第八章　複合型網路戰

曾怡碩*

壹、前言

2020 年新冠肺炎疫情影響全球網路使用型態，因疫情隔離與封城的居家工作與就學，讓家戶網路使用量大增，網路攻擊與勒索犯罪伴隨疫情而陡增。除因營業秘密與隱私保護需求，使得視訊、郵件與雲端安全備受重視，網路資訊傳輸穩定性也受到更嚴密關注。另一方面，因疫情所帶來的不確定性與恐慌，也讓網路不實訊息的散播以及由國家政府所發動的網路認知作戰攻防趨於熾熱。

美中科技新冷戰在 2020 年更趨壁壘分明，美國面對的是網路攻擊、網路竊密以及認知影響力作戰的升高，以及美中的軍事緊張情勢伴隨美國在 2020 年 11 月舉行總統大選而增溫。在此同時，美軍網路司令部的奉命介入拒止與美國司法部門的揭露，這些藉由網路攻防與網路爭議訊息的防制作為所透露出的，是在網路空間的灰色地帶衝突下，嚇阻的操作如果純粹倚仗網路溯源與數位鑑識，其實仍有相當大的侷限性。有鑑於 2020 年諸多局勢變動，本章接下來將藉由梳理疫情下網路威脅的變化，呈現這一年走向複合型網路戰之趨勢，並檢視安全部門反制因應之道。

貳、新冠肺炎疫情下的網路攻擊威脅

新冠肺炎疫情在 2020 年擴散成為全球大流行，各國雖然採取不同的檢疫與隔離政策，但多要求／鼓勵人們待在家裡、在家工作、非必要不要出門，這讓世人更加深對於網路的倚賴。面對新冠疫情的未知與不確定性，在人們對於新冠肺炎的正確醫療訊息需求迫切的同時，網路假消息充

* 曾怡碩，國防安全研究院網路安全與決策推演研究所助理研究員。

斥將造成恐慌加劇。民主國家政府基於緊急狀況特殊需要，一方面加強查緝網路假訊息，[1] 另一方面則放寬網路遠距醫療所用之網路平台限制。[2] 網路平台業者也配合加強檢測過濾虛假不實訊息，臉書與谷歌並開始提供新冠肺炎疫情相關訊息。

在此同時，惡意網路駭客利用人們關切新冠肺炎疫情相關訊息，諸如疫情發展、疫苗開發、醫療診所篩檢資訊，以及因新冠肺炎疫情造成經濟衰退而遭資遣的人對於就業資訊的關切，[3] 運用釣魚郵件、設置後門之網頁等社交工程方式，嵌入網路病毒取得控制權並封鎖檔案進行勒索，造成勒索病毒肆虐。美國在 2020 年第 1 季的網路攻擊就較前一年同期增加 273%，而 2020 年前兩季的勒索病毒案例就較前一年同期增加 109%。[4] 美國國土安全部發覺情況嚴峻，商請美國網路司令部協助反制打擊，才讓情況稍微緩解，2020 年第 3 季釣魚郵件減少 46.9%，但第 3 季詐騙網頁仍增加 47.4%。[5]

2020 年 9 月以後，隨著疫苗開發試驗陸續傳出消息，針對醫療院所或研究機構的員工之商務名義釣魚郵件攻擊及裝置勒索病毒（其中 Ryuk 占了 75%）尤其猖獗，僅從 9 月到 10 月就暴增 71%。然而，勒索病毒癱瘓醫院行徑，卻在德國造成醫院病患死亡。[6] 此外，對醫院及醫療研究機構施以勒索病毒攻擊，也阻礙了新冠肺炎疫苗研發期程。[7] 由於新冠肺炎疫苗牽涉龐大商機之外，也攸關國家安全利益甚鉅，不乏國家支持的網路

1 蕭博文，〈調查局查 3 假訊息 呂文忠：另受理 59 件囤積案〉，《中央社》，2020 年 3 月 18 日，https://www.cna.com.tw/news/asoc/202003180325.aspx。

2 Ricardo Alonso-Zaldivar, “To keep seniors safe at home, Medicare expands telemedicine,” *Associated Press*, March 18, 2020, https://apnews.com/58e118636f3e39c53370131561127a54.

3 “*Coronavirus Used in Spam, Malware File Names, and Malicious Domains*,” *TRENDMICRO*, November 11, 2020, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

4 Patterson Belknap, “Ransomware Attacks During COVID-19,” *Lexology*, September 3, 2020, https://www.lexology.com/library/detail.aspx?g=f85e4ffb-6c32-43ca-8240-33a5d9d94b2b.

5 同註 3。

6 Patrick Howell O’Neill, “A wave of ransomware hits US hospitals as coronavirus spike,” *MIT Techonology Review*, October 29, 2020, https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/.

7 Sarah Coble, “Ransomware Disrupts COVID-19 Medical Trials,” *Infosecurity Magazine*, October 5, 2020, https://www.infosecurity-magazine.com/news/ransomware-disrupts-covid19/.

駭客團體從事對於疫苗開發進展資訊之網路竊密之行徑，中共就被點名為其中之一。[8]

新冠疫情在網路相關層面的衝擊並非全然負面，遠距醫療的適用限制就因疫情而有所突破。由於醫療照護行為與醫藥具高度專業性，且關係健康與生命，不論醫療相關資訊或者診療、藥物及醫材，均受高度管制，而醫療過失屬於業務過失，須加重處分。對於幅員遼闊國家，鄉間就診不易，其餘國家也有偏鄉外離島就醫求診困難，網路遠距醫療一般是在此類情境下適用，也因此醫療資訊領域並未隨資通訊科技發達而獲大幅推廣。新冠肺炎全球大流行造成大規模居家隔離、上課、工作，加上避免醫療體系維運能量崩潰的考量，造就遠距醫療的大規模需求，促成美國政府在 2020 年 3 月 17 日宣布放寬遠距醫療使用之網路平台管制，便利有健康照護及慢性病處方需求民眾 —— 尤其是高齡人士，以網路取得諮詢、診療以及處方。為保障民眾權益，醫事責任仍舊存在，因此需要檢驗的項目，包括新冠肺炎檢疫，不得以網路行為取代，網路遠距醫療後端平台則須提供檢疫地點指南。[9]

根據研究報告指出，「美國政府更趁勢提出多項政策誘因來鼓勵其國內遠距醫療產業發展，包括：Medicare 擴大保險範圍，讓更多高齡者使用遠距醫療服務，並可支付醫方所開立的遠距醫療帳單。同時放寬『美國健康保險可攜性及責任法案』（The Health Insurance Portability & Accountability Act, HIPAA）隱私規定，允許醫療機構使用非公共的遠距通訊軟體替病患看診，如 FaceTime、Facebook Messenger、Google Hangouts 或 Skype，提供雙方會診的方便性。此外，『美國食品藥品監督管理局』（Food and Drug Administration, FDA）放寬醫療用途之遠距監測醫材可於居家使用，讓量測數據自動回傳至醫療機構判讀，降低醫護人員的照顧負擔與民眾至醫院就診的不便性。最後，美國『聯邦通訊委員會』（Federal Communications Commission, FCC）提出『COVID-19 遠距醫療計畫』

8　同註 6。

9　林秀英，〈新冠疫情助攻！2020 年上半年數位醫療投資金額再創新高〉，《經濟部中小企業 Findit 平台》，2020 年 7 月 27 日，https://findit.org.tw/researchPageV2.aspx?pageId=1462。

（COVID-19 Telehealth Program），為健康照護業者提供遠距照護服務所需的寬頻網路和物聯網裝置。」[10]

遠距醫療發展得到突破的同時，也浮現未來隱憂。運用網路空間傳輸醫療影音與資訊等敏感個資，加上傳輸中斷或遭改造，都可能造成醫事糾紛，因此過去只有通過資訊安全認證平台始可遂行遠距醫療行為。2020年是美國在其總統頒布緊急命令狀態下，才放寬遠距醫療的平台管制，但對資安防護仍附但書，遠距醫療運用之網路／社群媒體平台必須具端對端加密功能。因此，美國衛生部明文排除包括「TikTok」等相對開放、群組性，足以人臉辨識（public-facing）而不具隱私保障的網路平台。此外，基於良善原則，符合隱私與加密功能的網路平台若因發生遠距醫療資安事件，而導致機敏健康個資外洩，將無須擔責。[11] 雖說疫情過後，遠距醫療管制可能獲得放寬，但疫情期間遠距醫療行為之資安事件、居家網路用量過大導致斷訊與醫事糾紛究責風險，預期仍可能於疫情危機過後浮現。

參、結合網路攻擊的認知作戰威脅

民主國家雖於承平時期竭力保護網路空間言論自由，但在諸如選舉期間、傳染病疫期、內亂外患等非常時期，仍會加強管制網路不實訊息，並依法課罰究責，冀以遏制假訊息之製造與流竄。資訊戰的範疇包含網路攻擊之網路作戰以及影響力攻勢之認知作戰。前者為國家支持或非政府駭客團體，以社交工程或網路直接滲透方式散布病毒或進行部署，伺機發動分散式阻斷網路服務攻擊或遂行進階式持續威脅攻擊。後者則多藉由捏造、散播虛假爭議訊息，藉以達到影響訊息接受者之認知，形成對其身處體制之質疑與不滿，進而改變其行為並擴大社會分化對立。

對於民主國家而言，其民主開放與保障言論自由，成為認知戰攻防的不對稱特性分界線。敵意國家或團體可充分運用此特性施以認知戰攻擊，

10 林信亨，〈疫情之下的遠距醫療應用商機〉，資策會《AISP 資料庫》，2020 年 7 月 7 日，https://mic.iii.org.tw/aisp/Reports.aspx?id=CDOC20200703004。

11 同註 2。

而民主國家從事認知戰之際，卻往往受制於敵意國家專制體制對言論的箝制與網路控制。認知戰往往並非單獨進行，而是混搭其他諸如網路戰或者實體衝突。因此，必須要充分體認到認知戰從戰略層次到戰術層次，從虛擬空間結合實體向度的特質，進而在認知戰攻防上靈活應處。尤其認知戰絕非新的產物，其本身類似過去的統戰應用了新的科技手法。駭客網路攻擊與假訊息之影響力攻勢雖看似兩獨立行動，但在關鍵敏感時機的網路戰作為，卻能造成認知戰效果；或者，藉由網路戰與認知戰的混合運用，就足以發揮更大的認知影響。[12]

近年來俄羅斯對於西方國家選舉安全的威脅，則是藉由駭客網路攻擊將選舉陣營機敏文件竊出，再將文件經變造後外洩散布，即所謂「駭入再洩露」（hack and leak）的手法，意圖藉散播不實資訊、混淆視聽的事件，達到造成選民疑惑，進而影響選舉結果或質疑選舉效力的後果。最著名的案例，就是俄羅斯以國家支持之駭客團體，分別於 2016 年美國總統大選針對美國民主黨競選陣營，以及 2017 年法國總統大選針對馬克宏（Emmanuel Macron）競選陣營之「駭入再洩露」。我國總統府於 2020 年 5 月 16 日傳出遭駭客入侵，資料遭有心人士變造、偽造以黑函方式散布。[13] 由於過去我國遭遇資安事件多為網路駭客之網路戰，或者敵方施放假訊息之認知戰，較少遭遇類似此次之網路戰與認知戰混合運用之重大資安事件，這對民主政治運作之影響，實際已達影響力作戰層次。

中共師法俄羅斯資訊作戰手法的同時，自然會將過去統戰傳統，或者延續套路，或者針對台灣而加以客製創新。首先是 2020 年 5 月 4～5 日間，中共國安單位外圍駭客團體 APT41 對台灣的石油、石化及科學園區等關鍵基礎設施業者進行網路攻擊，中油公司、台塑企業及記憶體封測廠力成接連傳出遭勒索病毒箝制，三間公司都緊急要求員工關機斷網。由於中油公司的捷利卡、車隊卡及中油 PAY 等支付工具皆被迫暫停使用，引

12 曾怡碩，〈不對稱戰：認知作戰的途徑〉，國防安全研究院《國防情勢特刊》第 3 期，2020 年 7 月 10 日，https://indsr.org.tw/Download/%E5%9C%8B%E9%98%B2%E6%83%85%E5%8B%A2%E7%89%B9%E5%88%8A-3.pdf，頁 28。

13 溫貴香、范正祥、蘇龍麒、陳韻聿，〈總統府遭駭 國安人士：典型認知空間作戰製造紛亂〉，《中央社》，2020 年 5 月 16 日，https://www.cna.com.tw/news/firstnews/202005160148.aspx。

發社會大眾關切。類似這種鎖定台灣關鍵基礎設施業者發動攻擊的手法，將構成灰色地帶衝突的效果。在中共意圖犯台之前期，以及武力犯台之全程，均可能啟動平日滲透潛伏之 APT，進行攻擊阻斷運作與服務。台灣民眾日常生活秩序遭打亂的結果，勢必造成疑懼與恐慌，如此即形同造成混合式認知作戰威脅。[14]

其次則是以網路社群媒體假訊息，搭配運用中共對我軍機艦擾台之實體空間武力恫嚇，意圖製造困惑與擴大質疑分化。2019 年 4 月成立的中國北京大學「南海戰略態勢感知計畫」（SCSPI），其推特平台近期連續發布假訊息 —— 2020 年 8 月 30 日以 ADS-B 航跡質疑美軍機自台灣起飛，8 月 31 日釋出美軍機穿越台灣後逼近中國偵蒐；9 月 1 日則發布美軍艦疑似進入澎湖水道東側。[15]《環球時報》則協同接續發布報導與評論。中共利用 SCSPI 與《環球時報》以假訊息引發媒體跟進報導，如此精準的協同連動，其實是循 2020 年初台灣大選期間與新冠肺炎疫情期間，中共各部門所遂行的協同式假訊息認知作戰模式。[16]

肆、對網路攻擊之反制措施

網路攻擊之灰色地帶特性，很可能讓用於降低武裝衝突可能性的嚇阻手段失效。國家若能確定攻擊來源並遂行反擊，且其反擊迅速而有力，將可因此獲得相當之嚇阻效力。但由於網路攻擊難以明確辨識、確認攻擊來源，一般藉由 IP 位址溯源，則難以排除僅被利用作為跳板之嫌。故即使

14 黃彥棻，〈臺美聯手防駭，追緝並起訴 APT41 中國網軍〉，《iThome》，2020 年 9 月 18 日，https://www.ithome.com.tw/news/140054。根據該報導，APT41 又被稱為 Winnti Group、Barium、Winnti、Wicked Panda、Wicked Spider。APT41 利用中國四川省成立的「成都 404 網路公司」作為掩護，針對全球政府機關、通訊及科技業供應鏈、學術研究機構、醫療機構、電玩遊戲產業等全球超過一百家企業發動網路攻擊及間諜活動，受害企業散布台灣、新加坡、馬來西亞、日本、韓國、泰國、越南、巴西和澳洲等，攻擊活動則包括：非法入侵他人主機、竊取機敏資料以及進行電信詐欺等。

15 洪哲政，〈中共官媒惡炒美軍在台假訊息國防部大動作反駁〉，《聯合報》，2020 年 9 月 2 日，https://udn.com/news/story/10930/4829196。

16 曾怡碩，〈中共在武漢肺炎疫情下進行影響力作戰〉，國防安全研究院《國防情勢特刊》第 1 期，2020 年 4 月 28 日，頁 8-10，https://reurl.cc/pyx7ax。

一國關鍵基礎設施遭受網路攻擊，而導致相當於實體武裝攻擊所致之傷亡或損失，並欲據此發動自衛權反制之際，若循網路空間溯源，卻可能陷入缺乏明確具正當性之反擊對象的窘境，這很可能讓嚇阻失去效力。[17]

國家支持之網路駭客團體與影響力作戰團隊之崛起，意圖對他國形成不對稱作戰優勢的同時，網路攻擊之難以溯源歸咎之特質，造成遭受網攻國家無國際法理基礎以認定遭受武力攻擊，並據以遂行武力反制。面對此一境況，具備優越網路攻擊能力的國家，便可能針對嫌疑對象訴諸網路反擊予以懲罰制裁。但同樣囿於難以溯源歸咎特性，遭受所謂網路「反擊」的國家，也很可能無從主張遭受特定對象之網路攻擊。如此一來，將使發動懲罰制裁的國家徒具反制網路攻擊能力，卻仍無從形成嚇阻網路攻擊之明確效力。補救之道，就是由具備可信的反制網路攻擊能力的國家，藉由宣示其網路戰略或交戰規定，警告意圖進犯網路空間的潛在敵手。這種在灰色地帶畫上紅線的做法，如果缺乏迅速有力且持續精準的反制作為，反倒容易成為敵方不斷挑釁與模糊紅線的把柄。因此，膽敢公開宣示進行反制網路攻擊的國家，理應具備不畏遭受挑戰的網路反擊實力，或令人聞之膽怯的實際反制前例。

美國的補救措施，便是藉由網路空間以外的衛星偵照與人員情報手段，在明確辨識目標並鑑識蒐證齊備後，由其國內聯邦調查局或司法部公告，並以國內法起訴網路攻擊駭客。起訴的作用在於，可經由長臂管轄效力及於與美國簽署引渡條例之友盟，待被起訴對象過境之際，將其逮捕遣送美國受審，令其畏懼而不敢出境，藉此達到嚇阻效力。前述中油公司遭中共支持外圍駭客團體 APT41 網路攻擊勒索後，台灣的調查局與美國聯邦調查局結合美台網路犯罪偵防能量，共同打擊追緝並成功起訴該駭客團體成員，就是一個結合友盟以聯合反制網路攻擊的成功案例。[18]

17 James Lewis, “Cognitive Effect and State Conflict in Cyberspace,” *CSIS Report*, September 26, 2018, https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace.

18 同註 14。

2018 年以來美軍網路司令部對於境外勢力干預選舉安全，是以「前進防禦部署」（defending forward）加以反制。[19] 美國也會藉對網路攻擊來源國施以經濟制裁，進一步擴大嚇阻戰果。此外，對於蒐證未齊備而不足以呈上法庭起訴之對象，美國也可能直接對網攻駭客以網路郵件遞送警告函，並將此事昭告天下，以明示已掌握該對象真實身分與通訊往來管道，對該對象及其隸屬組織、國家，達到另類嚇阻效力。另一方面，對於未來發生類似突襲珍珠港式的災難性網路攻擊，網路安全領域的產官學界咸認機會不大。[20] 因此，因網路攻擊而造成相當於實體空間武力攻擊所導致之傷亡與毀損，進而構成武裝衝突，並據以行使自衛權的立論基礎，短期內難以獲得大幅度加強，故在國際法理上仍難以成立。這也將導致網路攻擊這類新型態衝突，勢將持續處於難以應處的灰色地帶，讓各方難以寄望國際法有所突破而對其有效規範。

國際法認定國家一旦遭受武裝攻擊，得行使自衛權遂行反制。鑑於網路攻擊並未構成如同一般武裝攻擊之傷亡與損害，國際法理對於其是否構成武裝攻擊的要件，如前所述迄今仍充滿爭議，網路攻擊也因其未達戰爭門檻而成為名符其實的灰色地帶衝突。故網路攻擊迄今尚為國際法化外之地，世人常舉《塔林手冊 2.0 版》（*Tallinn Manual 2.0*）為例，然而其僅為北約組織之規範，並未達國際法之效力。以國際法規範反制網路攻擊陷入膠著之際，北約的《塔林手冊》仍持續精進中，由一開始美國片面主導色彩濃厚而遭致反彈，迄今因各方的參與而逐漸融合私部門與歐洲元素的觀點。另一方面，為充分授權、保障與規範網路作戰執行人員在這類隱匿灰色地帶衝突中的作業操作，著手制定有限度公開的交戰規定，已逐漸成為美國及其友盟的共通作業準則。目前美、日、韓均稱制定頒布網路交戰規定；[21] 美軍也公開宣示，對美國之安全盟友的網路攻擊，將遭受美軍

19 Jim Garamone, "DOD Works to Eliminate Foreign Coronavirus Disinformation," *Defense News*, US Deppartment of Defense, April 13, 2020, https://www.defense.gov/Explore/News/Article/Article/2147566/dod-works-to-eliminate-foreign-coronavirus-disinformation/.

20 James Lewis, "Dismissing Cyber Catastrophe," *CSIS Commentary*, August 17, 2020, https://www.csis.org/analysis/dismissing-cyber-catastrophe.

21 根據 2020 年 8 月 25 日專案計畫對國防大學法律系田力品教授的訪談成果。

以符合比例原則之報復反擊。[22] 循此趨勢，美國安全社群已開始提倡軍隊需足以因應與適應灰色地帶衝突的威脅環境，[23] 並於境內外的網路部隊部署認知影響力作戰單位。[24]

伍、小結

2020 年由於新冠疫情影響，造成工作與生活型態改變，在家工作與上學更加仰賴網路的同時，也讓網路釣魚信件以及網路勒索犯罪遽增。這樣的全球性大規模傳染病所帶來的未知與不確定性，也讓利用網路製造散播不實訊息的惡意團體，更有可趁之機以運用假訊息進行認知空間操縱。如這般在網路空間的灰色地帶衝突，並不乏搭配實體空間的灰色地帶操作 —— 不論是對關鍵基礎設施的網路攻擊或勒索犯罪以製造疑懼，還是藉由軍機艦騷擾後釋放假造的數位航跡以擴大猜忌與紛亂，都是複合型網路戰，亦即網路假訊息搭配實體空間行動或網路攻擊的混合式威脅，意圖達到灰色地帶認知作戰的效果。面對網路威脅樣態的演變，為有效加以反制，如果依循過去單靠網路部隊的模式，恐怕不足以因應。2018 年以來美軍網路司令部對於境外勢力干預選舉安全，是以前進防禦部署加以反制。2020 年美國安全社群已開始提倡軍隊需足以因應與適應灰色地帶衝突的威脅環境，並於境內外的網路部隊部署認知影響力作戰單位。我國在 2020 年雖成功因應來自中國大陸武漢的新冠疫情，但還須面對來自中共以網路攻擊搭配認知空間操縱的灰色地帶混合威脅。未來我國可與印太區域美國等理念相近友盟積極合作，共同應處在新冠疫情下的複合型網路威脅新樣態。

22 Taketsugu Sato, Takateru Doi and Kenji Minemura, “SDF booting up capabilities to defend against cyberattacks,” *The Asahi Shimbun*, June 14, 2020, http://www.asahi.com/sp/ajw/articles/13429347.

23 Mark Pomerleau, “The military must learn to operate more in the gray zone,” C4ISRNET, November 4, 2020, https://www.c4isrnet.com/information-warfare/2020/11/04/the-military-must-learn-to-operate-more-in-the-gray-zone/.

24 Mark Pomerleau, “Cyber warriors are getting new teammates: information operators,”C4ISRNET, October 30, 2020, https://www.c4isrnet.com/information-warfare/2020/10/30/cyber-warriors-are-getting-new-teammates-information-operators/.