螞蟻搬家的風險啟示錄－阿桂觀天下，立於不敗之地

臺灣警察專科校前校長－陳連禎

清流 MJIB

螞蟻搬家的風險啟示錄—阿桂觀天地，立於不敗之地

◆ 臺灣警察專科學校前校長 — 陳連禎

古人仰觀天象、俯察大地，表面上不動聲色，實則偵知天地間的細微變化，進而採取相應的預防措施，以立於不敗之地。

大自然的預警，眾人經常視而不見

「月暈而風，礎潤而雨」，眾所皆知，但一般人通常視而不見。然而，萬事萬物發生變化前，大自然都會出現徵兆警示。仔細的人若用心觀察周邊動態，常常會發現其中隱藏細微而異常的先兆；如果進而及時採取相應的預防措施，就能趨吉避凶。自古以來明智的大將軍帶兵作戰，深知兵

清乾隆平定兩金川得勝圖之《勒烏圍賊舊官寨》，描繪阿桂攻克金川土司索諾木官寨情形。

凶戰危，因此「靜以幽，正以治」的運籌帷幄，表面上不動聲色，實則偵知天地間的細微變化，能適時化解危機。

清朝大小金川，地處偏僻動盪不斷

清朝乾隆皇帝好大喜功，南北外患反覆四起，大舉出兵，勞民傷財，雖勝而得不償失。其中位處偏僻的四川大、小金川國度，更是一反再反，令清廷非常頭痛。

大、小金川本是大清帝國的版圖，自古以來雖僅表面名義歸順中央，然其等只要按時履行納貢義務，其餘事情清廷多會睜一隻眼閉一隻眼。而大、小金川之所以會招惹清朝不斷用兵，固然是乾隆帝的主張，然根本原因還是大金川欲兼併小金川引爆內鬨所導致。

其實大、小金川本來就不適用中原的郡縣行政制，其自成體系，由當地土司自

行負責。不過，土司的政治權力猶如土皇帝，久而久之，當地人就只知有土司而不知有皇帝；土司們更自恃天高皇帝遠，日益猖狂而為所欲為，甚至自相殘殺，目無大清帝國國法。

亂世出英雄，清朝十大名臣阿桂現身

乾隆 36 年（公元 1771 年），西南方大、小金川之亂又起，大家束手無策。此時長期戍守西北邊疆的章佳 · 阿桂橫空現身，滿清貴族出身的他，年輕時就以好學備受矚目。當時他奉命參加剿平大、小金川之亂，前後歷時 5 年，期間運籌帷幄、有勇有謀，親自參戰不計其數，大家公認他是平定大、小金川之亂的首功人物。阿桂不僅驍勇善戰、廣博的知識更讓他深得部屬的敬愛。

阿桂驍勇善戰，為清廷平定許多戰亂，受乾隆封爵為一等誠謀英勇公。

將軍下令臨時移防，眾人怨聲載道

有一天傍晚，軍隊經過一番長途跋涉，已安置好營地準備休息。忽然傳來大將軍阿桂的命令，要求立刻拔營而轉移陣地。諸將軍都大惑不解，很不願移防駐地，於是紛紛求見阿桂，方得知並無戰事威脅又無危安預警情資，為何要轉移陣地呢？此際部隊行軍一整天，大家都非常疲憊，實在需要好好休息一陣子，更何況現在天色已晚、視線不佳，大軍臨時移防確有諸多不便。

阿桂大將軍見眾將軍視若無睹、不聽命令，不禁動怒，於是發出令箭，下令說：「立刻遷營，轉移陣地；立即行動，違令者立斬！」眾將軍無可奈何，只能服從軍令，立即回營執行移地命令，全軍上下怨聲載道。大家辛苦忙了一陣，終於找到一處向陽高地的新營區，而且擁有制高點的優勢。

阿桂命令移防引起眾人不滿，未料，眾人因此躲過一劫。

了解天文地理也是將領必備能力。

螞蟻搬家，強降雨將臨徵兆

這個新營地是大將軍阿桂尋覓後指定的，等大家睡到半夜，忽然變天而下起強降雨，頃刻之間，大地瞬間變成一片汪洋，而原來駐紮的營地早已被積水淹沒、不見蹤影。現在的駐地營區則因為地勢高陡，在暴風驟起的滂沱大雨肆虐下仍舊安然無恙。

雨過天青，將軍們欣喜躲過一劫，群起去謝阿桂，問道：「您怎麼會知道老天爺要下這場大雨呢？難道您懂得占卜術嗎？」阿桂笑著說：「我哪會什麼奇門遁甲，只不過我昨天晚上看到很多螞蟻在地上成群移動蟻穴，因而我知道地氣很熱，勢必將會有大雨來臨。這只是基本的天文常識而已。一個帶兵作戰的將領，不僅要懂得部署戰陣，而且也要了解天文地理，這樣才能立於不敗之地。」

觀天象察大地，方能趨吉避凶

下雨前的天象有徵兆，地理也會有徵候，前者如烏雲密布、燕子低飛，後者如螞蟻大舉搬家、蚯蚓爬出地面……古人知識取法自然，仰觀天象、俯察大地，即是探討大自然的奧祕，進而找出異常軌跡，由此得以辨識人身安危的風險因子。

至於地形相關知識的認知運用，如何趨吉避凶的判斷功夫，更是指揮官必備的常識。《孫子兵法》〈地形篇〉羅列了6種地形，孫子強調：「凡此六者，地之道也，將之至任，不可不察也。」*在〈九地篇〉也詳列了9種地形，反覆叮嚀地形對於軍隊進退安危的影響力。

孫子以為：「九地之變，屈伸之利，人情之理，不可不察也。」換句話說，孫子重視地形地勢，隨時要觀測周遭環境的轉變，進而判讀地形之利或不利，及時採取因應作為，這都是將帥必須扛起的重責大任。孫子警告指揮官在外行軍「必謹察之」，不是沒有深意。

知天知地，勝乃可全

兵書《六韜》闡明為將者身邊要有股肱羽翼，包括天文、地利、謀士、術士、腹心、耳目等各數人，以供驅策。而阿桂家學淵源，兵書唾手可得研讀，他自小勤學好問，加上細心觀察地形地物的好習慣，帶兵早已熟諳「地形者兵之助」的道理。無怪乎，阿桂能平定清朝最難搞的大、小金川之亂，厥功甚偉，出將入相，大受朝野稱道。

行軍作戰中，「知彼知己」本就不易，阿桂隨時觀察異常現象，保全了三軍免於災變之難，做到了孫子為將的最高境界「知天知地，勝乃可全」。

* 孫子將戰爭中經常遇到的地形分為6種：通、掛、支、隘、險、遠，並根據地形研究提出相應的戰術原則。「我們可以去，敵人可以來的地方叫做通。可以前進，不易返回的地方叫做掛。凡是我出擊不利，敵出擊也不利的地方，叫做支。在隘形地，若我先占據，就要用重兵堵塞隘口，等待敵人來攻；如果敵軍已先占據，那就不要進擊。在險形地，如果敵人已先占領，那就主動撤退，不要進攻它。在遠形地，雙方勢均力敵，不宜挑戰，勉強求戰，於我不利」。https://www.arteducation.com.tw/guwen/bookv_48.html。

本文摘自清流雙月刊中華民國111年11月 號P62-P66

如何降低CI遭網路攻擊的衝擊

華梵大學特聘教授－朱惠中

◆ 華梵大學特聘教授 — 朱惠中

以水領域為例，早期攻擊者只針對某家自來水公司，但現在因多個公共事業公司都擁有相似軟體系統，若未做好資安防護，則可能導致連鎖攻擊事件發生。

OT 與 IT 融合後之工作重點

隨著網際網路普及，使得營運技術（Operation Technology, OT）場域與資訊技術（Information Technology, IT）場域之間的界線越來越模糊，造成 IT 場域的資安風險，蔓延到 OT 場域。此一現象已使得關鍵基礎設施（Critical Infrastructure，下稱 CI，例如能源、金融、交通等）所在的網路環境頻遭網路攻擊，進而破壞工業控制系統（Industrial Control System, ICS），或是監控與資料擷取系統（Supervisory Control And Data Acquisition, SCADA）的正常運作，故網路環境的安全性是 OT/ICS 防護的重點。

組織資安長（Chief Information Security Officer, CISO）的首要工作即在強化 OT 與 IT 融合後的網路安全，以降低組織 OT/ICS 環境遭網路攻擊的衝擊。經綜整國外（美國、英國與加拿大）多位具實務經驗專家的意見後，歸納出資安長的工作重點如下，提供相關作業人員參考。[1]

一 利用縱深防禦的方法來規劃 ICS 安全。

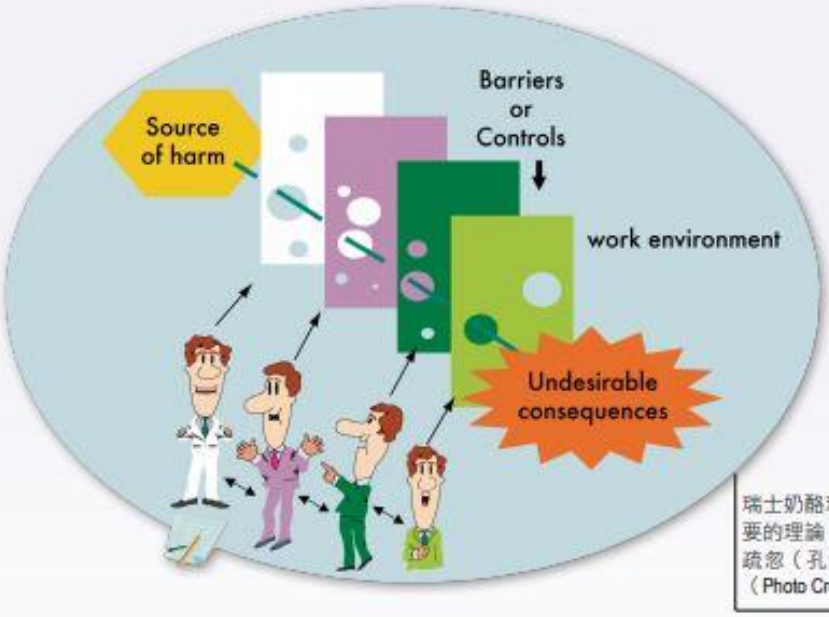
二 盤點影響 ICS 安全的關鍵項目。

三 身分識別、盤點資產及事件應變與復原。

四 降低攻擊途徑之數量。

五 控制與監視整體網路流量。

[1] "Pas: Lessons Learned: Protecting Critical Infrastructure From Cyber Attacks", https://mightyguides.com/pas-lessons-learned-protecting-critical-infrastructure-from-cyber-attacks.



瑞士奶酪理論（Swiss Cheese Model）是一個簡單但重要的理論，只要增加防護的層數（乳酪層數）、減少疏忽（孔洞）的發生，就能降低意外產生的機率。（Photo Credit: TGOWERJONES, https://w.wiki/5pMk）

利用縱深防禦來規劃 ICS 安全

為保護 CI 安全，首要工作為採用縱深防禦策略（Defense in Depth）來建置多層次的防禦機制。瑞士奶酪理論（Swiss Cheese Model）是一個簡單控制風險的重要理論，利用增加防護的層數（乳酪層數）及減少疏忽（孔洞）的發生，就能提高意外事件被阻擋下來的機率。控制系統通常需要多個組件一起工作才能執行功能，該控制系統中的每個設備都可能對整個系統功能產生至關重要的安全影響，特別是當網路系統組態改變時，都會採取 NIST CSF 資安架構為依據，[2] 以避免「步步錯，最後引發不幸」的例子，因為**只要任何一個環節做對，錯誤事件就不會發生。**

根據上述理論，美國紐澤西州 Public Service Enterprise Group（PSEG）公司經理 James Shank 建議可採取下列步驟，以降低網路被攻擊時所產生的衝擊：

一、檢視 OT 網路與 IT 網路的連接—特別是當允許資訊能雙向流通時，一定需要仔細評估輸入和輸出數據，以及瞭解環境中所有 ICS 設備配置及其通訊協議。

二、控制與 ICS 網路連接的所有可攜式媒體和設備—這項技術在 OT 網路上尤其重要，因為 OT 網路很少具有拒絕使用者存取個人媒體設備（如 USB）的能力。

[2] 即美國國家標準與技術研究所（National Institute of Standards and Technology）提出的網路安全框架（Cybersecurity Framework），為現今各機關組織所參考之資安架構，其以 Identify、Protect、Detect、Respond、Recover 等五個要件為基礎（即識別、保護、檢測、回應和恢復），https://www.nist.gov/cyberframework/online-learning/five-functions。

三、多層次防禦與威脅情資結合—將二者結合，將能強化監控功能，並可持續優化潛在攻擊的防禦能力。

盤點影響 ICS 安全的關鍵項目

美國 Exelon 公司網路安全顧問 Scott Saunders 認為，影響 ICS 安全的項目，在於知道自己擁有什麼、知道自己想做什麼與在做什麼，故需盤點影響 ICS 安全的關鍵項目，其核心工作如下：

一、瞭解 OT 與 IT 網路及其系統、可使用元件以及如何管理基準配置。

二、考慮如何存取 OT 與 IT 網路上的遠端設備。

三、務必瞭解存取設備之控制方式，例如使用者如何遙控及操作設備。因很多 ICS 都是自動化，現場甚至沒有操作員，故必須準確地瞭解這些設備如何被存取，以及由誰來操作這些設備。

四、要特別注意評估舊有設備的安全指標。儘管許多工廠已是自動化，但其中仍可能存在一些舊機電混和系統是不能自動化的，故須提醒操作員注意某些警報；當訊號出現，代表現場可能發生異常情況，亦表示可能面臨安全威脅。

五、確保舊有設備及系統的知識未存有技術落差（Technical Gap）。

身分識別、盤點資產及事件應變與復原

英國 Shell 公司工程師 Robin Familara 認為，雖然許多 ICS 已現代化，但仍有許多老舊設備和系統無法直接與程序控制域連接，這些設備系統將會是系統弱點。

由於 OT 網路很少擁有拒絕 USB 存取的能力，所以控制與 ICS 連接的所有可攜性媒體和設備格外重要。

現今已有許多自動化工業控制系統，必須準確地瞭解這些設備如何被存取，以及由誰來操作。

Familara 建議可採取以下步驟，以降低 ICS 受網路攻擊之衝擊：

一、確保正確的身分識別—使用者的身分識別與管理是第一步工作，不論是區域網路或是廣域網路，身分識別與管理都必須有適當保護。

二、定期更新組織的資產清單—組織資產清單蒐集過程須可利用手動及遠端蒐集方式進行，以達成資產清單為最新版本與完整之要求。

三、確保組織在遭受攻擊後能落實緊急應變處置—亦即需建立事件應變與復原之機制與能力。此項工作透過蒐集網路的事件日誌、系統日誌及緊急應變處置（Incident Response）等數據方可達成。

Familara 建議應定期更新組織的資產清單，並可透過手動及遠端蒐集方式進行，以達成最新與最完整版本之要求。

降低攻擊途徑的數量

所謂攻擊途徑（Attack Vector）是駭客用來攻擊系統漏洞的管道，包括人為因素、電子郵件附件、網頁、彈出視窗、即時訊息與聊天室等；其攻擊的方式，不外乎透過 virus、worm、Trojan horse 或是 port scan、sniffing 等來進行。

所謂攻擊面（Attack Surface）是指，未經授權的使用者（攻擊者）可以嘗試向目標網路輸入數據或從目標網路中存取數據等各種不同途徑（Attack Vector）的總成，且由於網路技術蓬勃發展，相關新系統又非常依賴網路，因此造成了一個可擴大的攻擊面。

以水領域為例，早期攻擊者可能只會針對自來水公司的計費系統，但現在則可透過遠端操作攻擊不同面向的系統，且一旦多個公用事業公司擁有相似的軟體管理系統，則可能導致供應鏈攻擊連鎖效應。

根據加拿大 SaskEnergy 公司分析師的經驗，建議可採以下步驟來降低攻擊途徑之數量：

一、應用程序白名單（Application Whitelisting, AWL）[3]—AWL 僅允許執行受信任的已知文件，定期審核以識別未經授權的存取，另可檢測並阻止惡意軟體執行。

[3] AWL 是一種端點上應用程式安全策略，預設拒絕其他所有程序，只允許經過驗證和授權允許的應用程式在端點上執行。而傳統黑名單是列出已知惡意檔案，並阻止它們執行。比起黑名單，AWL 不需要跟上不斷變化的惡意入侵，取而代之的是維護已被核可的（有限）應用程式。https://www.fineart-tech.com/index.php/ch/news/126-zerotrust/725-fineartsecurity-endpntzerotrust。

所謂攻擊途徑（Attack Vector）是駭客用來攻擊系統漏洞的管道，包括人為因素、電子郵件附件、網頁、彈出視窗、即時訊息與聊天室等。

二、適當的組態與修補管理—此程序將可減少駭客的攻擊面，並有助於使控制系統更安全，為達此目的，必須擁有完整的資產清冊及蒐集所有關鍵資產（critical asset）的配置，此亦是調查風險緩解活動並確定其優先等級的必要步驟。

三、分析及找出潛在的攻擊—沒有人能做到天衣無縫，因為 OT 與 IT 網路永遠都會有新弱點被發現。其具體作法如次：

1. 將 ICS 網路與任何不受信任的網路（尤其是 Internet）隔離。

2. 鎖定所有未使用的埠（Ports），並關閉所有未使用的服務。因內部與外部網路的連通性增加，故網路進行分段變成非常重要，特別是將其分成多個邏輯區域並限制主機通信（host-to-communications）的路徑，同時另需設置防火牆和入侵檢測系統，才能降低或阻絕在網路邊界遭到破壞時可能遇到的損害。

Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy

美國國家安全暨通訊整合中心（NCCIC）曾針對 ICS 之保護提出 7 項策略，其中，應用程序白名單機制的策略占比為第一，顯示其對惡意攻擊的有效阻擋力。（Source: Cybersecurity and Infrastructure Security Agency, https://reurl.cc/2mpEvn）

控制和監視網路流量是提高 ICS 安全性的關鍵，最終目標是形塑出「集中式即時掌控組織資訊安全狀態單位」（Security Operation Center）的服務。

控制與監視整體網路流量

最後，從戰略角度來看，美國新墨西哥州 PNM Resources 公司安全主管 Spencer Wilcox 認為控制和監視網路流量是提高 ICS 安全性的關鍵：我們需要掌控資產以及網路中正在發生變化的資訊。通過可見性，將能夠看到系統詳細資訊、所有進出流量、所有節點及其補丁程序級別，以及正在發生的通訊類型，最終目標是形塑類似 Security Operation Center（SOC，集中式即時掌控組織資訊安全狀態的單位）的服務。Wilcox 建議可採取以下措施，來使網路環境更加安全：

一、策略上不能僅依賴設備來控制和監視網路流量，而是要對網路流量進行絕對控制—一般而言，不論 TCP/IP 或傳統的 Modbus、DNP3 等通訊協議都無法支援網路流量之可視性，故 Wilcox 建議不要使用虛擬私有網路（VPN），而是引導用戶通過跳轉服務器（Jump Server）進行操作，因跳轉服務器對遠端存取活動會進行監視，故管理者可以知道誰在執行這些操作及起源。

二、儘可能限制遠端存取—由於大部分供應商都希望擁有遠端存取權限以支持其服務及產品，所以全面禁止遠端存取是個理想但卻難以落實的策略。

結語

CISO 處理網路安全原則，可歸納為以下五點：

一、「安全」為最優先考量項目。

二、「安全認知」是 ICS 網路安全的關鍵。

三、OT 網路必須有標準的操作程序。

四、OT 安全植基於關鍵安全組件的技術標準（ISO/IEC 62443）。

五、CI 之數位資產需有安全保護策略。

本文摘自清流雙月刊中華民國111年11月 號P11-P16