依假設之答案分別反覆求證

查證首先應擬定偵查方針，再按照計畫進行實施。

1.決定偵查事項：針對推測的事項，逐點查明。

2.決定偵查方法：偵查事項確定後應視其性質、型態

而決定偵查方法。

3.偵查結果：所推測的事項得到佐證，推測之事項可以得到正確認定；反之，則推測屬可疑。查證工作應盡所有方式及方法，再三反覆求證。

如本案模擬歹徒行進路線，並調閱監視器加以證實交通工具、居住地點及逃逸路線後，最後於宜蘭縣警方查獲；另模擬駭客攻擊F銀行主機及分行ATM，經數位鑑識後，證實係由F銀行倫敦分行入侵。

(五)實證階段（Validation, V）：偵查結果所得推斷用以證明犯罪事實

由偵查結果所得推斷（心證或主張）必須依下列方法，使其具備客觀性：

1.應以一定形式表達推斷（主張）。

2.應提示其推斷是真實的理由或證據。

3.表達推斷（主張）的形式通常是文字。以文字表達某些推斷為之命題。

如本案依ATM監視器可得知，車手未操作ATM，但機器自動吐鈔，確定本案係駭客以遠端操作方式犯案；破案後得知外籍犯嫌係以俄羅斯文並用通訊軟體與遠端駭客聯繫，並與數位鑑識結果相互佐證，本案駭客係由F銀行倫敦分行入侵等情形。

因此，欲證明犯罪事實是真實，必須使推斷表達命題外，並提示足以主張其推斷是真實的理由或證據。犯罪偵查的過程中，必須循一定的法則，按部就班、循序漸進，

以現場危機處裡及蒐集情報之處，運用科學方法及技術，進行清查核對或化驗鑑定，汰蕪存菁，然後深入分析研究，以利案情研判，期能發掘偵查線索，確定偵查方向，擬定偵查計畫，進而部署分工，採取適當偵查行動俾迅速發現犯罪真相，藉以證明犯罪事實及人犯身份，如表1所示（林宜隆，2017）。

表1

犯罪偵查知識工程化五大階段

犯罪偵查知識工程化五大階段方法			
五大階段	步驟內容	定義	以F銀盜領案導入犯罪偵查知識工程化
鑑定化階段(I)	蒐集所有現場犯罪痕跡及證物資料，找出問題。	1.犯罪偵查工作乃是一種解決問題的過程，首先要明確瞭解問題所在，才能確定偵查手段和方法。 2.進而蒐集所有關鍵資料，以便供應判斷推理案情的證據與參考。	如本案民眾發現F銀行ATM吐鈔異常後報案、F銀行通報特定ATM遭盜領、領鈔車手身分、共犯及交通工具。
概念化階段(C)	從事鑑識、檢討，以發現新的價值或認定問題。	1.將所蒐集之資料加以鑑識或檢討，往往又可以發現資料價值。 2.進而使其個化，如調閱監視器可發現車手樣貌，反求交通工具可得知住處及身分。 3.將異常吐鈔ATM進行數位鑑識可追溯駭客來源及入侵點。	如本案案發地相關監視器調閱小組、同一型號遭駭ATM數位鑑識、如何同步鎖定同一型號ATM地點並自動吐鈔及聯絡領鈔車手取款、車手取款後之作為。
正規化階段(N)	多方假設，進而演繹歸納案情。	1.以現場狀況和搜索所得痕跡、證物等資料為基礎。 2.運用智慧、經驗予以推測種種可能性，多方假	如本案模擬嫌犯各別入境時間、聯絡方式、如何分工、如何同步聽從指揮並至指定ATM進行

表1（續）

犯罪偵查知識工程化五大階段方法				
五大階段	步驟內容	定義		以F銀盜領案導入犯罪偵查知識工程化
		設並加以演繹歸納案情。		取款犯案、犯案後逃逸、集合、交付贓款及路線。
實作及測試階段(I)	依假設之答案分別反覆求證。	查證首先應擬定偵查方針，再按照計畫進行實施。	1.決定偵查事項：針對推測的事項，逐點查明。 2.決定偵查方法：偵查事項確定後應視其性質、型態而決定偵查方法。 3.所推測的事項得到佐證，推測之事項可以得到正確認定；反之，則推測屬可疑。 4.查證工作應盡所有方式及方法，再三反覆求證。	如本案模擬歹徒行進路線，並調閱監視器加以證實交通工具、居住地點及逃逸路線後，最後於宜蘭縣警方查獲；另模擬駭客攻擊F銀行主機及分行ATM，經數位鑑識後，證實係由F銀行倫敦分行入侵。
證實階段(V)	偵查結果所得推斷用以證明犯罪事實。	由偵查結果所得推斷（心證或主張）必須依下列方法，使備其客觀性。	1.應以一定形式表達推斷（主張）。 2.應提示其推斷是真實的理由或證據。 3.表達推斷（主張）的形式通常是文字。以文字表達某些推斷為之命題。	如本案依ATM監視器可得知，車手未操作ATM，但機器自動吐鈔，確定本案係駭客以遠端操作方式犯案；破案後得知外籍犯嫌係以俄羅斯文並用通訊軟體與遠端駭客聯繫，並與數位鑑識結果相互佐證，本案駭客係由F銀行倫敦分行入侵等情。

註：本研究整理。

參、案情說明與案例分析

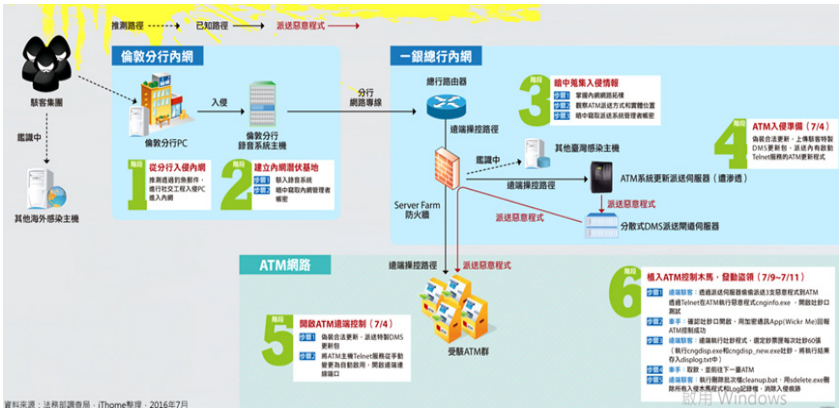
本文即以「F銀行ATM盜領案」為案例，分析臺北市政府警察局、法務部調查局新北市調查處及臺灣臺北地方法院檢察署所發布之新聞稿及偵查終結新聞稿，並參考各新聞媒體報導，分析F銀行ATM盜領案之犯罪事實及犯罪手法，導入「犯罪偵查知識工程化」方法之分析，以解決變化多端的犯罪型態，其詳細說明如下：

一、案情說明

本文根據臺北市政府警察局及法務部調查局新北市調查處發布之發生及偵辦過程新聞稿，及最後由臺灣臺北地方法院檢察署發布之偵查終結新聞稿，歸納出本案可能犯罪事實共6點，分別說明如下（如圖2）（iThome，2016）。

圖2

F銀行ATM跨國盜領案歸納出本案可能6項犯罪事實



註：本研究整理及參考法務部調查局和iThome整理。

(一)犯罪事實1：駭客製作惡意程式，選定ATM機型，尋找侵入F銀行之漏洞及跳板

集團內之不詳成員，先於2016年7月5日前（2016年7月5日係集團內之成員最早來臺之日期），製作專供取得「ProCash 1500」型ATM內現鈔資訊之電腦程式「cnginfo.eFe」、專供命令該型提款機執行吐鈔動作且限定僅能於2016年7月間執行之電腦程式「cngdisp.eFe」與「cngdisp_new.eFe」、專供犯案後呼叫「sdelete.eFe」之電腦程式，功能係針對欲刪除之檔案進行磁區抹除，使得刪除後之檔案難以透過專業軟體進行復原，以徹底刪除「cnginfo.eFe」與「cngdisp.eFe」進行滅證之電腦批次檔「cleanup.bat」等專供犯妨害電腦使用罪章之惡意電腦程式後，並於2016年5月31日晚上22時36分許，侵入F銀行倫敦分行電話錄音主機電腦系統之漏洞，便利作為日後侵入其他F銀行電腦之跳板（iThome，2016；臺灣臺北地方法院檢察署新聞稿，2016）。

(二)犯罪事實2：選定跳板及侵入點，並竄改特定ATM機型監控程式，連續將目的係在各ATM電腦上執行盜領前準備工作之電腦指令

謀議既定後，陸續於2016年6月28日起至7月4日間，利用F銀行倫敦分行電話錄音主機作為跳板，侵入F銀行內部網路中負責「ProCash 1500」型ATM電腦程式更新派送暨監控之應用程式伺服器，連續將目的係在各ATM電腦上執行盜領前準備工作之電腦指令，例如刺探ATM電腦軟硬體資訊、在ATM電腦上建立具有管理者權限之帳號

「support_487566a0」等準備工作之電腦指令，包裝為附檔名為dms之封裝檔，先後共33個，以操作AP伺服器上之派送程式，將前揭封裝檔派送至該集團為犯案選定位於臺北市、新北市、臺中市，共計41部之「ProCas h1500」型ATM之電腦上執行，而變更該等ATM電腦上之使用者帳號紀錄，並蒐集取得該等ATM電腦之資訊，作為進行盜領前之準備（蘋果日報，2016a；蘋果日報，2016b）。

(三)犯罪事實3：測試惡意程式執行狀況，並指派外籍犯嫌至選定地點觀察遭駭ATM吐鈔口執行情形

安排妥適後即於2016年7月5日前某日時，再利用F銀行倫敦分行電話錄音主機作為跳板，侵入F銀行內部網路中負責針對F銀行所使用另一系列由NCR公司生產之，ATM，進行ATM電腦程式更新派送之NCR伺服器，將上開惡意程式「cnginfo.eFe」、「cngdisp.eFe」、「cngdisp_new.eFe」、「cleanup.bat」存放在該伺服器內，以便後開始進行盜領時，供上述41部F銀行ATM得以連線至NCR伺服器後以ftp方式加以下載。另為驗證前述入侵與布署惡意程式機制是否可行，並於2016年6月30日凌晨2時11分，選擇位於臺北市萬華區F銀行西門分行ATM進行測試，透過NCR伺服器傳送「86.eFe」程式至該西門分行ATM之電腦，再於同日凌晨3時52分許，經AP伺服器將作用為建立上開管理者帳號並呼叫「86.eFe」程式以提高該帳號telnet權限之電腦指令封裝檔，派送至該西門分行ATM之電腦，以建立具有telnet連線能力之帳號後，復於

同日晚上9時18分5秒至31秒期間，一方面委請真實姓名年籍不詳男子，至該西門分行ATM前觀察，另方面由集團內成員自F分行倫敦分行電話錄音主機以telnet方式連線至該西門分行ATM之電腦，執行諸如「cnginfo.eFe」之程式以測試該ATM吐鈔口開闔情形，並由該不詳之人觀察後以手機回報，因而確認前述入侵與布署惡意程式之機制確實可行。

(四)犯罪事實4：16名車手分批抵臺，並執行惡意程式及干擾總行稽核連線後，開始進行盜領

嗣入侵F銀行內部網路及惡意電腦程式之製作與布署等前期作業完成後，即自2016年7月8日起負責之車手暨車手頭共15人先後分組、分批入境，並自同年月10日凌晨0時許起開始分組犯案，均利用手機通訊軟體通知該集團不詳之成員，由該成員利用F銀行倫敦分行電話錄音主機作為跳板，以Telnet（遠端登錄服務）之方式與該ATM電腦建立連線，並輸入事先已建立在該ATM電腦上之管理者帳號「support_487566a0」暨密碼後，侵入上述41部ATM之電腦，再由該ATM之電腦上以FTP（檔案傳輸服務）之方式，自NCR伺服器下載取得上開盜領用惡意電腦程式「cnginfo.eFe」、「cngdisp.eFe」與「cngdisp_new.eFe」、「cleanup.bat」，隨即執行「cnginfo.eFe」確認ATM之吐鈔模組狀態，再執行「cngdisp.eFe」或「cngdisp_new.eFe」，以干擾ATM電腦及ATM內之吐鈔模組，使該ATM在未經ATM電腦與F銀行帳務系統連線稽

核之狀況下，直接由ATM之吐鈔模組吐出上開惡意程式所指定數額之現鈔，並由守候在各該ATM前之車手或車手頭取款，而以此等不正方式，自各該具有自動付款功能之ATM內盜取款項，共計達新臺幣（下同）8,327萬7,600元，足生損害於F銀行。

(五)犯罪事實5：盜領既遂後，駭客經跳板及侵入點刪除惡意程式及登入紀錄檔案

得手後，上開集團內成員，為將侵入F銀行內部網路布署上開電腦程式之跡證湮滅，復於2016年7月12日，利用F銀行倫敦分行電話錄音主機作為跳板，再次侵入F銀行內部網路中之AP伺服器，將目的在於執行上開「cleanup.bat」程式，以便將犯案用惡意程式「cnginfo.eFe」、「cngdisp.eFe」與「cngdisp_new.eFe」進行徹底刪除之電腦指令，包裝為檔名為「60712001.dms」之封裝檔，再以AP伺服器上之派送程式將該封裝檔派送至遭盜領ATM之電腦上執行，以徹底刪除做案用之惡意程式及該等程式產生所產生諸如「displog.tFt」之電磁紀錄。另又針對作為跳板F銀行倫敦分行電話錄音主機，將硬碟內電磁紀錄刪除，使該電腦無法連線登入查看其狀態，足生損害於F銀行。

(六)犯罪事實6：另7位外籍車手成員抵臺，負責接應、通訊及贓款之後續置

繼之集團成員為處理贓款後續搬運、寄藏暨掩護同案共犯等事宜，上開犯罪集團復自2016年7月9日起安排陸夫

斯基等7位成員來臺接應。而上開集團內之各組車手暨車手頭完成ATM之取款後，第1組車手之贓款，連同該組車手柏克曼於2016年7月11日凌晨4時38分許，至第5組車手投宿之旅社內收取之第5組車手之贓款，將款項放置於所投宿之留在君悅飯店房內，等候同集團後續來臺成員入住該房間後進行後續處理；第3組、第4組車手之贓款係由車手頭巴比收取後，於2016年7月12日下午5時58分許，將款項裝入黑色大型行李箱、藍色小型行李箱各1只內，分別暫置在臺北車站地下1樓東出口前置物櫃；第2組、第6組車手之贓款則係由洛夫斯基收取後，與莎琪蘇娃共同處理，並於同年月11日下午5時55分許，裝在白色大型行李箱1只內，暫置於投宿之寒舍艾美酒店房內，復由車手頭巴比與保羅於同年月13日下午5時54分許，在寒舍艾美酒店會面後，由巴比至艾美酒店房內取走該只白色大型行李箱，並於同日下午6時47分許，存放在臺北火車站地下1樓東出口前置物櫃。安德魯則經上開集團之指示來臺，於同年月11日下午6時52分許，至臺北市君悅酒店，以訪客身分向櫃檯取得房卡後，取得第1組車手甫於同日上午離開時（未辦理退房，並事先已告知櫃檯將有另1名俄籍友人來訪，請櫃檯配合給予房卡），暫置該房間內之行李箱內之贓款，準備進行贓款之後續處理；惟斯時因F銀行ATM遭盜領之新聞已見諸媒體報導，安德魯經集團成員之指示，於同年月12日自君悅酒店退房，隨後攜帶贓款入住臺北市中山區民生東路之套房，並於同年月13日凌晨5時3分

許，將贓款裝放於1只黑色行李袋、1只電腦手提包後，藏放在臺北市內湖區內湖路登山口上方約50公尺處旁草叢內後返回上開套房，又於同日上午9時2分許再度回到上址藏放處，以便將該地點之GPS座標，透過手機通訊軟體回傳集團成員，並依指示前往宜蘭縣躲避，上開集團則另指派雷納斯，於同年月16日午間將新購得之三星牌A5型手機空機1支，藏放在宜蘭縣頭城鎮烏石港之消波塊中，指示安德魯前去取用，準備伺機再進行贓款之後續處理。而米海爾則經由巴比之指示偕同潘可夫來臺，於同年月16日下午4時50分許，自臺北車站地下1樓東出口前置物櫃，取得裝有贓款之上開3只行李箱，準備進行贓款之後續處理（臺灣臺北地方法院檢察署新聞稿，2016）。

二、本案案例分析

2016年7月8日、9日，經反向追查及調閱監視器畫面，得知歹徒搭乘國泰航空到臺灣，並在臺租車，於7月9日在臺北市萬華區、中正區及新北市汐止區等地區之F銀行ATM進行盜領動作。

2016年7月10日晚間8點，有民眾在F銀北市古亭分行提款，發現兩名男子戴口罩，鬼鬼祟祟的在提款機前操作，民眾以為是詐騙集團，當下報警，不過兩名歹徒在警方到達現場前已經離開，而吐鈔口還留下6萬元現金；古亭分行經理接獲通知後，立刻清查提款機的電腦系統行，並未顯示插卡獲不當方式提領紀錄，總計損失6百多萬，並即刻通知總行，結果到了11日下午，F銀古亭分行陸續

發現其他分行異狀，而且都為特定機型，而且也都沒有紀錄，全臺20家F銀分行，共41台提款機共被盜領約8,000多萬元，後來調監視器發現，兩名歹徒在完全無操作ATM的情形下，直接讓ATM吐鈔後大量提領，並立即將現金裝入背包離開，作案過程約5~10分鐘就在每台ATM輕鬆盜領數百萬元（如圖3）（蘋果日報，2016a；蘋果日報，2016b）。

圖3

F銀行歹徒盜領時序表

7月8日：2名俄羅斯籍車手搭機抵臺。

7月9日：車手從凌晨起陸續至臺中、臺北與新北的F銀行ATM盜領。

7月10日：車手兵分兩路，再到臺中、臺北與新北的F銀行ATM盜領。

7月11日：凌晨車手分別至臺北與新北的F銀行ATM盜領後出境，F銀行報案。

7月12日：警方清查總計遭盜領新臺幣8千多萬元，並鎖定安德魯等3名外籍犯嫌並通報境管。

7月13日：檢警約談ATM工程師與F銀行資訊主管。

7月14日：警方清查後確認，拉脫維亞籍嫌犯安德魯在臺灣境內，並擴大追查。

7月15日：涉及F銀行盜領案的外籍犯嫌至少11人，且多在11日出境。

7月16日：刑事局鎖定15名犯嫌，並公布涉及盜領案10名犯嫌照片，認定盜領案結束才入境的安德魯是善後組，負責將贓款匯出臺灣，並查出有一外籍犯嫌潛逃至宜蘭縣外澳鄉。

7月17日：犯嫌安德魯在宜蘭縣東澳鄉某餐廳用餐遭警方發現，並通報專案小組後循線逮捕歸案，並擴大查獲於北市藏匿之另2名外籍犯嫌。

註：本研究參照新聞內容製作。

綜上所述，其犯罪偵查知識工程化（ICNIV modelling）步驟如圖4所示，其詳細說明如下（林宜隆，2017）：

圖4

運用犯罪偵查知識工程化於刑案偵查實務流程

鑑定化階段	1.民眾發現F銀行ATM吐鈔異常後報案。 2.F銀行通報特定ATM遭盜領。 3.領鈔車手身分、共犯。 4.交通工具。
概念化階段	1.案發地相關監視器調閱小組、同一型號遭駭ATM數位鑑識。 2.如何同步鎖定同一型號ATM地點並自動吐鈔及聯絡領鈔車手取款。 3.車手取款後之作為。
正規化階段	1.模擬以下狀況。 2.嫌犯各別入境時間、聯絡方式、如何分工、如何同步聽從指揮並至指定ATM進刑取款犯案、犯案後逃逸、集合、交付贓款及路線。
實作及測試階段	1.模擬歹徒行進路線，並調閱監視器加以證實交通工具、居住地點及逃逸路線後，最後於宜蘭縣警方查獲。 2.另模擬駭客攻擊F銀行主機及分行ATM，經數位鑑識後，證實係由F銀行倫敦分行入侵。
證實階段	1.本案依ATM監視器可得知，車手未操作ATM，但機器自動吐鈔，確定本案係駭客以遠端操作方式犯案。 2.破案後得知外籍犯嫌係以俄羅斯文並用通訊軟體與遠端駭客聯繫，並與數位鑑識結果相互佐證。 3.本案駭客係由F銀行倫敦分行入侵等情。

註：本研究整理。

(一)鑑定化階段(I)：（本案犯罪偵查知識工程化之流程如表1所示）

1.民眾向警方報案疑有2名男子在ATM錢從事不法行為

民眾向警方報案後，警方立即聯絡F銀行，經清查提款機電腦系統，並未顯示插卡獲不當方式提領紀錄，總計損失6百多萬元，進一步清查，發現全國共41台提款機共被盜領約8,000多萬元。

2.犯嫌作案方式

涉案犯嫌以1至3人為1組，犯案時以通訊軟體聯繫，北市警局指出本案犯嫌多以搭乘計程車匆忙趕路方式前往F銀行各提款機提領現金，犯嫌多為蒙面、變裝，經過濾大量錄影監視系統畫面比對，目前已確切掌握6名以上共犯身分。

3.提領方式

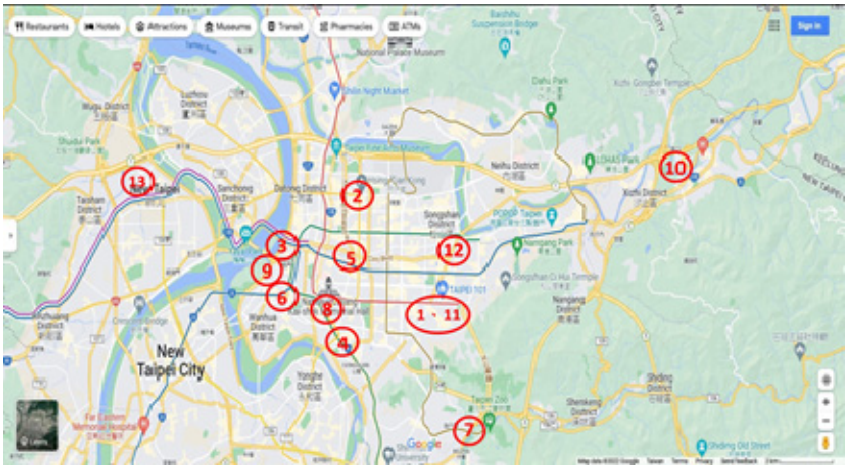
依照銀行的錄影系統發現，提款人幾乎是完全沒有碰觸到ATM的任何機器按鍵，鈔票竟然就從鈔票口流出。

4.ATM地點

根據統計，北中兩地共20間分行，42部ATM共遭嫌犯盜領8千多萬元，根據警方所掌握監視器畫面，初步研判嫌犯至少5人，而根據目前警方所公布，雙北共有12處ATM，被盜領13次（如表2），蘋果在大臺北地圖上標註，讓您瞭解這些嫌犯在2天之內，搜刮F銀行雙北ATM的地點（如圖5）（iThome，2016；蘋果日報，2016a；蘋果日報，2016b）。

圖5

F銀行在雙北遭盜領地點及次數地圖



註：iThome整理。

表2

F銀行在雙北遭盜領時間、地點及金額

1.	9日	09:00	信義光隆分行	基隆路二段82號	損失400多萬元
2.	10日	05:00	中山吉林分行	吉林路136號	損失380萬元
3.		05-08	萬華西門分行	西寧南路52號	損失約773萬
4.		07-08	大安古亭分行	羅斯福路二段95號	損失648萬元
5.		23-03	中正忠孝路分行	忠孝東路二段94號	損失約855萬元
6.		23:00	萬華雙園分行	中華路二段42號	損失260萬
7.	11日	00:15	文山木柵分行	保儀路12號	損失560萬元
8.		02:00	中正南門分行	南昌路1段94號	未遂
9.		01-02	萬華分行	康定路87號	新聞未提供
10.		03:00	汐止分行	大同路二段133號	新聞未提供
11.		05:00	信義光隆分行	基隆路二段82號	損失447萬元
12.		05:00	信義興雅分行	永吉路167號	損失188萬元
13.		05:00	五股分行	五股區五工路117號	新聞未提供

(二)概念化階段(C)

1. 確認ATM被破解原因

法務部調查局資通安全處確認國際駭客植入的兩支惡意程式分別為Cngdisp.eFe與Cngdisp-new.eFe，漏夜到F銀行測試發現，兩款惡意程式一次會讓ATM吐出現鈔6萬元，因此讓兩名嫌犯在短短60小時內，以遠端操控模式讓全臺20家分行及機關內38台自動櫃員機自動「開口吐鈔」，領走8千多萬元臺幣逃逸（如圖6）（聯合報，2016a；聯合報，2016b）。

圖6

F銀行ATM吐鈔大揭密

註：聯合新聞網及刑事局採訪整理。

2.犯嫌間如何聯絡、如何挑選機器

涉案犯嫌以1至3人為1組，犯案時以通訊軟體聯繫，目前已查知犯嫌國籍，以東歐國家居多，俄羅斯人為主，目前尚未掌握國人犯罪事證。

警方分析，犯嫌到指定的自動櫃員機後，以手機通訊軟體聯絡境外同夥，再遠端遙控櫃員機吐鈔；不過在北市領款過程並不順利，有兩次被熱心民眾察覺異狀報案，其他數次被打算領錢民眾干擾而未能得逞，後來另組人乾脆坐計程車到汐止、五股與新店等地盜領。

3.贓款流向

涉嫌盜領F銀行ATM鉅款的兩名俄羅斯籍男子，2016年7月11日上午從桃園機場出境；兩人略顯疲憊，通關時還打哈欠，得手的現金並沒隨身或託運攜帶，檢警專案小組因此研判贓款正透過國內地下匯兌管道匯出，正重建犯案軌跡試圖釐清贓款流向。

(三)正規化階段(N)

1.分析嫌犯各別入境時間、聯絡方式、如何分工、如何同步聽從指揮並至指定ATM進刑取款犯案

偵辦F銀行盜領案的警方專案小組，2016年7月12日清查確認來臺犯案的外籍嫌犯至少有6人，包括2名俄羅斯籍車手等4人已出境，拉脫維亞籍安卓斯等犯嫌還在臺灣；警方限制他出境，並撒網清查各大住宿處所準備抓人（聯合報，2016a；聯合報，2016b）。

根據入出境資料，犯嫌中有人在2016年7月2日抵達臺

灣，先遣部隊搭計程車到臺中「勘點」，2016年7月7、8日，安卓斯和2名俄羅斯犯嫌陸續抵臺，3人先到臺中與共犯會合「勤教」；2016年7月9日開始四處盜領，F個盜領地點就是臺中自由路的F銀行臺中分行。隨後，一組人留在臺中繼續盜領，貝瑞佐夫斯基、柏克曼和安卓斯及另外一組人轉往雙北犯案。由於臺北市是金融機構與自動櫃員機最多的地區，警方不排除犯嫌先到臺中是為了測試F銀行櫃員機系統、製作F銀行櫃員機分佈圖，並和地下匯兌業者接觸。

警方發現，2016年7月8日柏克曼和貝瑞左夫斯基來臺後，租車直奔臺中，與另2名先遣部隊人員會合勤教，警方查出這段時間他們的手機通話資料，有3、4通與臺灣人通話的紀錄，由於通話時間僅3~5分鐘，警方懷疑這名臺灣人可能是「帶路人」或「地下匯兌掮客」，正在清查釐清這名臺籍人士的身分（聯合報，2016a）。

2.分析犯案後逃逸、集合、交付贓款及路線

「抓到人，就能找到錢。」警方認為，F銀行遭盜領的8千多萬元贓款，還在這些滯留國內的犯嫌手上，他們試圖透過地下匯兌的管道將錢洗到國外，抓到人就能追回贓款。

(四)實作及測試階段(I)

1.歹徒選定F銀行於臺灣之ATM作為犯案目標，經分析有下列三項原因：

(1)首先，臺灣的ATM密度高。根據金管會資料，國

內金融機構ATM台數有2.7萬台，平均每850人就有一台ATM，業者說，最近幾年國外機構統計都指出，臺灣ATM密度在全球排名前十名，亞洲更是前三名。ATM一年交易金額高達9.6兆元，相當於五個中央政府總預算。臺灣地方小，歹徒犯案不必費太大力氣。臺灣人又習慣用現金，一台ATM裝了200多萬元現鈔，歹徒共得手8,000多萬元（聯合報，2016a）。

(2)第二，這次盜領沒有提領紀錄，沒有跟任何帳戶連結，機器就直接吐鈔，銀行主機也偵測不到。業者表示，如果是從帳戶異常提領，銀行主機馬上可以偵測，但沒有帳戶，主機無法立即偵測到，這個漏洞也讓歹徒有機可趁。

(3)F銀行2016年7月初大批更換34台ATM，剛好成為下手對象，而且分散北、中、南，顯見歹徒早就鎖定哪幾台要更換，而且是利用假日對帳空檔犯案。

2.模擬歹徒行進路線，並調閱監視器加以證實交通工具、居住地點及逃逸路線。

3.警方查獲3名犯嫌後，經數位鑑識使用行動電話及警詢筆錄，再調閱當地監視器，證實並釐清來去動線。

4.經數位鑑識後，證實係由F銀行倫敦分行入侵。

(五)證實階段(V)

1.依ATM監視器可得知，車手未操作ATM，但機器自動吐鈔，確定本案係駭客以遠端操作方式犯案。

2.破案後得知外籍犯嫌係以俄羅斯文並用通訊軟體與

遠端駭客聯繫，並與數位鑑識結果相互佐證，本案駭客係由F銀行倫敦分行入侵等情（臺灣臺北地方法院檢察署新聞稿，2016）。

肆、應用犯罪偵查知識工程化於刑案偵查實務

現行犯罪偵查工作都是遇案辦理，偵查人員僅被動地依照個人偵辦刑案經驗進行偵查工作，雖警政署訂有警察機關偵查犯罪手冊及警察機關分駐〈派出〉所常用勤務執行程序彙編，惟規範內容僅限於案件處理程序及處理原則，對於已偵破之案件尚未建立系統化、規則化之基本原則（如建立ICNIV modelling），致偵查人員如同「盲人摸象」，僅能慢慢摸索，並就個人過往偵辦經驗加以詮釋，因而容易在偵辦時產生盲點或謬誤，除了可能延誤偵破案件之時程而讓真正犯人逍遙法外，更可能因此造成第三人之權益受損，例如本案案發時，F銀行甚是婉拒警方關心，欲自行吸收損失，但翌日始知遭大規模盜領8,000餘萬，嚴重程度已非單一分行可承擔之問題。

犯罪偵查知識工程化正是為了協助員警針對過去偵破案例的經驗，提供即時、正確的案情研判方向，俾提供偵查人員快速掌握偵查要領，並協助偵查人員撰擬偵查計畫，建立具有專業及效能之偵查形象，提升偵查人員查緝能量。

偵查工作（ICNIV modelling），係從觀察犯罪發生

有關之人、地、時、事、物等事證著手（即所謂What to do工作，包括鑑定化階段），進而運用科學推理方法與科學鑑識技術，以被害人或目擊證人與犯罪現場及嫌疑人為偵查起點（即所謂How to do工作，包括概念化、正規化、實作及測試階段），找尋因犯罪所產生之一切變動現象，蒐集具體的事證或情報資料，經由推理論證與鑑定比對及分析研判，以期發掘更多線索（即所謂Why to do工作，包括證實階段），然後採取適當偵查行動，俾能緝獲犯罪嫌移人、查扣相關犯罪證據並正確推論犯罪事實，申言之，犯罪偵查之主要目的，在偵查「人」、鑑定「物」，以確定嫌疑人，瞭解犯罪事實之真相，掌握犯罪相關之證據，並且緝獲犯罪嫌移人，運用犯罪偵查知識工程化驗證偵辦結果（如表3）（林宜隆，2019）。

表3

運用犯罪偵查知識工程化驗證——依偵辦結果論證

F銀行ATM盜領案——運用犯罪偵查知識工程化驗證——依偵辦結果論證		
五大階段	步驟內容	依案例與偵辦結果論證
鑑定化階段(I)	蒐集所有現場犯罪痕跡及證物資料，找出問題。	1.民眾報案，疑有2名男子在ATM錢從事不法行為。 2.犯嫌作案方式。 3.提領方式。
概念化階段(C)	從事鑑識、檢討，以發現新的價值或認定問題。	1.確認ATM被破解原因。 2.犯嫌間如何聯絡、如何挑選機器。 3.贓款流向。
正規化階段(N)	多方假設，進而演繹歸納案情。	1.分析嫌犯各別入境時間、聯絡方式、如何分工、如何同步聽從指揮並至指定ATM進刑取款犯案。 2.分析犯案後逃逸、集合、交付贓款及路線。

表3（續）

F銀行ATM盜領案——運用犯罪偵查知識工程化驗證——依偵辦結果論證		
五大階段	步驟內容	依案例與偵辦結果論證
實作及測試階段(I)	依假設之答案分別反覆求證。	1.歹徒為何選定F銀行於臺灣之ATM作為犯案目標。 2.模擬歹徒行進路線，調閱監視器瞭解交通工具、居住地點及逃逸路線。 3.警方查獲3名犯嫌後，經數位鑑識使用行動電話及警詢筆錄，再調閱當地監視器，比對正確來去動線。 4.經數位鑑識後，證實係由F銀行倫敦分行入侵。
證實階段(V)	偵查結果所得推斷用以證明犯罪事實。	1.依ATM監視器可得知，車手未操作ATM，但機器自動吐鈔，確定本案係駭客以遠端操作方式犯案。 2.破案後得知外籍犯嫌係以俄羅斯文並用通訊軟體與遠端駭客聯繫，並與數位鑑識結果相互佐證，本案駭客係由F銀行倫敦分行入侵等情。

註：本研究整理。

伍、結論與建議

犯罪偵查是一種「高度智慧性」的活動（如知識工程化），它的主要目的是在偵查「人」、鑑定「物」，蒐集犯罪證據，以瞭解犯罪事實的真相；同時，犯罪偵查係在發掘犯罪行為心理上、物質上、社會上殘存的表徵，並依據一定的犯罪痕跡所能顯現的片段表徵來推理犯罪事實和犯罪人，進而蒐集證據等等基本的技術及推理法則；本案例中，犯罪集團係國際級駭客集團，不僅於犯案前可侵入F銀行倫敦總行電話總機為跳板，再進行單一機型ATM搜尋、植入惡意、測試吐鈔模組、執行盜領動作及最後之刪

除惡意程式及登錄紀錄，全程皆未遭發現，惟其一車手於取款時遺落現金而遭民眾報案發現本案，種種跡象顯見企業資安資訊不足，且間接嚴重影響檢警偵查形象，更是耗費大量警力人員投入偵辦此案。

犯罪偵查知識工程化正是為了協助員警針對過去偵破案例的經驗，提供即時、正確的案情研判方向，俾提供偵查人員快速掌握偵查要領，並協助偵查人員撰擬偵查計畫，建立具有專業及效能之偵查形象，提升偵查人員查緝能量。

建議如果我們能夠將特殊（重大）刑案等案例，逐漸累積相關偵辦經驗與建立刑案知識庫（Cases Knowledge Base, CKB）及犯罪偵查專家系統（Crime Investigation EFpert System, CIES），並且建立「合理化」、「科學化」、「系統化」、「規則化」之犯罪偵查基本原則，甚至建立犯罪偵查知識工程化（鑑定化、概念化、正規化、實作及測試與證實階段），不但可以強化證據取得之線索及連結有效性，同時更可以讓偵辦人員不用遇案摸索，並將犯罪紀錄之資料及資訊處理，提升至知識處理及知識管理，甚至是達到智慧管理及大數據分析（Big Data Analysis），並進一步提升其證據能力與證明力之有效性，且加速辦案效率、提升辦案形象。

參考文獻

- 林宜隆（1998）。整合性犯罪偵查專家系統之研究現況與未來趨勢。*警學叢刊，28*（4），263-278。
- 林宜隆（2009）。*網路犯罪理論與實務：網際網路與犯罪問題*（三版）。中央警察大學。
- 林宜隆（2011）。應用犯罪偵查知識工程化於刑案偵查實務之探討——以偵辦華采慧命案為例。2011年鑑識科學暨野生保育應用國際研討會。
- 林宜隆（2016）。應用犯罪偵查知識工程化於刑案偵查實務之探討——以八里雙屍命案為例。*電腦稽核，34*，78-92。
- 林宜隆（2017）。臺灣數位犯罪及數位鑑識發展現況與未來趨勢——以「創新司法警察IEK Model智慧模型」為例。*刑事政策與犯罪研究論文集(20)*（頁289-330）。司法官學院。
- 林宜隆（2019）。建立整合性行動鑑識標準作業程（iDEFSOP-M）與實際案例驗證之研究——以刑事警察局破獲之實際案例及驗證為例。*刑事政策與犯罪研究論文集(22)*（頁361-404）。司法官學院。
- 林宜隆、吳昆霖、施凱鏻（2016）。應用犯罪偵查知識工程化於刑案偵查實務之探討——以F銀行ATM跨國盜領案為例。Cyber2016研討會，大同大學，臺北。
- iThome（2016）。駭客入侵一銀AMT流程追追追。https://www.ithome.com.tw/news/107294
- 聯合報（2016a）。台版瞞天過海？一次看懂一銀盜領案始末。http://blog.udn.com/spark37/66173654
- 聯合報（2016b）。發展超戲劇化！一口氣看懂一銀盜領案始末。http://www.udnbkk.com/article-187032-1.html
- 蘋果日報（2016a）。這張圖告訴你　雙北被盜領ATM位置。

https://www.appledaily.com.tw/local/20160713/JXKALZYZRZC5NCPR2UTAEQB2TQ

- 蘋果日報（2016b）。11車手9人出境，警追台籍關係人。https://tw.appledaily.com/local/20160716/RN5JHKZNMJ6NQYD6CFZPNGRXEQ/
- 臺灣臺北地方法院檢察署新聞稿（2016）。臺灣臺北地方法院檢察署偵辦F銀行ATM現鈔跨國盜領案件，偵查終結簡要說明。