生物病原攻擊攸關國家安全+知識小學堂

美國加州大學柏克萊分校生物化學博士／陳淵銓

生物病原攸關國家興亡及戰爭成敗

生物病原是指任何可以引發疾病的病原體，亦可稱為傳染原，通常用於描述「傳染性」的動物、微生物或媒介，如細菌（病原菌）、病毒、真菌、原生動物、線蟲、寄生蟲、類病毒（viroid）及感染性蛋白質（prion）等。生物病原可以引發人類疾病，綜觀古今中外歷史，可以得知生物病原一直與國家興亡、戰爭成敗有密切的關係。舉例如下：

一、赤壁之戰成敗—不在「戰」在於「疫」

西元 208 年，東漢末年孫權與劉備聯軍在長江赤壁擊敗曹操大軍，是中國歷史上以少勝多、以弱勝強的著名戰役之一。歷史教科書雖記載曹操失敗是因為遭遇火攻，但《三國志》亦曾記載赤壁之戰有疾病侵襲，所以認為曹操失敗的主要原因並不是被火攻擊潰，而是遭遇大規模瘟疫（可能是血吸蟲病）感染而造成的嚴重死傷，亦即在雙方交戰之前，原攻勢凌厲的曹軍卻染上了「疾疫」致戰鬥力大減。赤壁之戰澈底改變中國的歷史進程，曹操錯失了一統天下的機會，三國鼎立的局面正式確立。

《三國志》曾記載赤壁之戰有疾病侵襲，所以認為曹操失敗的主因並非源於火攻襲擊，而是遭遇大規模瘟疫導致部隊嚴重死傷。

1918 至 1920 年西班牙流感爆發，導致全世界有數千萬乃至上億人喪命，間接促成了第一次世界大戰提前結束。

二、東羅馬帝國的中興失敗—源自鼠疫大流行

西元 476 年，西羅馬帝國滅亡，但東羅馬帝國皇帝仍然自認為是整個羅馬帝國的皇帝，希望重建羅馬帝國昔日的輝煌，尤其是查士丁尼一世一登基就實行多項改革，使東羅馬帝國成為地中海世界最繁榮和強大的國家。正當帝國處於巔峰之際，「查士丁尼瘟疫」（世界上第一次鼠疫大流行）破壞了帝國中興的進程，據說此疫情奪去了幾千萬人的性命，佔整個帝國人數的 25%。人口的大量損失及財政危機使得帝國在波斯戰爭中一敗塗地，隨後而來的是帝國勢力範圍急劇萎縮，東羅馬帝國的中興大業澈底失敗。

三、大瘟疫導致明朝滅亡

西元 1644 年，明朝末年闖王李自成率大軍抵達北京城的最後一道天險—居庸關，但李自成所面對的北京，實際已是一

座遭疫病蹂躪的鬼城。這場大瘟疫（包括鼠疫、傷寒、霍亂）早在城破的前一年在全國各地及北京大流行，當時的地方志上都有「瘟疫，人死大半，互相殺食」的記載。因此，有人認為闖王李自成為首的流寇之亂，只是壓垮駱駝的最後一根稻草而已，否則北京城牆高大堅固，御林軍強悍，連強大的蒙古軍都攻不下來，怎麼可能讓流寇如此輕易地進城。因此，瘟疫大流行使得軍民大量死亡、朝廷財政困難才是造成明朝滅亡的主因。

四、西班牙流感促成世界大戰提前結束

西元 1918 年，流感大流行（1918 flu pandemic）從法國散播到西班牙，故亦稱為西班牙流感（Spanish flu），於 1918 年 1 月至 1920 年 12 月間爆發，造成當時世界約 5 億人受到感染，導致數千萬甚至上億人喪命。當時第一次世界大戰主要參戰國（德國、英國、法國和美國等）許多軍人因感染流感致士氣低落或失去戰鬥力，由於大量 20 歲左右的青壯人口死傷，各參戰國缺乏補充兵源投入戰鬥，間接促成了第一次世界大戰提前結束。

生物病原攻擊影響國家安全

世界衛生組織（WHO）自 2009 年起，發布的 6 次國際關注的公共衛生緊急事件（Public Health Emergency of International Concern, PHEIC）均為病毒攻擊事件（包括 2009 年流感病毒 H1N1、2014 年小兒麻痺病毒、2014 年西非伊波拉病毒、2016 茲卡病毒、2018 剛果伊波拉病毒及 2019 年新冠肺炎病毒）。其中冠狀病毒（SARS-CoV-2）引發的新冠肺炎（COVID-19），由於迄無正式獲得核准的有效治療藥物及預防疫苗來控制疫情，所以世界各國紛紛祭出檢疫、隔離、普篩、鎖國、封城、停業、禁足及保持社交距離等斷然措施企圖緩和疫情。

COVID-19 在全球大流行，世界各國紛紛採取各種防疫措施以緩和疫情。

然而，COVID-19 疫情持續蔓延及防疫措施會造成以下影響，嚴重衝擊國家安全（圖 1）：

一、民心恐慌

人民對疫情持續延燒感到擔憂、對自身染疫的恐懼、對公共衛生體系是否仍能維持及對政府施政失去信心，造成政府與人民間及人與人間互不信任，整個國家社會陷於恐慌的狀態。

二、經濟衰退

許多行業（如觀光旅遊業、交通運輸業及飯店餐飲業等）因疫情而倒閉、停業或部分停工，相關工作人員因而裁員、減薪或放無薪假，經濟活動停止或下降，人民無收入或收入減少，消費不振，造成經濟衰退及人民生活困頓。

三、政府失能

許多政府機關必須暫時關閉，有些機關則因自身人員染疫而需隔離、治療、住院甚至死亡，參與工作人員不足，造成政府機關運作失去效能。

四、醫療崩潰

待檢及確診病人人數過多，超過醫療機構負荷，醫護人力不足，造成病人無人照護及院內感染，有些醫護人員自身受到感染或累倒，病人必須選擇性收治，甚至死者遺體無人處理。

五、國防受損

軍事裝備（如軍艦）內發生群聚感染，裝備必須澈底消毒，人員必須檢疫、隔離或治療，造成軍事裝備暫時停擺及人員無法執勤，均會影響國防戰力的維持。

六、交流中斷

各國採取的斷航、封鎖邊界及檢疫、隔離等防疫措施，造成國際間貨物運送及人員交流停擺或大幅減少，貿易、科學、文藝、旅遊及體育等活動無法正常進行，很多國際經貿活動及人員交流因而中斷。

有效防疫策略　防止生物病原攻擊

一、安定民心

成立中央疫情指揮中心定期向全民說明最新疫情及公告防疫措施，以公開、透明且有效的防疫策略來爭取民眾的了解、信任、支持及配合。

二、落實防疫

密切監控集中檢疫及居家檢疫、隔離人員的行動及健康情形，避免社區及家庭傳染，嚴格執行違規處罰規定，對於配合者則予以適當補助。

圖 1　COVID-19 疫情蔓延及防疫措施造成民心恐慌、經濟衰退、政府失能、醫療崩潰、國防受損及交流中斷而衝擊國家安全

三、紓困補助

對於因疫情而受到影響的產業及相關從業人員提供紓困補助，包括低利或無息貸款、延後還款、減免稅賦及發放現金等，以提振經濟並安定民生。

四、分區（艙）分流

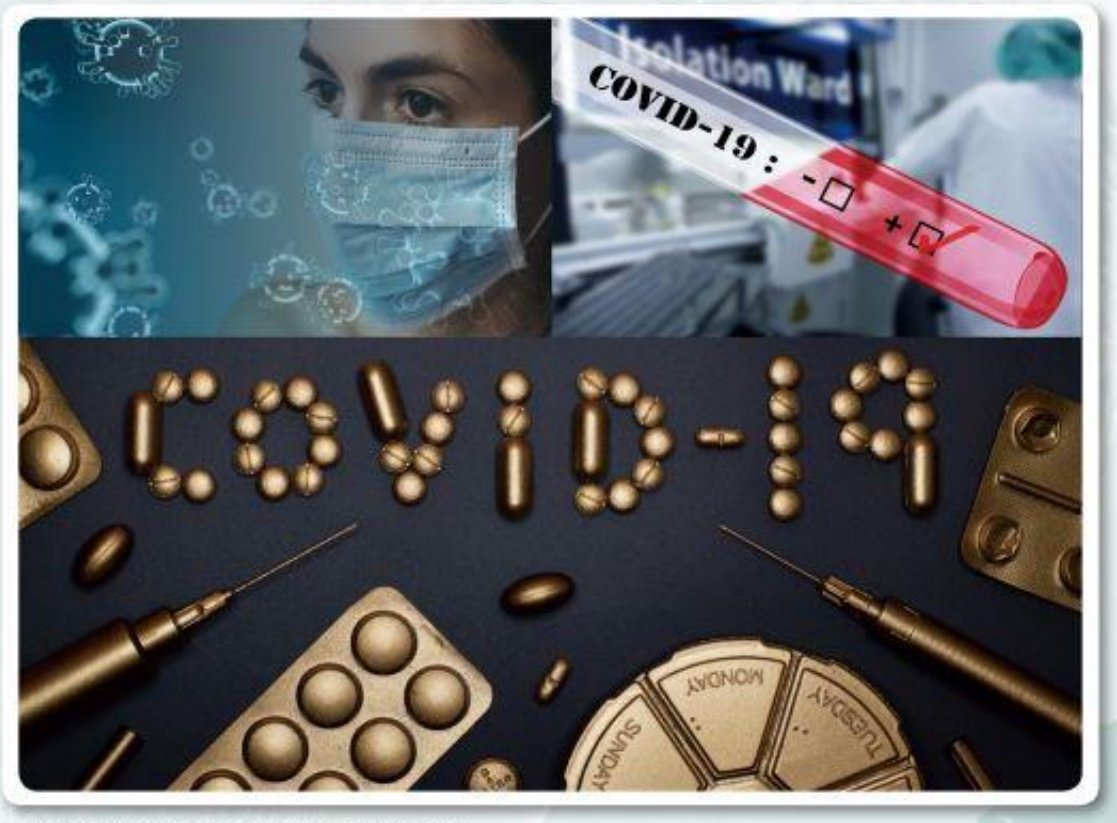
對於容易發生群聚感染的機構或密閉空間（如醫院、軍營、軍艦等）採取人員分區（艙）工作，不同區域或艙間予以適當區隔，且人員互不交流，一旦發現有疑似感染者立即執行分區隔離，避免人員交叉感染。

五、國際合作

與世界各國交換疫情訊息及防疫措施，作為制訂本國防疫策略的參考，根據需求交換防疫物資（如酒精、體溫計、防護衣、口罩等），並對需要協助國家提供支援。

六、鼓勵研發

基於 COVID-19 目前尚無有效治療藥物及預防疫苗上市，對於相關篩檢試劑、候選藥物及疫苗的開發應予鼓勵協助，必要時提供經費補助。



各國競相開發篩檢試劑、有效治療藥物及預防疫苗。

臺灣的口罩國家隊、實名制和隔離者電子圍籬系統等防疫措施及超前部署策略，是世界各國競相學習的重點。（圖片來源：總統府；基隆市政府，https://www.klcg.gov.tw/tw/News/Detail2?

家隊、實名制和電子地圖的設置、隔離者的電子圍籬系統的建立、根據大數據制定的防疫措施及超前部署的防疫策略，更是世界各國競相學習的重點。

國內 COVID-19 疫情已漸趨緩和，國人慶幸可逐步恢復正常生活型態之際，仍不可鬆懈，應持續勵行勤洗手、戴口罩、保持社交安全距離（室外 1 公尺，室內 1.5 公尺）及避免群聚活動的防疫新生活。因為目前世界上大多數國家疫情仍未趨緩，我國應在行有餘力之際，秉持人飢己飢、人溺己溺的精神，協助其他各國早日脫離疫情的威脅，以期早日恢復各國人民正常的生活方式，並確保國際間的貿易、留學、觀光、旅遊、科學及文化交流等活動可以不受干擾，如此方能確保我們的國家利益及國家安全不受損害。

結論

我國 COVID-19 防疫成效十分顯著，亦無明顯大規模社區感染現象，是全球少數仍可正常上班、上課及從事戶外活動的國家，受到世界各國的稱羨與讚揚，國際媒體紛紛報導臺灣防疫成效，尤其口罩國

知識小學堂：殺菌消毒劑的種類及作用原理

隨著全球 COVID-19 疫情持續延燒，防護衣、體溫計及口罩等防疫物品已成為戰略物資，甚至各類殺菌消毒劑，如肥皂、洗手乳、酒精、乾洗手、次氯酸水及漂白水等，也成為民眾搶購的物品。然而，想要有效對抗新型冠狀病毒（SARS-CoV-2），上述成分真的有效嗎？作用原理是什麼呢？在使用時機、方法上又有哪些注意事項或限制呢？茲簡要分述如下：

1. 肥皂（洗手乳）： 一種有效、溫和而無刺激性的清潔劑，主成分是介面活性劑（硬脂酸鈉）。由於微生物的最外層由脂質膜（lipid membrane）包覆，而介面活性劑可破壞脂質膜，殺死病原體，至於較頑強者，也會使其數量大幅減少而且致病率降低，是清潔身體及手部的最佳選擇。

2. 藥用酒精（乙醇）： 使得微生物的蛋白質變性、降解而殺死病原體，但高濃度藥用酒精（95%）會使微生物表面蛋白凝固，而使酒精無法順利穿透，反而是 70 ～ 75% 的穿透力最佳，在沒有肥皂（洗手乳）及清水可用時，可使用濃度 75% 的藥用酒精作為清潔手部的替代選擇，或作為清潔環境及擦拭物品之用。工業用酒精因含甲醇，故不適合使用。

3. 乾洗手： 主要由乙醇、甘油、香精、三氯沙（triclosan）、三氯卡班（triclocarban）組成，或另添加香料、色素和甘油等保濕劑，為在沒有肥皂（洗手乳）及清水時可作為折衷的手部清潔方式。

4. 次氯酸水（HClO）： 可穿透無外套膜（envelope）的病原體而使其膜蛋白分解，可作為食品用洗潔劑，適用於食品、食品器具、容器及包裝之清潔或環境的消毒，僅可在缺乏其他清潔劑的急迫情況下作為洗手的臨時性替換用品。

5. 漂白水： 一種強而有效的消毒劑，主成分是次氯酸鈉（sodium hypochlorite, NaClO），能使微生物的蛋白質變性而殺死病原體，但因刺激性較高而不可作為手部清潔替代品，只適用於環境消毒及清潔。

殺菌消毒劑使用時的注意事項或限制

殺菌消毒劑	注意事項或限制
肥皂（洗手乳）	• 使用前須有清水潤溼，使用後要用清水沖洗。
藥用酒精	• 只對具有外套膜的病毒有效，如流感病毒（influenza virus）、冠狀病毒（coronavirus）等；對無外套膜者效果不佳，如鼻病毒（rhinovirus）、腸病毒（enterovirus）、諾羅病毒（norovirus）等。 • 噴灑於皮膚上，揮發時易帶走水分或溶解的皮脂而造成皮膚乾裂。 • 具揮發性，長期置放成分可能會改變而影響殺菌、消毒的效果。 • 噴灑於吸收性的材質上（如衣服、紙張），會延緩揮發速率，若遇到火花或靜電放電，有燃燒的風險。
乾洗手	• 組成成分太複雜，在殺菌、消毒的效用上很難分析。 • 長期接觸三氯沙、三氯卡班成分，可能會刺激皮膚、干擾荷爾蒙分泌及損害免疫系統。 • 酒精成分揮發時易帶走水分或溶解的皮脂，造成皮膚乾裂。
次氯酸水	• 非准用之食品添加物，亦不可飲用。 • 對皮膚及黏膜具有刺激性，應避免使用在人體上。 • 穩定性差，保存期限不長。 • 照光易分解。
漂白水	• 具較強揮發性和刺激性，使用時須配戴口罩和手套以避免刺激皮膚及呼吸道黏膜，並防止吸入過多揮發氣體。 • 不可與酸性、氨氣或胺類成分混合，會產生有害物質。

本文摘自清流雙月刊中華民國109年7月 號P20-P29

從勒索軟體談關鍵資訊基礎設施防護

行政院環境保護署政風室科長／李志強

圖 1　我國 CI 包含 8 項主領域及 20 項次領域

而關鍵基礎設施安全防護（CI Protection, CIP），則指維護 CI 正常運作之相關政策與作為，其目標在於：

一、維護國家與社會重要功能持續運作，確保攸關國家安全、政府治理、公共安全、經濟及民眾信心之基礎設施與資產之安全。

二、以全災害[1]為安全防護考量，掌握設施相依關係，辨識潛在威脅與災害影響，降低設施脆弱性，縮減設施失效影響範圍與程度，提高應變效率並加速復原。

三、促進夥伴關係，健全跨領域、跨公私部門合作與資訊分享，進行實體、資

[1] 指天然災害、資安攻擊、意外事件、人為攻擊、非傳統攻擊及軍事威脅等災害，係 CI 辨識風險與威脅之主要依據。

通訊以及人員的保防與安全防護，預防因應各類災害所造成的衝擊影響，強化設施的安全性與耐災韌性[2]。

何謂關鍵資訊基礎設施防護？

其次，關鍵資訊基礎建設（Critical Information Infrastructure, CII），係指支持 CI 持續運作所需之重要資通訊系統或調度、控制系統，此為 CI 之重要元件（資通訊類資產）。

而關鍵資訊基礎設施安全防護（CII Protection, CIIP），即是讓 CII 正常運作之政策與作為。此部分不僅涉及領域內各機關，亦牽涉到跨領域的協同合作。申言之，由於 CI 之資訊機房及設備，莫不倚賴網路系統傳遞資訊，一旦網路失靈或遭到駭客入侵，將嚴重影響 CI 之正常運作，對於全民生命財產甚至國家安全，均可能造成重大衝擊。

資通安全已成顯學

在資訊化時代，大數據、物聯網、移動裝置及雲端服務等科技應用普及，網路與實體世界緊密結合。在高度倚賴網路之情況下，網路罪犯日益猖獗且難以杜絕，無論是竊取個人資料或商業機密，甚至駭客癱瘓公務網路系統，可謂司空見慣，若破壞 CI，後果更是難以想像，可見資通安全（Cyber Security）與民眾生活、政經穩定及國家安全等息息相關，故如何強化 CII 之安全及韌性，確屬當前重要議題。

為因應國際趨勢與新型態資安攻擊與威脅，行政院國家資通安全會報逐步提升我國資通安全防護能量，提出《國家資通安全發展方案（110 年至 113 年）》，該方案即指出網路攻擊已為資通安全顯學，經綜整全球重大網路攻擊事件，以資安事件發生之種類與多寡，分析全球相關資安事件，歸納出六大資安威脅趨勢[3]，其中即指出勒索軟體攻擊與 CII 之風險遽增。

勒索軟體攻擊實例

勒索軟體乃一種惡意程式，會加密在各種設備或系統上之文件或檔案，致使無法開啟使用，而駭客即藉機要求受駭者支付贖金，進而取得解密金鑰。勒索軟體可以進行無差別攻擊（Indiscriminate Attack），亦即駭客大規模且不加選擇地散布勒索軟體進行攻擊，或者針對性目標攻擊（Targeted Attack），如鎖定大型企業或醫療組織等行業，以脅迫取得更高之贖金。勒索軟體攻擊

[2] 指 CI 能夠降低運作中斷事故的影響程度與時間之能力。

[3] 行政院國家資通安全會報分析全球相關資安事件，共歸納出六大資安威脅趨勢，包含「個人資料與憑證外洩攻擊白熱化」、「勒索軟體攻擊風險激增」、「IoT 與行動式設備資安弱點威脅升高」、「APT 鎖定式攻擊竊取機敏資料」、「資安（訊）供應商持續遭駭破壞供應鏈安全」及「關鍵資訊基礎設施資安風險倍增」等，https://nicst.ey.gov.tw/。

資訊化時代，網路與實體世界緊密結合，由於 CI 之資訊機房及設備，莫不倚賴網路系統傳遞資訊，一旦網路失靈或遭到駭客入侵，將嚴重影響 CI 運作。

方式主要是網路釣魚，透過釣魚電子郵件或網站，誘導受害者點擊執行惡意連結與附件，或者利用資安漏洞直接傳播病毒，另亦有駭客入侵到內網後，取得管理者帳號密碼等資訊，在內網擴散勒索軟體並同時加密多臺重要主機資料。

一、美國最大燃油供應公司被勒索

2021 年 5 月間，Dark Side 勒索軟體集團攻擊美國最大燃油供應商 Colonial Pipeline 公司，致使該公司關閉所有輸送管道長達 5 天，影響美國東岸 45% 的燃料供應，美國總統拜登更因此宣布進入緊急狀態，甚至破例讓業者透過一般道路運送燃油。另根據媒體報導，Colonial Pipeline 公司在被駭的幾小時內雖然支付了數百萬美元的贖金，但卻換來了速度超慢的解密工具。

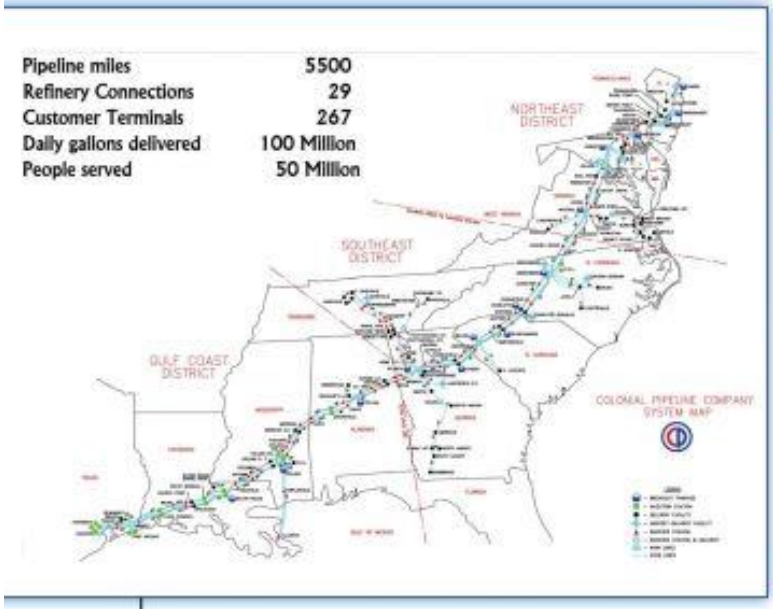
對於向駭客支付贖金之做法，官方及資安專家均不表認同，認為此舉無異於鼓勵犯罪組織未來將更肆無忌憚地向 CI 下手。對此，美國國務院在 2021 年 11 月間祭出高達 1 千萬美元獎金，鼓勵民眾舉發 Dark Side 勒索軟體集團關鍵人物之身分或位置，另外還提供 5 百萬美元獎金，給予

協助逮捕或將 Dark Side 勒索集團成員定罪之線民。

二、美國用水與污水系統被攻擊

然而，前述勒索軟體攻擊美國 CI 並非偶發事件，如美國聯邦調查局（FBI）、國家安全局（NSA）、網路安全及基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）與國家環境保護局（Environmental Protection Agency, EPA）在 2021 年 10 月間發表聯合公告，指出勒索軟體駭客正在針對美國用水與污水系統（Water and Wastewater Systems, WWS）處理廠展開攻擊，在 2021 年已至少發生 3 起攻擊事件，破壞 WWS 處理廠的資訊網路及各項裝置，影響提供乾淨飲用水或管理污水之能力。

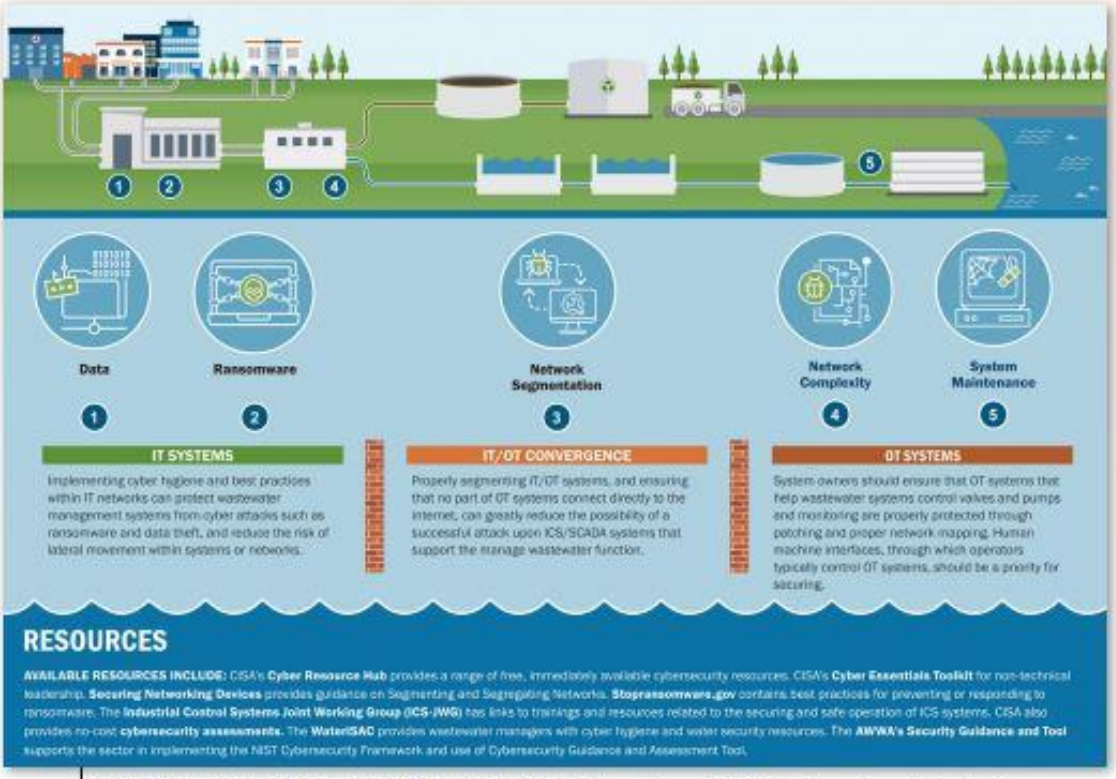
美國官方也因此針對 CI 水資源業者提供防範勒索軟體安全指引，建議 WWS 處理廠應提高警覺小心駭客入侵，如提醒員工注意網路釣魚攻擊、即時修補安全漏洞與定期更新作業系統、設置防火牆、隔離 IT 與 OT 網路，且應監控 SCDA[4] 系統之活動。



Colonial Pipeline 為美國東南部燃油的主要供應商，遭駭客攻擊後，致使該公司關閉所有輸送管道長達 5 天，影響美國東岸 45% 的燃料供應。

美國國務院在 2021 年 11 月祭出高達 1 千萬美元獎金，鼓勵民眾舉發 Dark Side 勒索軟體集團關鍵人物之身分或位置。（Photo Credit: Official FBI Twitter, https://twitter.com/FBI/status/1456344912224522241?s=20）

[4] IT 為 Information Technology（資訊技術）、OT 為 Operational Technology（營運技術）、SCDA 為 Supervisory Control and Data Acquisition（監視控制與資料擷取系統）。



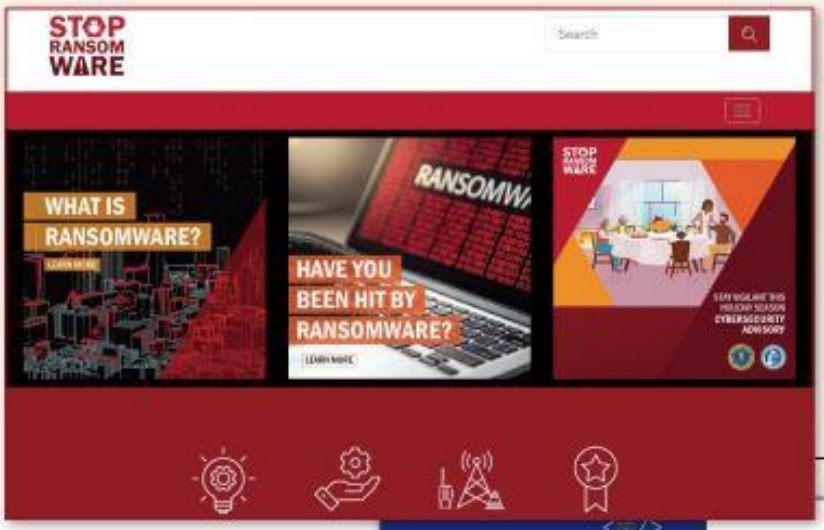
美國官方針對 CI 水資源業者提供防範勒索軟體的安全指引。（Source: CISA, https://www.cisa.gov/ncf-water）

各國之防範措施

值得注意者，為因應勒索軟體威脅，美國 CISA 整合相關情治單位設立 StopRansomware.gov 網站，除了揭露勒索軟體相關資訊外，還提供如何偵測、對抗及回應勒索軟體攻擊之指南，以增強網路防禦能力並降低勒索軟體攻擊之風險。該官方網站還提供免費健檢服務，如掃描與測試以幫助評估、識別及減少政府機關、公司企業甚至是個人所面臨之資安威脅[5]。

其實早在 2016 年 7 月，歐洲司法警察機關與資安業者就共同創立對抗勒索軟體入口網站 www.nomoreransom.org，目前已有 40 幾個國家的執法機關加入，包括我國法務部調查局、內政部警政署刑事警察局等，該網站提供超過 10 餘種勒索軟體的免費解密工具，成為全球對抗勒索軟體之重要資源網站。

[5] 其服務項目包括：1. 弱點掃描（Vulnerability Scanning）：識別容易遭受攻擊之系統或設備。2. 網路應用程式掃描（Web Application Scanning）：識別攻擊者可能利用之網站弱點與不良配置。3. 網路釣魚活動評估（Phishing Campaign Assessment）：評估員工或民眾打開惡意電子郵件（即網絡釣魚）之可能性，這係勒索軟體主要攻擊方式。4. 遠端滲透測試（Remote Penetration Testing）：通過模仿駭客之攻擊手法來測試防禦能力。5. 網絡安全評估工具（Cyber Security Evaluation Tool, CSET）：屬獨立桌面應用程式，即協助透過自我評估方式，以瞭解防禦勒索軟體事件及遭駭後之恢復能力。



美國 CISA 整合相關情治單位設立 StopRansomware.gov 網站，揭露勒索軟體相關資訊，並提供應對勒索軟體攻擊之指南。（Source: CISA, https://www.cisa.gov/stopransomware）

2016 年歐洲司法警察機關與資安業者共創對抗勒索軟體的入口網站 www.nomoreransom.org，目前已有 40 幾國的執法機關加入，該網站提供超過 10 餘種勒索軟體的免費解密工具，為全球對抗勒索軟體之重要資源網站。（Source: NO MORE RANSOM, https://www.nomoreransom.org/zht_Hant/index.html）

數位經濟浪潮來襲，提高資安意識為首要之務

當前數位經濟及資訊科技可說日新月異，世界各國皆以數位化、智慧化及網路化發展基礎建設，同時也進入情報戰、資訊戰之科技時代。隨著疫情蔓延，公私部門遠端線上作業之情況大幅增加，同時也助長了駭客攻擊。

俗話說道高一尺、魔高一丈，安裝防毒軟體固然重要，但要面對詭譎多變的駭客，提高資安意識應是首要之務，亦為防範勒索軟體攻擊之重要關鍵，尤其是良好的網路使用習慣，例如識別可疑電子郵件，不要隨意點擊連結，也不打開未知或不受信任來源電子郵件之附件。

展望未來，我國或許可以建立跨部會且整合政府資源之對抗勒索軟體入口網站，例如仿效美國官方網站 StopRansomware.gov；同時持續加強國際合作，以掌握駭客最新手法及因應之道。

本文摘自清流雙月刊中華民國111年1月 號P58-P64