

## 鑑識&資安

社團法人台灣E化資安分析管理協會理事長、中央警察大學資訊密碼暨建構實驗室/王旭正教授

清流 MJIB

# 鑑識 & 資安 buddy buddy

◆ 社團法人台灣E化資安分析管理協會理事長、中央警察大學資訊密碼暨建構實驗室 (ICCL) — 王旭正教授

### 鑑識—判斷真假的代名詞

鑑識這字眼，直接聯想，就是追查新聞事件裡犯罪的軌跡。在臺灣擁有槍枝，甚至使用槍枝犯罪，那可是不得了的事件啊！從推敲的瞬間開始，就需要「鑑識」，因為由現場所遺留的子彈，可以推測槍枝種類，並進一步獲得彈道落點曲線等數據，抽絲剝繭地還原現場。是呀，這就是「鑑識」給人的印象—專業、判斷真假、還原事實。

### 訊息傳遞，「鑑識」需派上用場

然在這資訊時代裡，鑑識再也不單純只是專業形象而已，在人手一機，所有訊息都通聯的情況下，不經意間就會有各式的互動。訊息的傳遞怎會跟「鑑識」有關係呢？這可是有趣的事呢。還記得我們在前二期中提到的網路嗎？現在的資訊網路無遠弗屆，人們也是人手一機，隨時隨地在滑手機。透過手機，隨時上網找資料，應付工作需求或作為報告參考依據；也經



網路釣魚利用盲點設陷，在人眼對文字、圖像辨識的模糊下，讓人被導入惡意程式、病毒而成為受害者。

常在手機操作網路下單、交易買賣，手機網路的便利，使我們不經意成為訊息、資料的傳送者，亦或是接收者。當身為傳送者（主動角色），即是將所知道、擁有、經手的訊息，主動經由網路，在各個時間（anytime）傳遞到各個可到達的人（anyone）與地方（anywhere）。

主動者還有可能誤觸網路裡設下的圈套陷阱，您經常聽到的「網路釣魚」就是如此。設陷者用各式盲點，針對人眼對文字、圖像辨識模糊與好奇，例如“ICCL”與“iccl”，您有無看到前者的“l”是後者的“1”呢？讓您不經意進入異想新鮮的世界，自以為「樂透了」、「中獎了」而喜不自勝，事實上，卻是逐步陷入迷網，被反導入非法惡意程式、病毒，進入主動者的手機（或工作、作業的電腦平臺）反遭監控、破壞與洩漏主動者的個資資訊。這種情況便落入俗話俚語所說的「公親變事主」，

無端惹出麻煩來了呢。而當主動者反倒成了被攻擊的受害者時，「鑑識」隨即派上用場，在資訊流、資料流、時間流、啥「關連流」裡，能逐次釐清因果關係，尋出真假異同，那即是鑑識觀念在主動端的重要並立見真章。

在這個互動頻繁的網路世界裡，主動者當然也會變身為被動的接收者角色。在被動者方面，一般會接收到3種型態的訊息，一則是文字訊息，二則是多媒體性訊息，三則是程式碼訊息。就網路資訊傳播發展早期，這3種型態裡，最令人畏懼的是第三種「程式碼」訊息，避之唯恐不及呀。

### 病毒程式發明者

程式碼訊息型態病毒來源可回溯自1960年代，由美國電話電報公司（AT&T）貝爾實驗室裡的幾個年輕小伙子所設計出來。原先動機只是好玩，設計出會覆蓋或破壞對方玩家電腦記憶體體的程式，由於病毒（遊戲）程式的原始碼很小，使得此程式極容易被複製，而具有高存活率，也會攻擊與破壞另外的病毒（遊戲）程式，這就是程式設計者與玩家認定的最有趣之處——在相互攻防裡，取得最終的勝利，呵呵，換言之，就是把對方程式（遊戲）完全消滅，讓「病毒」成功入侵系統。

1986年，巴基斯坦人製造出Brain病毒程式，讓全世界注意到病毒程式會影響到電腦的正常運作。臺灣在1999年也不遠

多讓，有一聞名世界的 CIH 病毒，即由臺灣年輕人所設計，讓當時亞洲災情極為慘烈。

這些程式碼訊息隨著時空科技的演進快速翻倍進展，早已集結各家「精華」、各路「險招」、行極「冰寒」於一身。從古早的遊戲病毒（virus）源起，進化成本馬程式（Trojan Horse），網蟲（worm）、攻擊程式（attack programming），讓資安世代網民經常誤陷泥沼。

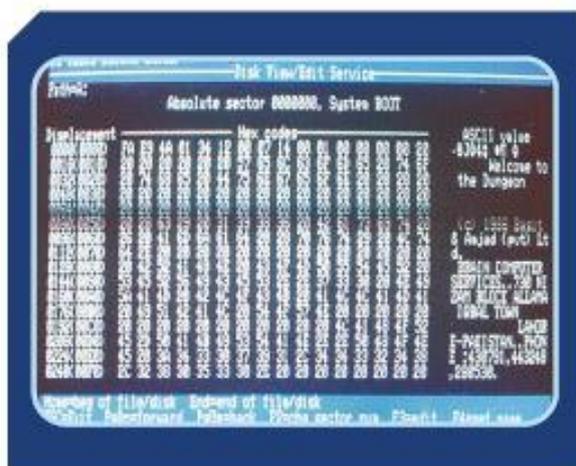
## 看不見的敵人最可怕

程式碼訊息雖最令人懼怕，卻也因敵在「明」，我們可藉「跡證」來辨識訊息「真假」，以避免踩到地雷。最直觀的方式，就是當收到不明的檔案或程式碼，尤其是具有執行能力的程式碼（例如副檔名

為 exe 者）時，即刻快閃刪除，就免惹到「無妄之災」。

再則，我們來到被動者接受訊息的第二種型態，那就是多媒體訊息。多媒體訊息在資安領域裡，是有別於密碼學（cryptography）的，我們稱為偽裝學（steganography），兩者最大不同在於「偽裝」二字，即「有看沒有懂」，亦即英文「Seeing the unseen」。以大自然生態為例，許多動植物都是偽裝專家，就像變色龍般，能隱藏於樹叢枯枝中，然後隨著綠葉枯樹的色澤而進行調變其身體顏色，讓食物鏈上層的獵食者，瞬間看不見其蹤跡，其實牠非「消失無蹤」而是「近在眼前」呢！

偽裝，不只發生在大自然裡，在生存遊戲中，更是「適者生存」的重要工具。



1986 年，巴基斯坦人製造出 Brain 病毒程式，此病毒會感染開機磁區，影響電腦正常運作。（Photo Credit: Avinash Meeto, <https://commons.wikimedia.org/wiki/File:Brain-virus.jpg>）



「木馬」是一種後門程式，駭客用其盜取使用者的個人訊息，甚至進行遠端控制。（Photo Credit: BrayLockBoy, [https://commons.wikimedia.org/wiki/File:MEMZ\\_Trojan\\_running\\_on\\_Samsung\\_N130\\_13\\_December\\_2019.jpg](https://commons.wikimedia.org/wiki/File:MEMZ_Trojan_running_on_Samsung_N130_13_December_2019.jpg)）

人類歷史在偽裝運用上頗精彩絕倫，尤其在戰爭史實上，最讓人嘖嘖稱奇。看似無奇的一頭秀髮，當剃光頭髮後，竟看到機密訊息，得以完成戰事攻防裡，祕密通訊的目的。

### 霧裡看花，花還是花？

在當代，我們所接觸到的訊息更具變化，真真假假、五花八門。為何包裝程式碼的多媒體訊息能如此活躍？主要是因人類眼睛對於色彩具有失真的容忍度，也就是我們玩笑話裡的「朦朧美」、「霧裡看花、花還是花」的感官意識。

對於影像，當人腦認定有何涵義時，是草、是河、是山、是屋，那是深刻烙印在腦海，不會因模糊而改變的印象。而數位時代，構成數位影像圖的每個像素，若改變裡頭一些像素資料時，且在視覺容忍度與感官意識可接受下，人眼將無法識別其差異性，此時多媒體影像所包裹的訊息就可以混水摸魚，逃過一劫，達到得以祕密傳遞的目的。

當然，對於訊息暫時接觸者所接觸到的是一張、一份多媒體假訊息的影像圖，所認定也是一份貨真價實的、具有意義的多媒體資訊，所以暫時接觸者因此以為是「真訊息」。然對為達成訊息傳遞的通訊雙方——即訊息的傳送者與接受者，目的是要讓中間的暫時接觸者，看到「假訊息」，即誤以為影像圖是「真訊息」。到此，真假之間，是



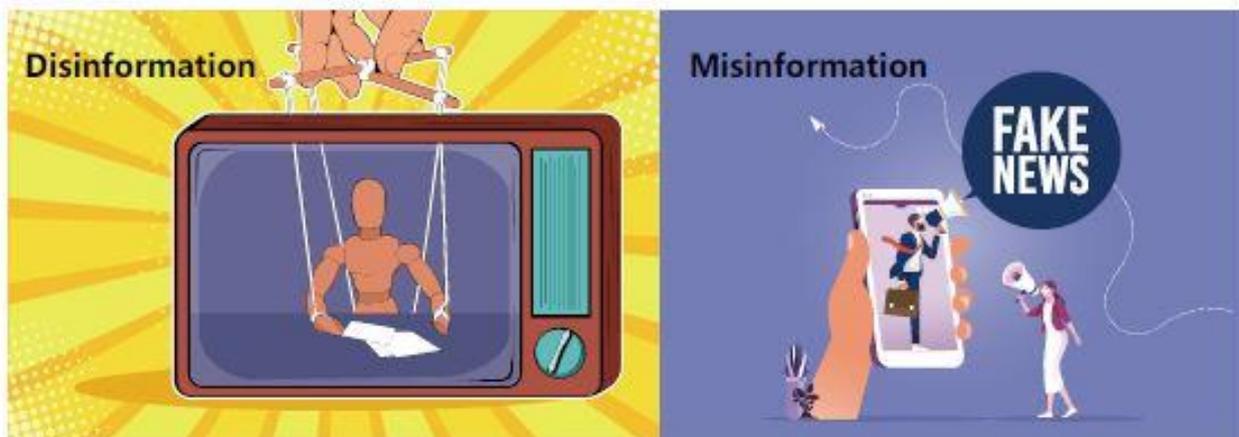
大自然生態中，許多動植物都是偽裝專家，多媒體訊息在資安領域裡亦為偽裝大師。

否您也看得霧裡看花，不再是花，而是「霧煞煞」了。

偽裝之意，在於欺敵，在第二種的多媒體訊息形態裡，或許無誤導於呈現多媒體訊息時的具體內容（有論無意或蓄意），因該訊息意在偽裝多媒體內涵裡的真實祕密。

### Misinformation 與 Disinformation

然而被動者的訊息接收裡，第一種訊息型態的文字訊息，是最令人毫無防備的。若其為假訊息，將是這 3 種訊息型態中影響最為深遠的訊息。對於假訊息，歐洲理事會有一相關名稱為「資訊失序」／「Disinformation」（原文：Information that is false and deliberately created to harm a person, social group, organization or country），其是指經過刻意編造，用以傷害個人、社會團體、組織或國家之訊息，目的在煽惑或鼓動人



Disinformation 是指經過刻意編造的錯誤訊息，用以傷害他人、組織或國家之訊息；Misinformation 為內容有虛假嫌疑，惟因缺乏惡意欺騙之意圖，故多屬誤傳。

心，藉以謀取某種政治或商業利益；另外「資訊失序」還有一種描述用語為「Misinformation」（原文：Information that is false, but not created with the intention of causing harm）則是指內容錯誤但目的並非為造成傷害而刻意創建的訊息。在假訊息之要件上，國際組織主張應符合真實性（fidelity）與目的性（intention），所以「Misinformation」雖內容有虛假嫌疑，惟因缺乏惡意欺騙之意圖，多屬誤傳性質之訊息。而「Disinformation」是目前較符合國際對假訊息之定義或共識，是有系統性的作假，企圖製造損害、影響特定人士或組織，導致社會紊亂，屬政府部門應該積極防處之範疇。

### 透過資安密碼技術 管理訊息傳送

對於文字的假訊息，咱資安科技裡的密碼技術，並不因此坐視不管，反倒有好的因應呢。回顧上一期的 PK（public key），在公開金鑰系統裡的使用，如果訊息的傳遞，由真實來源的傳送者在傳送的

過程中，加上與訊息緊密相關的驗證碼，那麼不就可以清楚地知道訊息是真、是假，有無被竄改。

在現代密碼技術中，有個重要名詞叫「HASH」，「HASH」這武器是能夠不管訊息有「山這麼高、海這麼深」，都可以變成一個短短的資料量，好像是神奇的魔術一樣。例如一個超大硬碟容量，可以變成一串短短字串，只要硬碟裡的一絲點位元或一根寒毛被動到，這短短字串就會變得不一樣。因此，當訊息在 HASH 第一次運算和 HASH 第二次運算後，結果都一樣，就代表這個硬碟裡的東西沒被動過，很神奇吧！

在假訊息傳遞充斥的世代裡，我們運用資安科技裡的密碼技術處理假訊息，就不用流於口水戰。有了這兩大法寶——「PK」還有「HASH」，假訊息就無所遁形了。發布訊息時使用 PK 系統，然後再進行比對，如果兩邊內容一樣，就可證明訊息是由真實來源端所提供。

處理機制裡，我們可先用 HASH 做訊息的處理，因為一般訊息較長，用 HASH 的技巧可變成比較短的訊息，而且用 HASH 也可以用來保證一旦訊息被更改後，可以很快地發現被竄改。因為一旦原始訊息的一個文字或一丁點的位元資料被改變，整個 HASH 的結果都會不一樣，接下來就是再用 PK 系統來產生驗證碼。以前兩期孫悟空與牛魔王的故事裡，我們稍作小技巧，增加了 HASH 技術，可立見真章，讓人一點就通。

這裡我們討論真、假訊息的兩種狀況，第一種訊息傳遞是無論訊息真假，但發布訊息的人是假（不對）的，舉例來講：今天要發布獎懲訊息，這種訊息不是每個人都

可以發布的，一定要是權責單位發布的。假設今天是路人甲、乙、丙說的，擅自發布的訊息都要打個問號，因為這些人不是權責單位。當然若是權責單位承辦人、發言人講的，那訊息可信度即是相對提高的。在 PK 系統的驗證碼比對中，真正權責單位的 PK 再搭配 HASH 的處理，能讓事實立即擺在眼前。

另外訊息傳遞的第二個情形是，權責單位的確發布事實訊息，但發布的訊息被蓄意先下架，內容遭竄改後，例如把褒獎令的內容改掉，再進行發布。此情形裡，發布的權責單位是對的，但是內容是被改過的。但是在這一個過程中加上一個 HASH，就可以把這問題爭議處降到最低，因為依照所提



圖 1 PK 系統與 HASH 的搭配處理



訊息漫飛時代，各式傳聞不斷，虛虛實實、假假真真，民眾看多假訊息之後，可能連政府發布的真訊息也不再相信了。

到的密碼技術概念，HASH 這武器可清楚證明訊息是否被造假竄改。例如，若今天褒獎令的訊息裡有相關人物數量的名額是「10」位，被修改成「9」位，就會發現所傳遞褒獎令的訊息經第二次 HASH 的運算後會很不一樣，所以搭配 PK 的 HASH 也是解決假訊息的關鍵技巧之一。

## 假做真時真亦假 假訊息竟成「網紅」？

訊息漫飛時代，各式傳聞不斷，虛虛實實、假假真真，套句紅樓夢賈寶玉的名言「假作真時真亦假」，因此當民眾看多假訊息之後，可能連政府發布的真訊息也不再相信了。

在資安科技裡，除了最為直觀認知的重要「隱私」保護外，另一訴求就是「鑑定」，也就是對於來源能清楚、對於訊息的真假判斷能有依據，得具有說服力。而「鑑識」即是在「鑑定」的各式場合、各式情境裡，在人為、人治世界的生活互動裡，無論有意、無意的侵犯裡，在所遺留的證據痕跡中，能抽絲剝繭、步步推理，找到真相、重建現場。資訊生活裡，我們使用的 3C 平臺讓我們更方便操作訊息，是傳遞訊息的主動者，也是接收訊息的被動者。在享受訊息多元化、知識普及化的同時，另一類資安危機也浮上檯面。真、假訊息在這些年來，成了「網紅」，不知覺淪為各式可能不當企圖運用的操作，得以混淆人的意識與判斷，影響生活，甚至造成社會問題與資安危機，甚至被科技犯罪利用得以獲利。現在藉由資安的密碼技術發揮，在人手一機的訊息來回裡，訊息得以「鑑識真假」。傳統的人腦思維判斷方式已轉化成資安科技的「鑑識」加乘確認，藉此得以保障「真假」訊息傳遞的真實性，減輕可能的權益損害，「鑑識」儼然成為資安生活中共生共存的 buddy buddy 新重要搭檔。



社團法人台灣 E 化資安  
分析管理協會 (ESAM)



中央警察大學資訊密碼  
暨建構實驗室 (ICCL)

## 社群媒體你相信嗎？網路訊息誰說了算？

社團法人台灣E化資安分析管理協會、東海大學資工系／賴俊鳴

生活中的資安



# 社群媒體 你相信嗎？ 網路訊息誰說了算？

◆ 社團法人台灣E化資安分析管理協會、東海大學資工系 — 賴俊鳴

隨著社群媒體盛行以及步調愈來愈快的資訊速食文化，使得民眾愈來愈難接觸到專業且客觀的資訊，「假新聞」一詞漸成為互相攻訐的工具。

### 訊息戰並非社群媒體獨有

從歷史的角度來看，散播不實謠言以達到娛樂，甚至政治、經濟的目的案例比比皆是。最著名的有出自荷馬史詩與希臘神話的「特洛伊之戰」，希臘聯軍利用巨大木馬躲藏伏兵，並派奸細至特洛伊城內散布希臘聯軍已撤退，且巨大木馬為獻給神的戰利品等錯誤資訊，最終讓久攻不下的特洛伊城陷落。另一方面，訊息真偽也可能隨著時間而改變，例如：「地球繞著

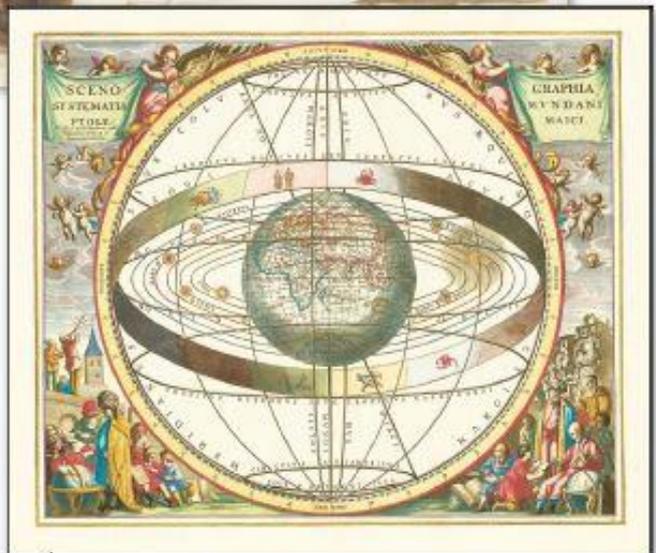
太陽轉」於中世紀被認為是偽科學，因該時代人們普遍相信地球乃是宇宙中心。試想，若連最嚴謹的同儕審查之學術論文也無法保證其真確性，更遑論缺乏監管機制且幾乎人人可發文的社群媒體？

自從美國前總統川普多次稱呼對他負面報導以及評論的資訊為「假新聞」，加上各大網路巨擘因資料隱私問題紛紛被傳喚至美國國會聽證會後，社群媒體安全與隱私議題迅速席捲全球。



歷史上著名的「特洛伊之戰」即是希臘聯軍利用巨大木馬躲藏伏兵，故意傳播錯誤訊息，成功欺騙敵軍，最終順利奪下特洛伊城。(Photo Credit: Created by Giovanni Domenico Tiepolo, circa 1760)

臉書 (Facebook) 於 2018 年開始終止其他應用程式透過 API 取得帳號階層的資訊，包括討論、留言、按讚，以作為對於「劍橋分析」事件<sup>1</sup>的防火牆，因為「劍橋分析」事件已證明廣告足以影響選舉結果。<sup>2</sup> 推特 (Twitter) 更成立了一整個部門，透過人工智慧以及資料探勘技術，定期公布其檢測之可疑帳號，包括中國大陸、俄羅斯、烏干達以及委內瑞拉等國家的可疑帳號。<sup>3</sup>



「天動說」是一種天文學學說，認為地球是宇宙中心，其他日月星辰環繞著地球運行，初期頗為人民普遍接受；文藝復興時代後，隨著科學技術的進步，以太陽為宇宙中心的「地動說」證據逐漸出現，偽科學因此被證實取代。(Photo Credit: Created by Andreas Cellarius, 1660)

<sup>1</sup> Cambridge Analytica 聲明透過單一平臺的帳號歷史資料之搜集、探勘與分析，足以使政治廣告公司推薦用戶相關資訊，進而影響選舉。  
<sup>2</sup> 劍橋分析是一家英國的數據公司，創立於 2013 年，曾在 Facebook 上推出一款免費心理測驗 App，被發現在未經用戶許可的情況下，盜用 Facebook 5 千萬用戶個資，同時，也被質疑是 2016 年美國總統大選川普團隊用來左右選舉的幕後黑手。<https://www.bnext.com.tw/article/55756/cambridge-analytics-election-taiwan-facebook>。  
<sup>3</sup> [https://blog.twitter.com/en\\_us/topics/company/2021/disclosing-state-linked-information-operations-we-ve-removed](https://blog.twitter.com/en_us/topics/company/2021/disclosing-state-linked-information-operations-we-ve-removed)



「劍橋分析」是一家數據公司，曾受聘於川普競選團隊。當時在臉書推出一款心理測驗 App，取得部分用戶資訊，後被發現未經許可盜用臉書 5 千萬用戶個資，涉嫌用來操縱美國總統選情。(Photo Credit: Book Catalog, <https://fic.kr/p/Hoh2Y>; Gage Skidmore, <https://fic.kr/p/MQVjM6>)

臉書前資安長 Alex Stamos 教授將資訊頻道依據溝通方式分成數類，<sup>4</sup>如圖 1 所示。倒三角形最下方為一對一的溝通模式，例如臉書即時訊息 (Facebook Messenger)、Line 帳戶對帳戶等皆為此類，愈往上觸及受眾愈多，即擴大效應愈

明顯，另一方面，愈往下對隱私的考量愈重。從最下方一對一的溝通模式往上依序為群組訊息 (例如 Line 群組)、私有個人帳號、邀請制的粉絲專頁、公開個人帳號、公開粉絲專頁，接著透過推薦引擎將所有資訊與演算法結合，推送最容易吸引使用者花費更多時間的內容。

### 有創意的攻擊者帳號

相比於傳統媒體，社群媒體通常不具編輯審查機制，好處為資訊的流通更即時且開放，缺點則為資訊真偽難以驗證。

為吸引相對多的使用者透過按讚、留言、分享方式與文章互動，一個最通用且常見的特徵為發布之初，攻擊者先利用程式同步創造一群一群的帳號，<sup>5</sup>等到收到指示要炒熱某文章後，再透過「養好的」帳號群 (Clusters) 向社群推薦系統發起攻擊，結合所謂「心理學認知攻擊手法」，

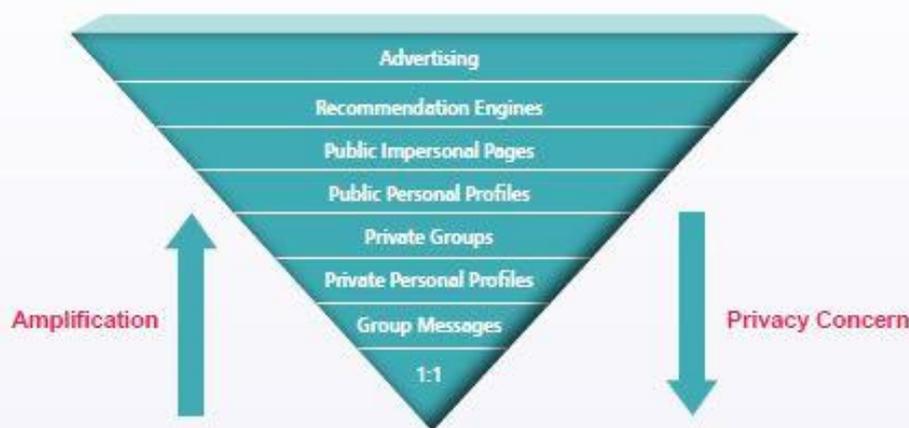


圖 1 資訊頻道分層圖

<sup>4</sup> 2019 年於全球頂尖資安會議 USENIX 大會分享其於臉書以及史丹佛大學長期研究社群媒體安全議題。

<sup>5</sup> 攻擊者可透過逆向工程方式得知如何使 (欲散布) 訊息被社群平臺之推薦引擎所擴展。

例如從眾效應（Bandwagon Effect）、<sup>6</sup> 沉默螺旋（Spiral of Silence），<sup>7</sup> 使某文章收到比預期強大的效果，進而影響使用者現實社會中的行為。

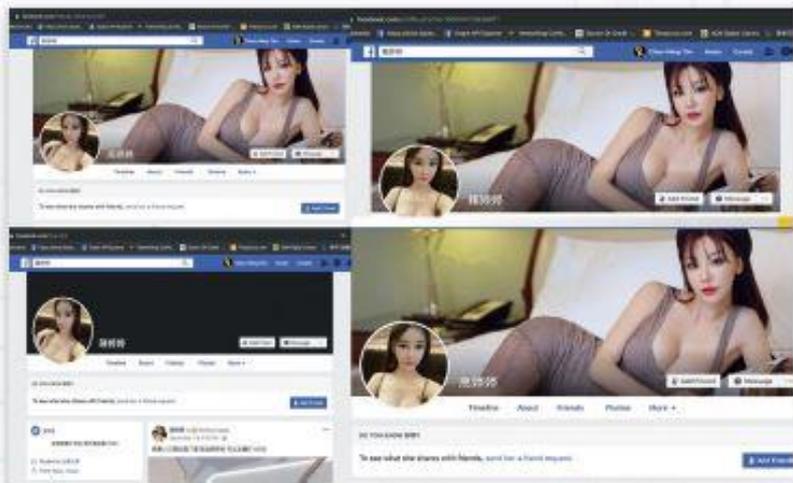
根據筆者研究，這些殭屍帳號取名相當有創意，例如有古詩詞家的帳號群（李清照、李白、杜甫等）、古代皇帝的帳號群（李世民、朱元璋、朱標等），還有類似 AI 影像處理變換的美女身分，創立不同帳號，彼此為朋友，經常針對某議題「共同出擊」，因此，偵測「同步非真實行為」（Coordinated Inauthentic Behavior, CIB）議題目前為社群媒體安全之重點發展領域。

然而刪除帳號此一舉動，對於投資人衡量社群公司有顯著負面影響，例如 2022 年 Q1 因為臉書月活躍用戶（Monthly Active Users, MAU）數量首度下滑，造成一個禮拜股價大跌 39%，市值蒸發約 7.4 兆臺幣；<sup>8</sup> 因此各大社群公司對於處理此類可疑帳號仍然保持曖昧不明的態度。

### 驗證訊息真偽方式

目前學術界以及社群媒體公司對於社群平臺上的資安問題大略分成四個方向來偵測與緩解，如圖 2 所示。最上層為根據文字語義與內容，通常透過大量人力來逐一檢驗訊息的真偽，以類似學術論文之同儕審核機制，根據每一則回報訊息發表核實報告。國內常見的組織有「台灣事實查核中心」、「Cofacts 真的假的」以及「MyGoPen（麥擱騙）」等；<sup>9</sup> 缺點為人工審核耗時費工，且資金來源若為商業以及政府計劃，易招惹不中立之批評。最底層為帳號階層的防禦，透過 Captcha 以及帳號活動關聯等技術，

抑制殭屍帳號的創造與維持；



殭屍帳號通常採用某種固定模式設定身分，圖為 4 個不同帳號，但影像資料皆相同，彼此為朋友，且經常針對某一議題「共同出擊」。（圖片來源：作者提供）

<sup>6</sup> 指人們受到多數人的思想或行動影響，而跟從大眾想法或行為的現象。

<sup>7</sup> 當人們發現自己意見與主流意見不同時，因為害怕被孤立或迫害，便會選擇隱藏自己意見，保持沉默，最後支持主流意見的聲音會愈來愈大，而弱勢意見的聲音逐漸消失。《和主流意見不同的人，為什麼會選擇沉默？》，<https://www.managertoday.com.tw/glossary/view/55?>

<sup>8</sup> “Down 39% in 2022, Meta Platforms Is a Screaming Buy Right Now”, <https://www.fool.com/investing/2022/02/28/down-39-in-2022-meta-platforms-is-a-screaming-buy>.

<sup>9</sup> 台灣事實查核中心，<https://tfc-taiwan.org/tw/>；Cofacts 真的假的，<https://cofacts.tw/>；MyGoPen（麥擱騙），<https://www.mygopen.com/>。

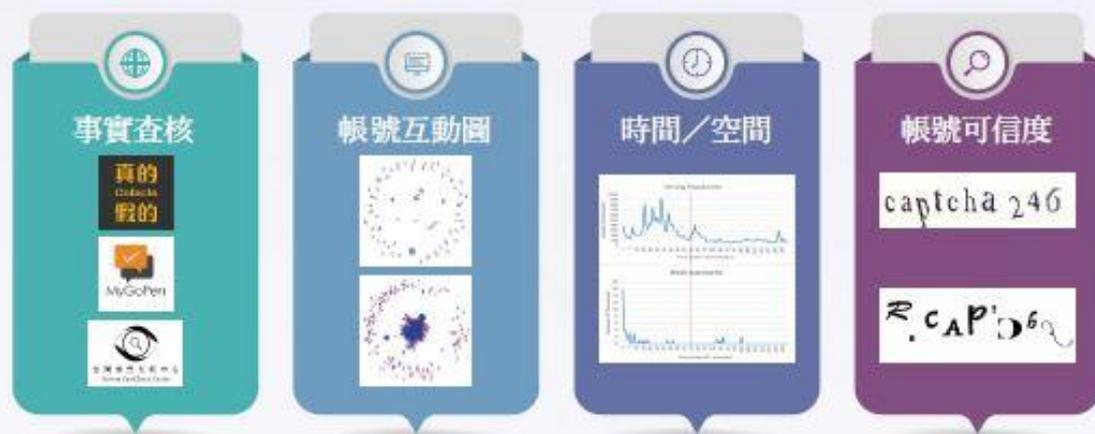


圖 2 目前檢驗訊息可信度的方式

缺點則為平臺掌握絕對權力，且容易侵犯用戶隱私。

除了帳號偵測與人工審核之外，另可針對可疑訊息的流傳範圍、特徵下手，給定一則訊息，觀察其流傳的頻道（粉絲專頁）、時間、地理位置，以及其參與者彼此間是否有不正常之協同行為。透過近年發展迅速的人工智慧以及巨量資料等技術，搜集大量標記的可疑訊息之特徵，運用文字向量化、圖卷積網路等深度學習技術訓練一分類器，使得電腦自動分類未來訊息是否為可疑新聞，或者來自地理位置變換快速的發文者，進而自動化調整社群推薦系統權重，在降低可疑文章推送的同時，也同步標記可疑的粉絲專頁以及個人帳號，使得攻擊者做逆向工程以及發動殭屍帳號群的成本大增。缺點為只要知道平

臺檢測的人工智慧演算法，攻擊者還是有辦法創造出可以混淆分類器的可疑新聞，繞過電腦的檢測，可謂是「道高一尺、魔高一丈」。

### 傳統中心化社群媒體

為什麼社群媒體平臺安全問題近年來引起關注，我們需要從其特性講起。中心化社群媒體主要由少數人控制和單一集中伺服器運作，而每個社群媒體都有各自不同的訊息審查標準及權限規則，也因如此，使用者在分享或發布訊息時，並不一定能夠暢所欲言，甚至公眾人物可以發布不實訊息去影響群眾。

中心化社群媒體主要有以下特性：伺服器由單一組織掌控<sup>10</sup>、少數人對於社群

<sup>10</sup> 伺服器屬於某社群媒體公司，社群媒體的一切運作皆由該伺服器執行，所需資訊均在伺服器統一管理。當有需求者向伺服器尋問時，可以快速取得所需資訊，然若使用者數量增加到一定程度時，伺服器將面臨擴充性的問題，或是伺服器故障時無法分散風險系統將會整體癱瘓。



中心化社群媒體的伺服器由單一組織掌控，擁有極大的控制權、主觀的審查標準，且資料為封閉、集中式的儲存，恐面臨系統整體癱瘓、使用者資料被出售、言論爭議產生與駭客攻擊時資料全數外洩等各項風險。(Source: floyx, <https://www.floyx.com/learn-more#section3>)

媒體擁有極大的控制權<sup>11</sup>、主觀審查標準<sup>12</sup>與資料為封閉且集中式儲存<sup>13</sup>等，恐將面臨系統整體癱瘓、使用者資料被出售、言論爭議產生與駭客攻擊時資料全數外洩等各項風險。

### 區塊鏈與社群媒體

區塊鏈技術透過密碼學數位簽章、雜湊函數以及共識獎勵機制來達成四大特性，包括：去中心化、匿名性、不可篡改、

共識與獎勵機制。而上述特性恰為當前中心化社群媒體所需要革新的方向。

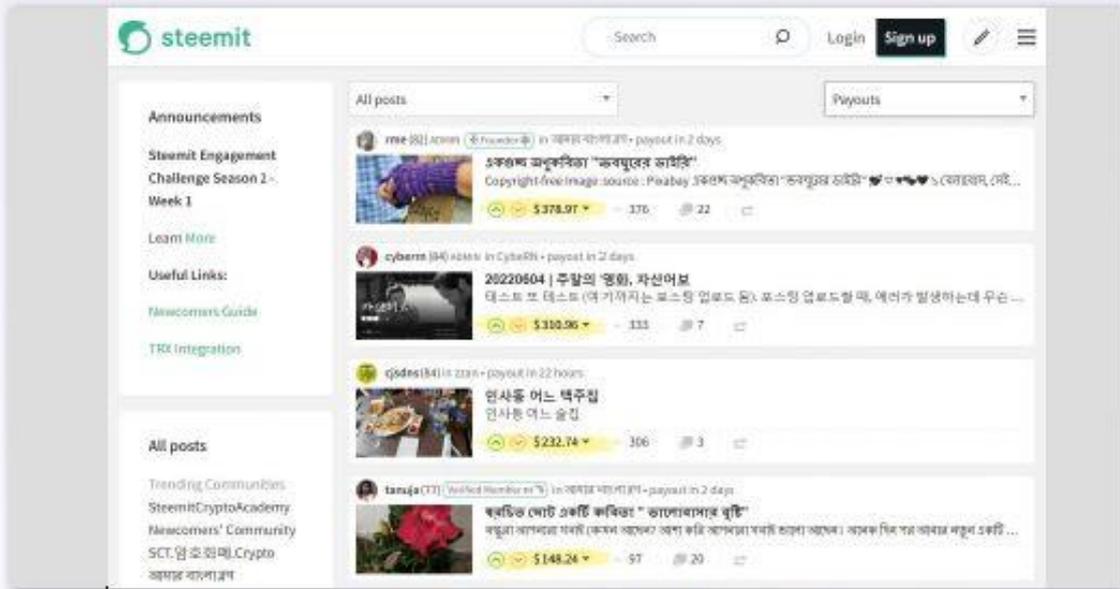
關於去中心化特性，因為區塊鏈會在全世界擁有多個複本，因此應用於社群平臺發表言論可說是「覆水難收」。<sup>14</sup>在帳號管控方面，區塊鏈社群平臺與比特幣、以太坊系統一樣，只要用戶產生出公私鑰配對，即可以加入討論區且保持匿名性。最後也是最重要的是，區塊鏈社群平臺改寫了由傳統社群媒體公司壟斷的分潤機制

<sup>11</sup> 在社群媒體上所有的使用者資料都掌控在該社群媒體公司，而社群媒體公司擁有刪除使用者資料的權力，甚至將使用者資料出售給利益團體。

<sup>12</sup> 每個中心化的社群媒體對於言論尺寸拿捏的規則標準不一，皆是由該中心化社群媒體主觀單方面認定為不當言論，而當言論的適切性皆由主觀認定時，最後將導致控制使用者言論的爭議產生。

<sup>13</sup> 集中式儲存雖然可使需求者快速獲取資料，但資料無法分散資料流出風險，例如發生駭客攻擊事件時將會有很大的可能性資料全數外洩。

<sup>14</sup> 包括 Twitter、Facebook、Instagram 等平臺只要結束運營，或者可由使用者、平臺端刪除某言論。然而在以後的區塊鏈社群平臺所有發言一旦上鏈後，所有的文章、留言皆永久保存。



區塊鏈社群平臺的特色為「使用者即股東」，全球最大的 Steemit 平臺盈餘有 90% 分配給股東，其中包含發布訊息的獎勵；而篩選訊息內容好壞則由全體用戶投票決定，訊息品質愈高的人獲得獎勵愈多。（Source: Steemit, <https://steemit.com>）

出來，讓用戶投票，誰的股權多，占比就愈高，最後訊息品質愈高的人獲得獎勵愈多。為了防止用戶惡意炒作，其引入類似否決票（即有正義用戶舉報）、投票速度限制以及延遲文章獎勵機制，類似各國申請信用卡所需審核的「社會安全碼機制」，任何不良記錄都會永久保存，信用值較低的帳號起不了任何炒作的的作用。

總體來說，區塊鏈社群平臺機制相當複雜，且變動極其快速，但其擺脫了中心化社群媒體固有的封閉框架，然而是否真為一可靠資訊傳播平臺，仍有待時間以及市場來證明。



社團法人台灣 E 化資安  
分析管理協會 (ESAM)

### 區塊鏈社群平臺技術， 防範假訊息流竄新利器

各種通訊軟體愈來愈多元，接收各種資訊的頻率越來越高，這些平臺默默蒐集使用者資料並且導致許多安全與隱私問題。在治標方面，包括人為識別可疑訊息、定期辦理澄清工作坊、殭屍帳號偵測與移除、運用人工智慧篩選可疑訊息異常傳播時空路徑、訴諸法律管理等措施，皆為有效杜絕有心人士藉社群平臺詐騙、認知作戰，進而瓦解人民、特定組織與國家安全的手段。在治本方面，新興區塊鏈社群平臺技術或可帶來革命性的創新，惟尚須時間證明。