# 認知作戰與全民防制

調查局兩岸情勢研析處前處長-劉文斌



# 認知作戰與全民防制

◆ 調查局兩岸情勢研析處前處長 — 劉文斌

以訊息作為改變他人認知，進而改變他人行為，此趨勢已由個人事務提升至國家高度，成為各國政府所無法忽視之國安問題。

## 認知作戰已成為現代戰爭的第6個場域

以訊息（information）影響對手決策，使事件發展對己有利，並非新聞，在歷史故事中的空城計、草船借箭，近代的心理作戰等等不勝枚舉，但隨著快速方便的通訊器材普及，尤其個人攜帶式智慧型通訊裝置的盛行，更使以訊息作為改變他人認知進而改變他人的行為被發揮到極致，此種趨勢已由個人事務提升至國家安全高度，是當前各國所無法忽視的問題。

而北大西洋公約組織在將現代戰爭衝突分為陸、海、空、太空及電腦空間等5個場域之後，[1] 認知作戰已逐漸被認證為第

※ 本文依據2022年「兩岸情勢與區域安全前瞻」研討會之劉文斌「認知作戰與防制—以訊息傳遞模式為視角」論文改寫而成。

[1] Lea Kristina Bjørgul , "Cognitive warfare and the use of force," *STRATAGEM*, November 3, 2021, https://www.stratagem.no/cognitive-warfare-and-the-use-of-force/. NATO currently recognizes five warfighting domains: land, sea, air, space, and cyberspace.


空城計、草船借箭是歷史上知名以謀略取勝的故事，出自名著《三國演義》，後廣為人所知。

6個場域，[2]致使認知作戰的攻防已攸關國家安全，不得不慎重以對。

## 認知作戰無平戰、敵我之分

傳統對戰爭的認知，無法擺脫兩個國家或團體的武力爭鬥，但如今又演化出經濟戰（economic warfare）、電腦戰（cyber warfare）、法統戰（political-legal warfare）等對抗形態的無煙硝戰爭，[3]致使當前的「戰爭」可以被理解為一個團體（國家或非國家）利用一切可用的手段，如外交、經濟、資訊、社會和教育及軍事力量，影響對手遵行他們的意願。[4]而致使在無煙硝中改變對手認知行為的「認知戰」，就無平時、戰時之分，[5]成為必須警惕的第一道防線。

而認知作戰對象，不僅針對敵方，更涵蓋友方，不論對敵友都日以繼夜地進行訊息對抗（information confrontation is waged constantly in peacetime）。[6]換言之，在平時亦要對不論敵友的對手進行認知觀念改變，其目標當然是希望「友我者更加友我，敵我者較不敵我或甚至轉變成友我」。若友我者因敵人之認知作戰變成不友我，而敵我者卻更敵我，則可以預見認知作戰的失敗；反之，若友我者更友我，敵我者少敵我甚至友我，則可被確定是認知作戰的成功。

[2] Dean S. Hartley III and Kenneth O. Hobson, *Cognitive Superiority*, Springer, 2021, pp. 12, 15.

[3] Diana Mackiewicz, "Cognitive Warfare," November 16, 2018, https://www.researchgate.net/publication/337228818_Cognitive_Warfare_-_Mackiewicz-Diana_2018.

[4] Jill Long, "What is War? A New Point of View," *Small Wars Journal*, May 12, 2012, https://smallwarsjournal.com/jrnl/art/what-is-war-a-new-point-of-view.

[5] Kimberly Orinx and Tanguy Struye de Swielande, "Cognitive warfare and the vulnerabilities of democracies," *CECRI*, May 12, 2021, p. 2, http://cecrilouvain.be/wp-content/uploads/2021/05/cognitive-warfare-.pdf.

[6] Keir Giles, "Russia Information Warfare," in Timothy Clack and Robert Johnson Eds., *The World Information War*, Routledge, 2021, p. 139.


現今各國已演化出經濟戰、電腦戰、法統戰等對抗形態的無煙硝戰爭，已非傳統的武力爭鬥對戰。


## 諸多案例令人警惕

臺灣是遭受境外假訊息最頻繁的國家，早被國際社會關注，更已蟬聯 9 年遭境外假訊息攻擊的冠軍，這代表中國大陸對臺灣認知作戰不曾間斷，[7] 一般民眾都可輕易感受到認知作戰的無所不在。以調查局於 2022 年間公布查獲之認知作戰案件為例：

### 案例一

經調查發現「朱○卉、丁○風……」等近 20 個假帳號，利用境外手機門號及電子郵件，在卡提諾論壇註冊後，頻繁發布有關疫情及政治相關爭議訊息，甚至利用網頁瀏覽器開發者模式，編輯竄改 PTT 既有的文章內容，藉由中國大陸、柬埔寨背景人士管理的「筷客有點兒甜」等數個臉書粉絲專頁，進行第一層散布，再利用「郝○茹、喬○雲、悅○汪、琬○曹……」等近 400 個臉書假帳號，進行第二層分享，廣泛散布到臺灣地方社團、宗教、生活娛樂等各類不特定公開臉書社群，由社群成員進行第三層之分享，以營造錯誤認知及挑起人民對立，嚴重危害臺灣社會秩序及國家安全。[8]

[7] 《假訊息攻擊台灣「連 9 年世界最多」　國防院抛 3 招抵抗中國認知戰》，EToday，2022 年 5 月 7 日，https://www.ettoday.net/news/20220507/2246138.htm。

[8] 《假帳號入侵卡提諾論壇！竄改 PTT 文章散布假訊息　調查局發動約談》，蘋果新聞網，2022 年 1 月 21 日，https://tw.appledaily.com/local/20220121/3EPD6MUNGRGVZE4WUOEXXUD6CQ/。


調查局查獲扭曲訊息散布流程。（圖片來源：法務部調查局，https://www.mjib.gov.tw/news/Details/1/756）

### 案例二

世界衛生組織秘書長譚德塞於2020年4月8日指控，臺灣政府及民眾對其進行言語誹謗攻擊，隨後出現大批以臺灣人代表的道歉文回應；經查是境外勢力蓄意操作，[9]目的在引發臺灣內部、臺灣與國際間的血鬨。

### 案例三

2022年11月九合一選舉期間，調查局更破獲「中華〇〇」及「兩岸頭條」等臉書粉絲專頁散布「日本爲「臺海突發狀況」預作撤僑準備，認臺灣將踩踏中共紅線」等不實訊息，該等粉絲專頁與位於中國大陸、香港之「大陸微視網絡科技江蘇有限公司」、「香港中華微視有限公司」及在臺灣設立之「中華〇〇股份有限公司」高度關聯，共同藉由社群平臺設放爭議內容且捏報不實訊息，企圖帶動社會輿論風向影響民眾認知。[10]

這些案例共同的特徵是都具有虛假訊息發送的源頭（中共），經由傳播的中繼單位（節點或意見領袖）對外傳播。

## 認知作戰的特性與防制

細究認知作戰的資訊傳播，不論是直接傳播或以各種方式掩飾，如偏離來源模式、利用對方內部勢力協力模式等，其傳

[9] 《查獲大量中國網軍假冒台灣網友道歉「攻訐譚德塞」調查局火速溯源！》，關鍵評論網媒體集團，2020年4月10日，https://www.inside.com.tw/article/19475-fake-post-apologize-who-tedros。

[10] 《調查局查獲中華〇〇公司收受大陸微視公司資金對臺進行認知作戰》，法務部調查局，2022年11月18日，https://www.mjib.gov.tw/news/Details/1/822。


世界衛生組織秘書長譚德塞在記者會上表示，遭受許多來自臺灣的羞辱與人身攻擊言論；隨後出現大批以臺灣人代表的道歉文回應，經查是境外勢力蓄意操作。（圖片來源：截自公視新聞網，https://youtu.be/BXogOmsqPj0；Samson Ellis twitter，https://twitter.com/samsonellis/status/1248451053634252800）

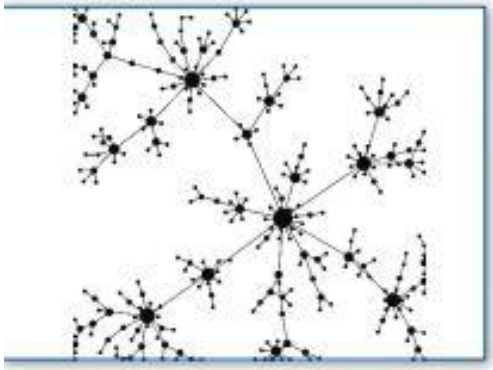


圖 1　社會網絡節點與聯繫

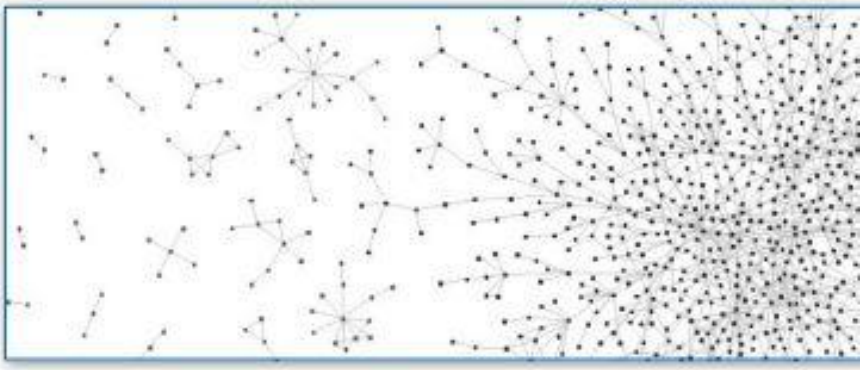


圖 2　疏密不同的社會網絡分布

Source: Martin Buoncristiani and Patricia Buoncristiani, "A Network Model of Knowledge Acquisition," 2017, https://www.researchgate.net/publication/255575571_A_Network_Model_of_Knowledge_Acquisition.

播方式都絕非大水漫灌，而必須經由特殊網絡完成，[11] 就如前述多個案例中顯示，都有特定發送訊息源頭與中繼點。

若將認知作戰理解為硬體與軟體兩個領域，則訊息的內容顯然屬於軟體，而傳送的路線或網絡則可視為硬體，「軟體」內容多變，目前我政府依惡、假、害為取締原則；而「硬體」是「軟體」傳播的管道，若能同時予以防制才顯效果。那麼訊息傳遞的「硬體」網絡到底又呈現何種態樣？據各方的研究顯示如圖 1。

不論是意見領袖的大黑節點，或是跟隨者的小點，社會上每個人都可以在此圖上找到相對應的位置。而整個社會網絡因疏密不同又呈現如圖 2 型態。

[11] Hartley III and Hobson, *Cognitive Superiority*, pp. 106, 149, table 5.8.


圖 3　俄羅斯之扭曲訊息製作散布的 4 個環節

更有趣的是，依據對俄羅斯認知作戰的假訊息組成與散發調查顯示，認知作戰包含 4 個環節：1. 扭曲訊息（dis-information）編寫；2. 哏圖（cartoon）；3. 假冒身分評論；4. 以眾多，尤其是看似女性帳號發送至所能接觸到的所有社交媒體上。[12]

扭曲訊息編寫，是負責則將真假訊息混合致難辨真假；哏圖目的在簡化事件讓受眾產生刻板印象，以影響國家的政治、經濟等政策；假身分評論，是以詮釋方式帶風向；假帳號在不斷推出相關訊息，而看來像女性的帳號更容易令人放鬆戒心獲得信任，擴大傳播效果。此 4 個環節的相互結合，也才能依據如圖 3 過程發揮認知作戰應有的效果。

依據此 4 個環節的分進合擊特性，以認知作戰防制角度看，顯然可將此 4 個環節視為發動認知作戰者的位置標定，對此 4 個環節阻斷或將此 4 個環節作為打擊對象，更將有利於提升反制認知作戰的效率。而認知作戰更具有如下特性：

一、群聚特性：同質性結成小群，意識形態相同者所獲知的訊息相似而強化其認知，難以接受不同觀點。

二、節點特性：小團體亦有意見領袖（節點）的存在，訊息由節點向下傳播。節點包含個人、特定網頁、網站、媒體……等等，而在社交媒體盛行的當前，「網紅」（influencer）更成為各方關注的新焦點。

三、媒介特性：溝通載具相同有利於傳播，因此兩岸同文同種、思維相同有利於傳播，依此脈絡在兩岸認知作戰的攻防中，拉幫結派建立在地協力團體不難想像。

四、不斷精進特性：運用人工智慧分析與鎖定特定目標，不斷餵給特定（假）新聞，讓其傳播，還可不斷檢查評估更換。

[12] David Patrikarakos, "Homo Digitalis Enters the Battle," in Clack and Johnson Eds., *The World Information War*, Routledge, pp. 35-36.

幾乎所有研究認知作戰者，都認為認知作戰的核心是信任（trust），只有獲得信任才足以發揮影響力（Trust is central and offers a target of influence），[13]因此，在認知作戰攻防中，不僅要受眾可以聽懂、看懂攻擊方的訊息，更完全信任其所言，才有具體效果。換言之，**若以不斷地即時澄清還擊認知作戰的攻擊，並教育全民或自我砥礪提高媒體辨識能力**，不斷公布散布假訊息的意見領袖（節點），使其信用破產，**則其傳播假訊息進行認知作戰的能力就將大幅下降**。在意見領袖信用破產後，跟隨個體可能轉而跟隨其他意識形態相若的意見領袖，反制者依前述方法再度破解，對於認知作戰的防制顯然將大有助益。

## 瞭解認知作戰傳播模式，才是捍衛家園安全的最大力量

認知作戰無煙硝味，更無平戰之分，隨時隨地都在進行，且敵我雙方都具有類似的訊息傳播網絡，終日進行著激烈攻防。

在防制敵方攻擊上，不僅要隨時闢謠以真實狀況攻破對方傳播假訊息意見領袖節點的信用，讓對方無法再進行假訊息的傳播，並輔以如國安、社會秩序維護、防疫、食安……等法規的制裁，摧毀敵方的訊息傳播中繼點，更要在己方進行真實訊息的傳播，讓己方的意見領袖傳播對我有利的真實訊息，以壯大我方的力量，使友我者更友我，而敵我者不敵我。

因此，認知作戰絕不是僅守不攻，而是攻守兼備，攻守之最大力量卻是來自全民對認知作戰傳播模式的理解，並由政府支援以迅速真實的訊息，在友我陣營傳播強化心防，更將其擴散至敵方訊息網絡，揭露敵方陣營的虛假，方能達成全民防制認知作戰，以維護家園安全的目的。


若不斷地即時澄清認知作戰的攻擊，並教育全民提高媒體辨識能力，則傳播假訊息進行認知作戰的能力就將大幅下降；圖為行政院澄清假訊息的圖文資料。（圖片來源：行政院粉絲專頁，https://zh-tw.facebook.com/photo/?fbid=573130084859000）

[13] Hartley III and Hobson, *Cognitive Superiority*, p. 43.



本文摘自清流雙月刊**中華民國112年3月** 號P27-P33

# 武功極界-無影手 VS 麥擱騙啦-有影沒

社團法人台灣E化資安分析管理協會、逢甲大學資訊工程系　李榮三主任/教授


◆ 社團法人台灣 E 化資安分析管理協會、逢甲大學資訊工程系 — 李榮三主任／教授

由臺灣警政署與美國網路犯罪投訴中心（Internet Crime Complaint Center, IC3）統計的網路犯罪資訊，可發現近年來國內外的網路攻擊、詐騙等犯罪事件數量居高不下。

據臺灣警政署統計，自 2017 至 2021 年間，平均 1 年發生 1 萬 3 千例以上。雖近年來的犯罪統計稍有下降趨勢，但受害者仍成千論萬。況且，這些統計數量僅計算已通報的案件，未通報的案件更是不計其數。美國則更甚，IC3 的報告中指出每年平均有 55 萬例，且數量有顯著提升，2017 至 2021 年的通報案數量已暴增 2.8 倍。甚至網路犯罪受害者損失的金額平均每年高達 370 億美金，由此可見，網路犯罪所帶來的威脅不可估量。其中，最常見的手法即為「網路釣魚攻擊」。網路釣魚如同真實世界釣魚，釣客即為隱匿於網路背後的駭客，常見的公務通訊軟體、社群媒體等則是作為駭客的釣場，駭客透過散播魚餌誘使民眾點擊上鉤。


藝人周杰倫於 2022 年 4 月 1 日當天在 Instagram 上發文，表示自己無聊猿 NFT 被網路釣魚偷走，起初還以為是愚人節玩笑，「結果一去查看，真的沒了」。（圖片來源：周杰倫 IG，https://www.instagram.com/jaychou/；Ghost.R.C，https://flic.kr/p/qAWP1a）

參考 Medium 中 Tyler Chen 所提出的電子郵件範例與社群軟體上的詐騙實例，一旦民眾點擊其中所夾帶的鏈結、下載檔案或是開啟指定程式，便等同於上鉤，駭客成功竊取使用者個人資料、帳號密碼與信用卡號等。

## 個人案例與防範策略

接著，我們進行個人與企業的受害案例分析，並且說明防範策略。

### 一、周杰倫無聊猿 NFT 被偷損失上百萬

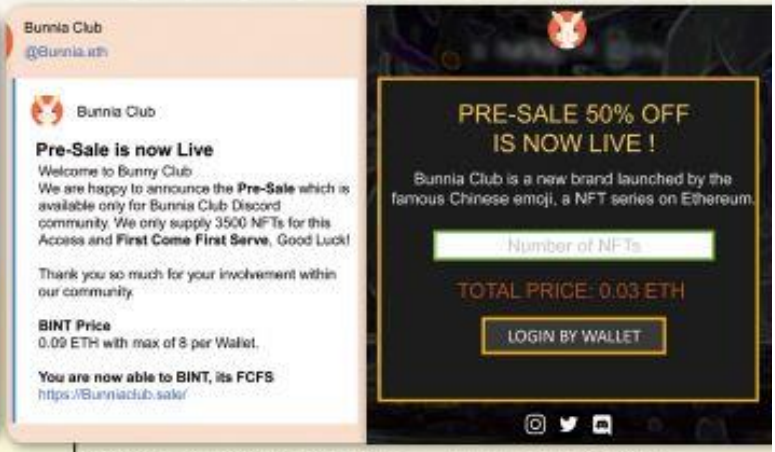
2022 年 4 月，明星周杰倫在社群網站公布其「無聊猿」非同質化代幣（Non-fungible Token, NTF）被釣魚網站偷走的消息。所謂「無聊猿」是由無聊猿遊艇俱樂部（Bored Ape Yacht Club, BAYC）推出的 1 萬隻各有獨特表情的猿猴 NFT 作品，當時每隻價格約在 100 枚以太幣（約 26 萬美金）。

這類事件的起因就是駭客在官方社群網站放上釣魚網址來誘騙被害人。使用者在社群媒體上看見 NFT 的預購訊息，以為可以用較便宜的方式來購買新的 NFT；誘使使用者點擊鏈結後會進入釣魚網站，便可選擇金額開始進行交易手續。然而釣魚網站的交易內容並非預購 NFT 作品，實際上是受害者被鏈結的文章所吸引，毫無警覺內容的真偽，導致駭客成功騙取授權交易。

### 二、FB Messenger 點擊網址詐騙達高峰

亦有受害者 2020 年在 Messenger 收到名為「我不敢相信是你」的假 YouTube 影片鏈結，想觀看者必須先輸入 Facebook 帳號密碼，一旦使用者於假網站中登入，駭客便成功盜用使用者帳號密碼，隨後再將


無聊猿遊艇俱樂部推出 1 萬隻各有獨特表情的猿猴 NFT 作品。（Photo Credit: Bored Ape Yacht Club, https://boredapeyachtclub.com/#/gallery）




駭客透過官方推特私訊被害人（左），放上釣魚網址誘騙被害人點選購買商品（右）。（圖片來源：作者提供）

鏈結散播給該帳號的好友，讓被害人淪為散播惡意鏈結的工具。根據國外資安廠商 Pixm 發布的最新研究報告，**推估全球臉書至少有數百萬位用戶遭誘騙導致個資外洩**。

## 三、個人防範策略

在網路資訊發達的年代，駭客偽裝成一般使用者來散播惡意鏈結進行釣魚已是常態，因此資安意識對於民眾而言已是必修課題之一。防範作為有：

（一）**提升潛在威脅警覺性**：當收到陌生訊息、開啟未知網址、下載非官方軟體時，人們其實難以辨別其中是否夾帶惡意行為或攻擊，應提高警覺性，避免落入駭客陷阱。

（二）**陌生訊息**：當使用者瀏覽社群媒體上陌生人所發布的訊息時，應時刻保持懷疑的態度，在進入網址前要先查證訊息的正確性。如 NFT 遭盜取事件中，在社群網站看到 NFT 鏈結時，**應先去向官方求證**，而不是相信社群網站的訊息。只要使用者對內容產生懷疑並查證，就可以有效避免釣魚事件發生。


FB Messenger 曾遭駭客利用傳送假訊息，誘騙使用者登入釣魚網站，藉此竊取個資。（圖片來源：作者提供）


圖 1　一般使用者遇到的網路釣魚情況

（三）未知網址：收到朋友傳遞的未知網址時，使用者**應先確定該消息為本人傳遞，才點擊鏈結**。如案例 FB Messenger 點擊網址詐騙中，使用者在收到可疑鏈結後，可透過打電話的方式來確認朋友身分的真偽，避免朋友的個人帳號遭到駭客利用而不自知。

（四）使用威脅檢測軟體：使用檢測軟體可以有效偵測惡意鏈結和惡意程式，大幅降低使用者被釣魚的風險。當使用者遇到必須點擊陌生鏈結或執行來歷不明檔案的情況時，可以利用 Virustotal 檢測軟體，使用者將鏈結或檔案上傳後，該軟體會自動偵測其是否被資安廠商認證為惡意鏈結或檔案，並產出相應的報告。使用者可自行評估該檔案所伴隨的風險。基於安全考量，倘若有任一廠商對該鏈結報有疑慮，建議使用者不要點擊。

## 企業事件與防範策略

有別於個人案例，駭客對於企業的攻擊更具威脅性，其會針對企業的特色、員工的素質、工作內容進行釣魚郵件的客製化，進而達成各種攻擊目的。這種持續針對特定組織發起的網路攻擊我們稱之為進階持續性滲透攻擊（Advanced Persistent Threat, APT），以下為 APT 案例發生的過程。

### 一、SolarWinds 網路監控軟體公司遭駭客入侵

SolarWinds 開發的軟體 Orion 主要是幫企業進行網路監控及管理。**2020 年 12 月傳出 Orion 遭到駭客入侵的消息，其嚴重性不只影響 SolarWinds 本身，連透過該軟體進行網路管理的企業都深受其害。比較知名的包括美國國務院、國防部、司法部及 NVIDIA、Microsoft 與 Intel 等國際企業皆傳出災情。**只要使用該軟體，駭客就能一舉獲得該組織的網路架構，並且遠端執行惡意程式碼進行攻擊。


圖 2　SolarWinds 軟體遭駭散布流程

這次事件 SolarWinds 企業本身並不是駭客的主要目標，而是與其合作的相關企業。駭客首先透過社交工程手段入侵 SolarWinds 後，並沒有急於進行攻擊，而是持續蒐集資料，第二階段目標就是將惡意程式混入 Orion 軟體中且不被發現，在最終階段經由各企業下載，將帶有惡意程式的軟體散布出去。

根據上述實例可發現，駭客主要是透過釣魚郵件來進行攻擊，因現今企業仍然以電子郵件為主流的通訊方式，其不限時間地點的特性便於員工使用。然而企業中每天需要處理的郵件數量非常多且種類繁雜，一不小心便讓駭客有機可乘，其中最常見的郵件設計內容為商業電郵詐騙（Business Email Compromise, BEC）。

## 二、BEC 釣魚郵件實例

根據 2022 年臺灣資安公司對 BEC 郵件進行的分析，得出一些常見案例，駭客經常使用像“office”、“president”、“chief”、“director”等高階職務名稱作為電子郵件帳號，透過偽造身分，來向員工索要機密檔案。或是會偽造一個與被冒充人非常相似的地址，包括將某些英文字母和數字互換以達到混淆的目的，像是英文 l（小寫 L）與數字 1（數字一）、英文


圖 3　真實與混淆的郵件地址

o 與數字 0 等，讓受害者難以在第一時間辨認出真偽。因此，使用者收到信件時，應多留意信件的來源地址是否正常，若有異常之處即可通報或忽略該信件。

## 三、現今企業的防範措施

整體來說，釣魚郵件的設計類型千變萬化，只要謹慎檢查寄件方的電子郵件與檔案就可以有效避免。當你在郵件中看到檔案，可以先確認是否為圖片偽裝、檢查寄件人電子郵件地址是否完全正確等等，千萬不要忽略這些重要步驟。

但企業中每天需要處理的郵件數量極多，單靠員工本身的資安意識來抵擋所有的釣魚郵件有點不切實際，倘若能實現沙盒測試與零信任架構，必定能有效抵抗威脅。因此以下分別介紹沙盒測試及零信任架構這兩種現今企業可用的防範措施。

（一）沙盒測試：BEC 商業詐騙之所以難以抵擋，是因為很難斷定該郵件檔案是好是壞，依目前技術來說，最有效的方式就是進行沙盒測試。通過將環境徹底隔離，模擬檔案執行的情況，並觀察這些程式會做哪些動作？連到哪些網站？安裝哪些程式？做一個詳細完整的分析紀錄並上傳至監控中心。雖然執行過程要一段時間，但只要取得該惡意程式


圖 4　沙盒測試示意圖

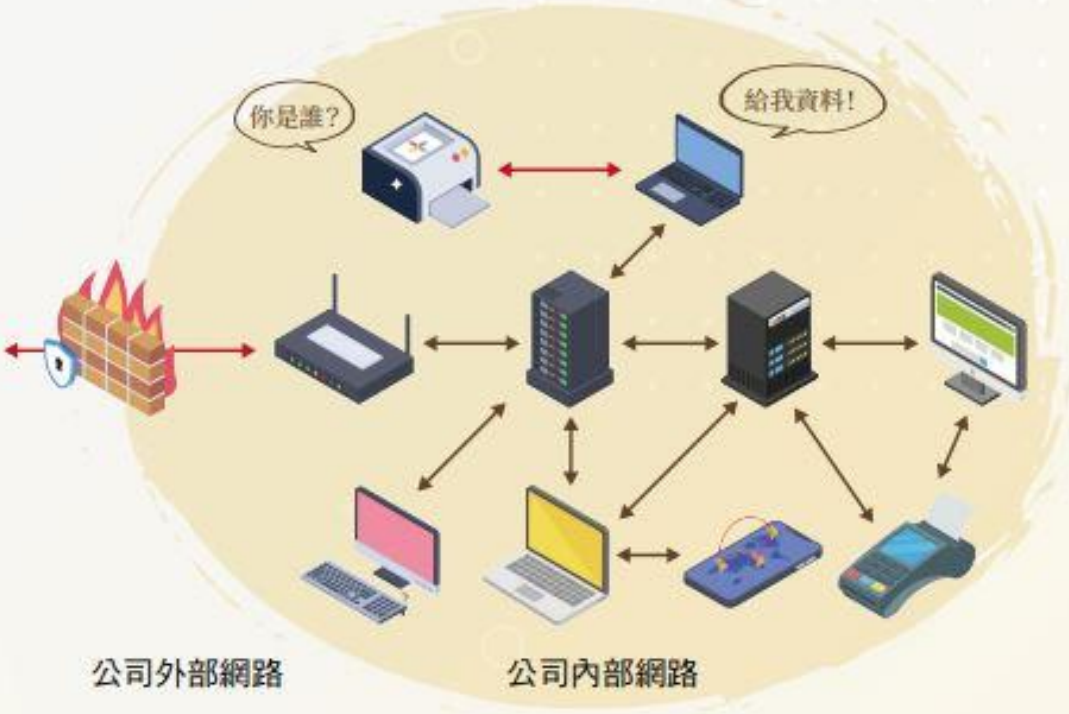



圖 5　零信任架構示意圖

的特徵後，之後檔案只要進行比對就可以確認是否為惡意程式，不必再模擬一次。透過這種方式，可以很好且有效率的分辨出惡意檔案。

（二）零信任架構：於此架構下，不論進行任何操作都需要進行身分驗證，以抵擋駭客入侵後所造成的威脅。基於對各種流量頻繁的驗證，儘管駭客入侵員工的電腦，也難以繞過員工的身分驗證系統進行進一步的攻擊，因此零信任架構是近幾年資安持續推動的方向。例如美國聯邦政府在頻繁遭受攻擊後，於 2021 年 9 月 7 日公布《聯邦零信任戰略草案》（Federal Zero Trust Strategy），目標是讓企業組織的網路安全架構，都是基於零信任原則而成。

## 結語

無論是一般民眾或是政府企業，都會收到來自駭客的釣魚攻擊，手法層出不窮且越加高明。除了依靠系統提供的自動防禦偵測機制外，全民應提升對於釣魚訊息的警覺性以及基本認知，才能計出萬全，去危就安。

社團法人台灣 E 化資安分析管理協會（ESAM）



本文摘自清流雙月刊中華民國112年3月 號P53-P59