由俄烏戰爭談CI安全防護

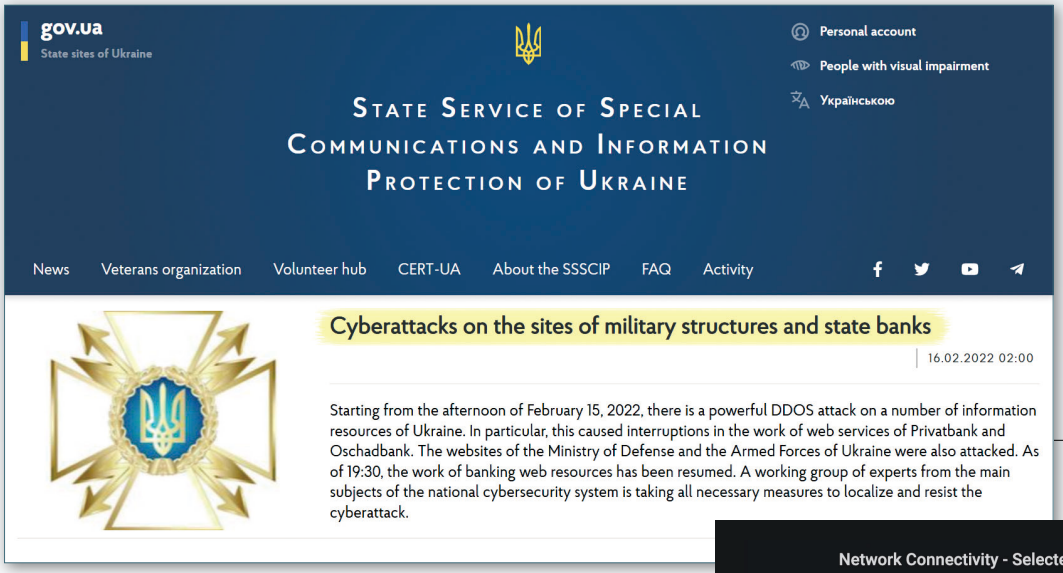
◆ 關鍵基礎設施防護研究室研究員 — 陳永全

國家關鍵基礎設施在天然災害、資安威脅及恐怖攻擊以外，已面臨到更嚴峻的挑戰，那就是戰爭所引發的戰災。

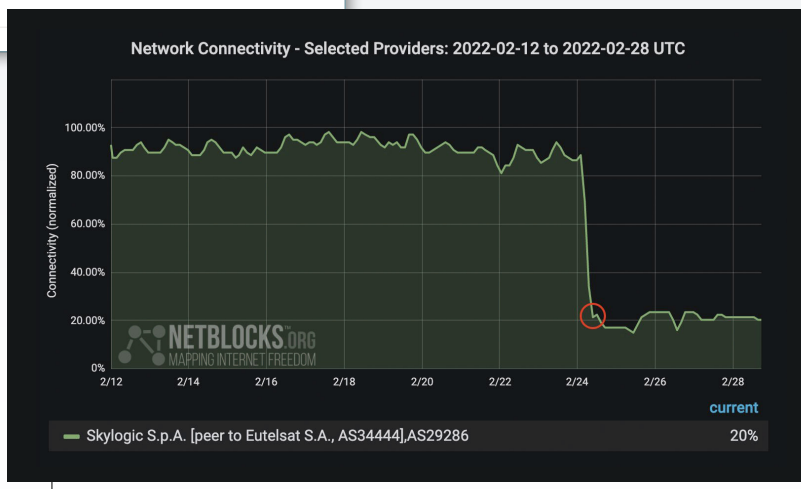
CI 的最嚴峻考驗

俄烏戰爭從 2022 年 2 月 24 日開戰以來，似乎陷入了看似拉鋸但卻遍尋不著終點的局面，而隨著氣候逐漸步入寒冬，交戰情勢也更顯冷冽與膠著。

衛戍烏克蘭安全的軍隊，在俄羅斯不斷地攻擊下，竭盡所能，想方設法維持其境內國家關鍵基礎設施（Critical Infrastructure，下簡稱 CI）的安全，也為 CI 防護詮釋了在面臨天然災害、資安威脅及恐怖攻擊外，所遭遇到的更嚴峻考驗，那就是戰爭所引發的戰災。



烏克蘭國防部、武裝部隊網站、國家銀行遭受網路 DDoS 攻擊。（Source: State Special Communications Service of Ukraine, https://cip.gov.ua/en/news/shodo-kiberataki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv）



網路流量分析業者 NetBlocks 曾公開網路數據，顯示 2 月 24 日烏克蘭和歐洲大部分地區的網路連線中斷，後證實為隸屬美國電訊公司 Viasat、支援該區的 KA-SAT 衛星在戰爭中遭受駭客攻擊。（Source: NetBlocks twitter, https://twitter.com/netblocks/status/1498365220107997191）

俄烏戰爭前夕—網路攻擊頻繁出現

俄烏戰爭開戰前一週，烏國即飽受疑似來自俄羅斯的駭客入侵，至少有 10 個以上與政府相關網站，包括國防部、外交部、文化部及 2 家國營銀行受到駭客攻擊；[1] 受攻擊網站都是被大量垃圾數據封包阻塞，使網站呈現癱瘓的狀態，研判是遭到大規模「分散式阻斷服務攻擊」（DDoS）。

DDoS 攻擊者運用多個盜用或掌控的來源持續不斷地攻擊目標，其意圖係讓烏國民眾生活不便，造成其等恐慌，打擊民心士氣，進而製造社會的不安與動亂。

俄烏戰爭發起日—虛實攻擊併用

俄羅斯總統普丁於 2 月 24 日 5 時 50 分批准對烏克蘭發動「特種軍事行動」，烏國總統澤倫斯基旋即於 7 時發布緊急動員命令。在開始進行全國動員任務之際，多數烏府網站遭受駭客攻擊，網站失能癱瘓。據烏國數位轉型部表示，大規模 DDoS 除針對境內多家銀行外，亦發現駭客鎖定烏國防部的郵件伺服器，利用殭屍網路病毒 Dana Bot 進行攻擊。

[1] "Ukraine's defence ministry and two banks targeted in cyberattack", https://www.euronews.com/my-europe/2022/02/15/ukraine-s-defence-ministry-and-two-banks-targeted-in-cyberattack.

俄羅斯在 2 月 24 日當天進行超過 2 百次襲擊，摧毀癱瘓多處機場與導彈系統，其中包含全世界機身最長、承載重量最大的飛機 AN-225 Mriya。（Photo Credit: Kyiv City Council, https://w.wiki/5pGe）

在實體軍事攻擊上，據《法新社》報導，俄羅斯在 2 月 24 日當日進行超過 2 百次襲擊，俄國防部更於 2 月 24 日當晚宣稱，其已導致烏境內 11 處機場、3 個指揮所、1 處空軍基地、18 處 S-300 型地對空導彈系統和 1 處薩姆（SA-11）型導彈系統，全數摧毀癱瘓。

俄烏戰爭開戰後第一週—網站攻擊大爆發

俄烏戰爭開戰後的第一週內，相關網路攻擊事件更是不斷傳出，從政府機關、石油公司、軍事單位等，到電視臺、學術機構、協助烏克蘭難民的歐洲國家官員，也相繼成為駭客下手的目標。[2] 另有駭客入侵竄改烏政府網站，散發意圖動搖軍心士氣的不實訊息。例如，烏國特別通訊暨資訊保護局（State Service of Special Communications and Information Protection, SSSCIP）與安全局（Security Service of Ukraine, SSU）發現，駭客入侵烏國地方政府網站，宣稱「烏克蘭已經投降，俄羅斯和烏克蘭即將簽署和平協議的不實訊息與謠言」。烏克蘭議會也提出類似警告，指駭客入侵赫爾松公共廣播新聞臺，散布烏國投降的謠言。此外，烏國安全局也指控俄國軍事情報局（GRU），利用 Telegram 頻道不斷散發類似「烏克蘭政府即將投降及兩國即將簽署和平協議」等不實訊息。

[2] 《【資安週報】2022 年 3 月 1 日至 4 日》，https://www.ithome.com.tw/news/149711。

戰爭初始，腹地廣大的烏國民眾根本無從辨明訊息的真偽；俄軍突如其來的特別軍事行動，尤其是早有計畫地運用虛假訊息作為，除讓烏府措手不及外，更增添烏府在開戰初期緊急動員人力的難度。

俄烏戰爭開戰後迄今—持續不斷的 CI 攻擊事件

茲針對俄烏戰爭期間之 CI 攻擊態樣與影響層面整理如下頁表 1。開戰後，俄羅斯軍隊步步進逼，不間斷地奪控烏境內 CI，3 月即占領烏南札波羅熱（Zaporizhzhia）核電廠，該廠是歐洲最大核電廠，也是全球十大核電廠之一。由於俄烏雙方在核電廠周邊不停交火，更引發舉世擔心核災因此爆發之恐慌。

針對 CI 的網路攻擊，根據 SSSCIP 公布資料，俄羅斯攻擊目的，有 242 件涉及資訊蒐集，192 件是為了植入惡意程式；攻擊標的，有 179 起是鎖定該國與地方政府組織，104 起是針對安全與國防部門，另有 54 起鎖定能源產業。[3]

俄國駭客入侵烏克蘭政府網站，佯稱烏克蘭已投降，兩國要簽署和平條約，烏克蘭安全局而後發布闢謠消息。（Source: Security Service of Ukraine twitter, https://twitter.com/ServiceSsu/status/1499418645537116160）

從衛星空拍可見烏克蘭札波羅熱核電廠之俄烏交火對峙，引發舉世擔心核災爆發之恐慌。（Photo Credit: Planet Labs, https://www.planet.com/gallery/#!/post/zaporizhzhia-nuclear-power-plant）

[3] 本統計數據截至 2022 年 6 月，《烏克蘭統計自開戰以來已遭到近 800 次網路攻擊》，https://www.ithome.com.tw/news/151719。另截至 2022 年 8 月底，烏克蘭電腦緊急回應組（CERT-UA）已檢測到 1,123 次網路攻擊。“Ukraine has recorded over 1,100 cyberattacks since the beginning of the year”, https://cybernews.com/cyber-war/ukraine-records-over-1100-cyberattacks.

表 1　俄烏戰爭中受攻擊之 CI 設施

項次	CI 分類	被攻擊目標	衝擊影響
一	能源 關鍵基礎設施	1. 烏克蘭車諾比核電廠 2. 烏克蘭札波羅熱核電廠 3. 俄羅斯煉油廠 4. 烏克蘭哈爾科夫電廠 5. 烏克蘭卡霍夫卡電廠 6. 烏克蘭阿佐夫斯卡爾煉鋼廠	大規模停電
二	水資源 關鍵基礎設施	1. 盧甘斯克州（Luhansk）供水站 2. 北頓涅茨河水庫 3. 基輔水庫	大規模斷水
三	資通訊 關鍵基礎設施	1. 烏國與地方政府組織 2. 國安與國防部門 3. 銀行金融機構 4. 商業機構 5. 能源部門 6. 其他部門	大規模網路中斷
四	交通 關鍵基礎設施	1. 文尼察國際機場（Vinnytsia） 2. 敖德薩機場 3. 斯韋托戈爾斯克橋樑 4. 馬立波港口 5. 克里米亞大橋	陸海空交通受阻
五	銀行與金融 關鍵基礎設施	1. 烏克蘭國營銀行 Privat bank 2. 烏克蘭儲蓄銀行 Oschad bank	金融交易 大規模中斷
六	緊急救援與醫院 關鍵基礎設施	1. 烏克蘭馬立波（Mariupol）醫院 2. 烏克蘭約 400 家醫療院所	緊急救援 服務中斷
七	中央政府與主要都會 關鍵基礎設施	1. 烏克蘭國防部網站 2. 烏克蘭外交部網站	訊息傳遞受阻
八	高科技 關鍵基礎設施	1. 烏克蘭基輔衛星服務站 2. 烏克蘭數位轉型部網站	重要通信傳播訊息 傳遞受阻

資料來源：作者自行整理。

他山之石，可供借鏡

在戰事發動後，烏國並不像外界預期地被斷網斷訊，反而能號召網路戰士反制俄羅斯駭侵，且透過不間斷地對外傳送戰況，以及進行種種心戰喊話影音，讓俄方未能達到「速戰速決」的作戰目標。

這歸因於近 10 年來俄羅斯對烏克蘭的數次大規模網攻經歷，尤其是 2017 年的「NotPetya」勒索軟體事件，[4] 其攻擊烏國境內私人企業與銀行等，造成數億美元的損失。烏國經此事件成為數位焦土後，烏府痛定思痛，傾盡全力地強化網路防禦能

力，透過中斷對俄能源依賴及在世界各地建立資料庫等方式，成功打造出強大韌性的網路安全系統。[5]

另戰爭一開始，烏國數以百計的中小型網路業者，主動冒著生命危險努力維持網路運作，尤其是當光纖電纜遭俄軍炮火破壞後，該國電信業者儘快搶修恢復通訊的效率，頗令外界印象深刻，所以當俄軍入侵後，烏國網路始終保持暢通，這也讓澤倫斯基能透過視訊對全球喊話，進而得到驚人的外界馳援。加以美國 Space-X 大舉援烏衛星通訊，更是讓烏方得以維持通訊傳輸、發動網攻以及認知作戰攻防的重要利器。[6] 因此，從烏國過去教訓直到發展出強大網路防禦等的相關經驗，實值得我方多加借鏡學習。

美國國際開發署與 Space-X 合作，提供烏克蘭 5,000 個衛星接收終端設備，讓烏方在戰爭中得以維持通訊傳輸。（Source: Mykhailo Fedorov twitter, https://twitter.com/FedorovMykhailo/status/1498392515262746630）

全災害風險管理概念

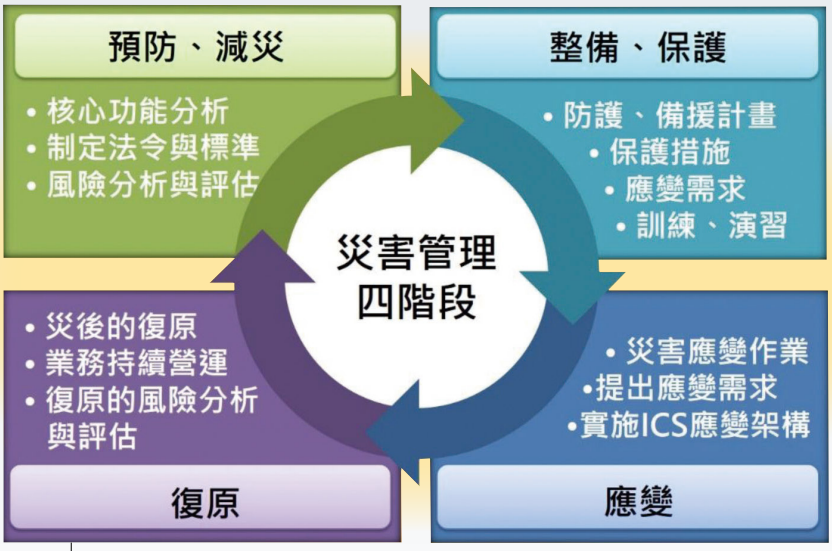
面臨戰爭的嚴峻考驗，須知 CI 防護之災害管理不應只有強調應變或是整備，災害管理政策要能成功推行，必須要完整地考量災害管理的四階段（預防減災、整備保護、應變、復原）全面作為，並互相配合，相輔相成。

換言之，即管理方式事實上與災害類型無關，而是對應各種災害都應該如此處理；且當管理災害方式能跳脫出僅侷限於純粹應變的思維，以災害管理四階段的角度思考—即全災害管理（All-Hazards approach）時，在人、實體及網絡面向上均妥善地加以管理，方可降低各項風險與各類型災害所帶來之危機。

[4] "US charges Russian hackers blamed for Ukraine power outages and the NotPetya ransomware attack", https://techcrunch.com/2020/10/19/justice-department-russian-hackers-notpetya-ukraine/.

[5] 《烏克蘭數位戰全靠他！ 31 歲科技部長花費 2 年強化網路韌性，俄國網軍難以癱瘓》，https://www.storm.mg/article/4258342。

[6] 《俄烏戰事中的網戰攻防、數位韌性與其對全球網路治理之衝擊》，https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1629。



災害管理四階段的全面作為（左）與安全防護的管理要領（右）。（資料來源：行政院國土安全政策會報，《國家關鍵基礎設施防護演習參考手冊》、《國家關鍵基礎設施安全防護指導綱要》，https://ohs.ey.gov.tw/Page/6C4A1386ACBA6734）

我網路安全情勢嚴峻，堪稱首見

8 月 3 日美國眾議院議長裴洛西來臺訪問，中共運用網路攻擊我便利超商、臺鐵、高鐵車站看板，並顯示不雅涉及人身攻擊文字等；另加以入侵我公路總局、台電電網、內政部警政系統、高雄市環保局官網、外交部甚至是國防部網站等，[7] 造成部分網站癱瘓、人心惶惶。此等全面遭入侵攻擊事件，堪稱臺灣首見，亦不輸俄烏戰爭前夕之俄國駭客頻繁入侵烏國網站情節。

然以正面態度觀之，此次中共軍演與駭客攻擊，無疑係對我形成最佳的 CI 安全防護總體檢。另藉由觀察俄烏戰爭的過程，我政府與國人應深刻體認、從中學習，進而發揮災害管理思維，以主動積極態度及早部署與加強數位韌性，方能面對 CI 安全防護的最嚴峻挑戰。

[7] 《臺灣 8 月初因裴洛西訪臺而遭到網路攻擊的事件總覽》，https://www.ithome.com.tw/news/152491。