2025 年中共對我國關鍵基礎設施網駭威脅分析

壹、整體趨勢發展

一、中共對我網駭侵擾逐年上升

2025 年，我國安情報團隊掌蒐重大資安事件，中共對我關鍵基礎設施（**包含政府機關、能源、通訊傳播、交通、緊急救援與醫院、水資源、金融、科學園區與工業區、糧食等 9 大類**）侵擾數平均每日約達 263 萬次，較 2024 年成長 6%（**如圖 1**），顯示中共對我國關鍵基礎設施進行全面性駭侵，伺機干擾或癱瘓我國政府及社會正常運作，以配合平時及戰時對臺發動複合式威脅之戰略需求。

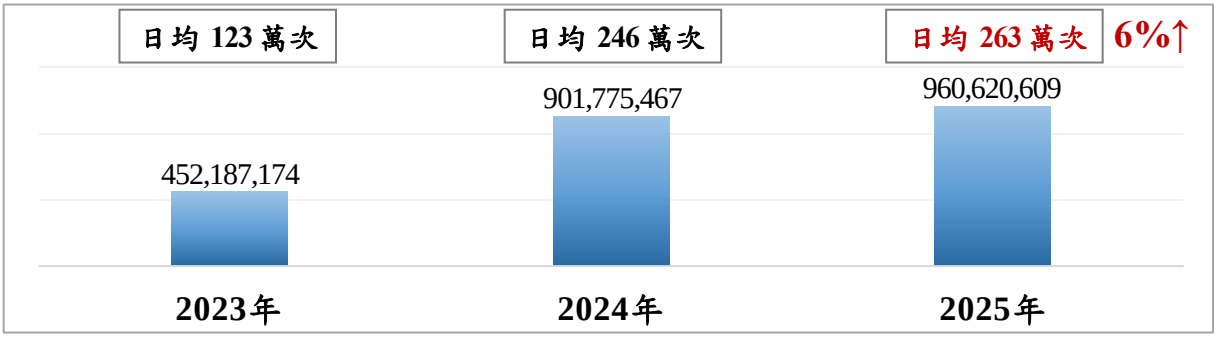

圖 1：2023 至 2025 年我國關鍵基礎設施遭侵擾情形

此外，2025 年中共網軍對我國關鍵基礎設施攻擊，與 2024 相較，以能源、緊急救援與醫院領域增長最為明顯（**如圖 2**）。

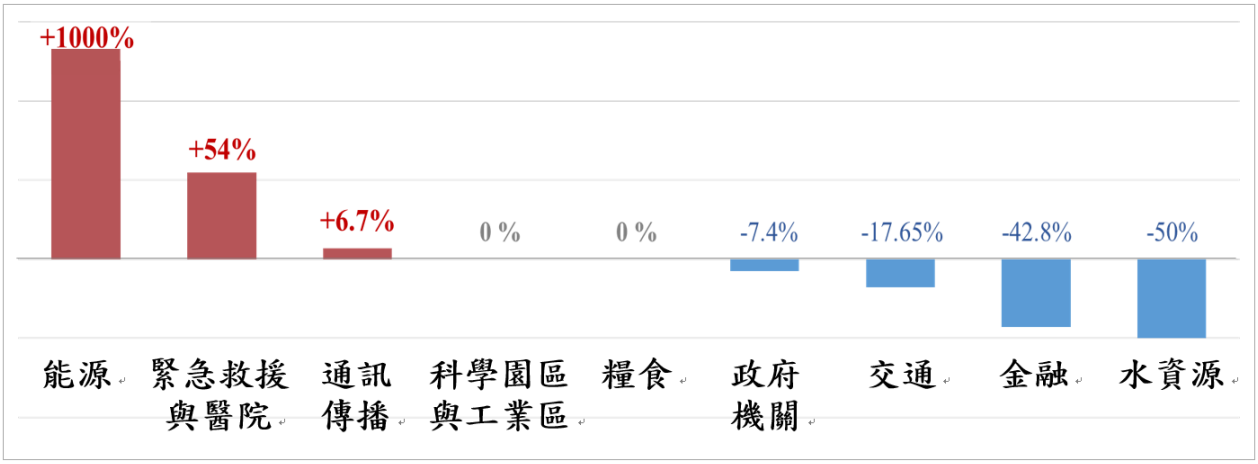

圖 2：2025 年 9 大類關鍵基礎設施遭駭消長圖

二、網駭活動結合政軍施壓

中共對我網駭具政軍施壓特點，2025 年相關網路侵擾活動的時間點，與解放軍對臺「聯合戰備警巡」，具一定程度關聯性，全年共軍對我國進行 40 次「聯合戰備警巡」，其中中共網軍同步配合升高對我國資安侵擾活動共計約 23 次。

另外，在我國重大慶典、政府高層發表重要談話或出訪時，中共亦會升高網路侵駭活動，企圖干擾我政府施政與社會民心，並對我進行複合式威懾，尤在 2025 年 5 月總統就職週年期間到達年度高峰（**如圖 3**）。

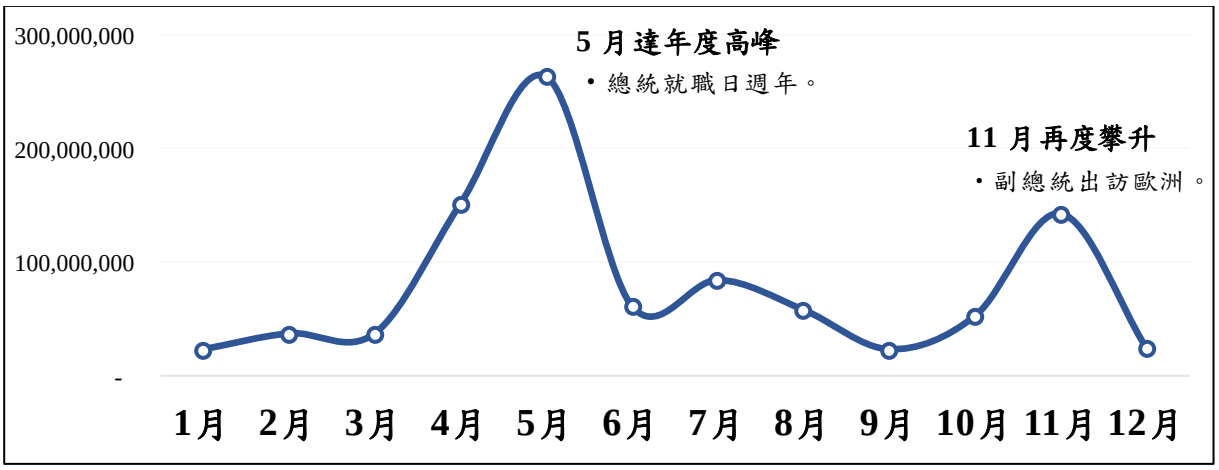

圖 3：2025 年我國關鍵基礎設施遭攻擊情形

貳、駭侵手法與攻擊目標

一、4 大駭侵手法

中共對我國關鍵基礎設施進行網路駭攻，以「軟硬體漏洞攻擊」、「分散式阻斷服務攻擊」、「社交工程攻擊」及「供應鏈攻擊」等 4 大攻擊手法為主，並靈活交錯運用。

（一）**軟硬體漏洞攻擊**：在中共對我網駭手法中，占比超過 5 成（**如圖 4**），反映中共積極蒐集國內產官學界發掘之網路漏洞，並用以擴充「漏洞武器化」（**Vulnerability**

Weaponization）之技術能量。中共持續專研國際資通設備大廠或我政府共約採購之軟硬體漏洞，並鎖定未修補之關鍵基礎設施資通設備，藉以規避使用者身分登入驗證機制，進而取得設備管理權限駭侵竊資。

（二）**分散式阻斷服務攻擊：**中共網軍利用大量「殭屍網路」（Botnet），同時發送高頻次連線服務請求，干擾關鍵基礎設施對外網路運行，造成服務延遲或癱瘓，企圖影響我民生正常運作。

（三）**社交工程攻擊：**中共網軍善於偽裝合作對象往來電郵，誘使特定目標點擊惡意連結、開啟惡意附加檔案，或運用「點擊修復」（ClickFix）手法，假冒錯誤訊息或更新提示等，誘使受駭者執行惡意程式，以伺機取得更高系統權限。

（四）**供應鏈攻擊：**中共網軍亦試圖入侵我關鍵基礎設施供應商及合作企業，透過共用系統、更新機制、設備維護等管道，竊取合法身分掩護非法活動，對關鍵基礎設施進行惡意程式擴散與部署。

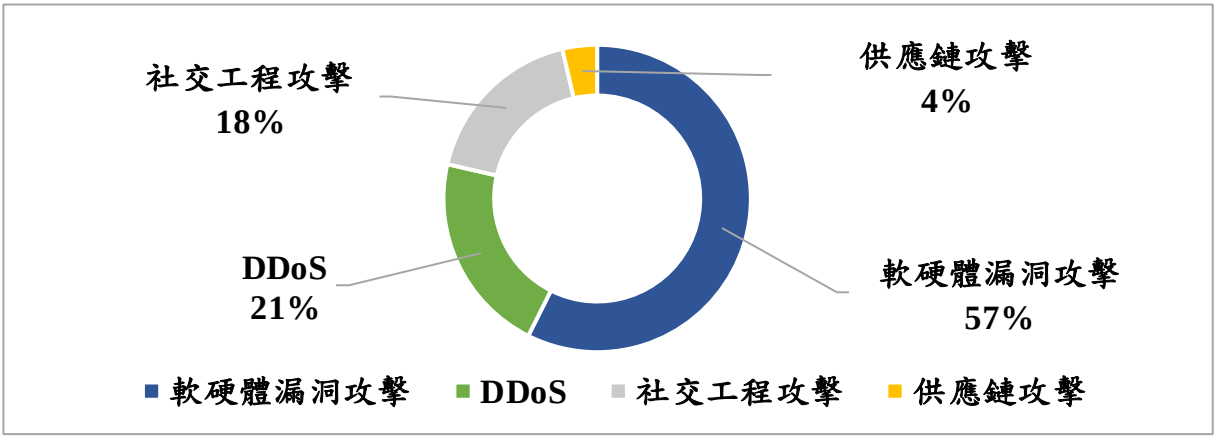

圖 4：2025 年中共對我國關鍵基礎設施攻擊手法占比

二、5 大攻擊目標

中共網軍駭攻我關鍵基礎設施，主要包括 BlackTech（黑

科技）等 5 個駭客組織（如表 1），其攻擊我國關鍵基礎之領域亦有不同。

駭客組織	側重攻擊領域
BlackTech（黑科技）	政府、通訊、科技園區等領域。
Flax Typhoon（亞麻颱風）	緊急救援與醫院、科技園區等領域。
Mustang Panda（野馬熊貓）	政府、能源等領域。
APT41	政府、能源、通訊、緊急救援與醫院、科技園區、交通、水資源等領域。
UNC3886	政府、科技園區等領域。

表 1：2025 年中共對我關鍵基礎設施駭攻之前 5 大駭客組織

(一)能源領域：滲透工控設伏干擾

中共網軍密集探測我國石油、電力、天然氣等公、民營能源公司之網路設備及工控系統；另企圖利用軟體更新時機，對我能源業者暗植惡意程式，目的在掌握我能源產業運作機制、物資規劃及備援部署等營運計畫。

(二)醫療領域：竊取個資勒索傳散

中共網軍持續利用我國大型醫療院所網站系統弱點，以加密勒索軟體妨礙醫院運行，甚或竊取病歷個資、醫療研究成果等相關資訊。2025 年中共網軍將相關醫療機構駭竊資料，在暗網論壇兜售傳散至少 20 次，試圖達到資訊竊獲、經濟牟利與大眾恐嚇等多重目的。

(三)通訊領域：利用漏洞潛伏路由

中共網軍攻擊我國通訊產業網通設備漏洞，意圖潛伏通訊業者及協力廠商電腦系統，再透過「中間人」（**Man-in-the-Middle, MITM**）攻擊模式（**指攻擊者劫持通訊鏈路，且在通訊雙方不知情狀況下，攔截、竄改通訊內容**），從中竊取通訊數

據、用戶資料，以及滲透機敏與備援鏈路，進而伺機影響我國內、外通訊網路安全及韌性。

(四)政府領域：結合時政客製攻擊

中共網軍針對我中央政府特定單位，以高客製化社交工程電郵，偽冒業務交流或提供國際經貿及兩岸情勢報告等名義，並於附檔夾帶惡意程式，誘使目標對象開啟檔案後植入後門竊資。尤在竊資後予以加工改寫，並在暗網及特定論壇傳散，試圖蒐集我政府資訊，同時影響社會大眾對政府資安治理能力之信任。

（五）科技領域：置重晶圓軍工技術

中共網軍除鎖定我國科學園區發動攻擊外，亦駭侵半導體與軍工企業相關之上、中、下游供應廠商（**含設計、製造及測試**）。尤其利用供應鏈攻擊、社交電郵及漏洞滲透等多元手法，從中竊取高新技術、產業規劃與決策情報，謀支援中共自身科技及經濟發展，並避免在美「中」科技競合處於劣勢。

參、結語

2025 年以來，印太國家、北約及歐盟網安機構及情報單位，多次指出中共係全球網路安全威脅主要來源國（**如表 2**）。

時間	國家及組織示警	示警內容
0326	美國情報機構發布《年度威脅評估報告》。	中共是美國最大軍事與網路威脅。
0527	北約及歐盟發布聲明公開聲援捷克應處網駭攻擊。	判捷克關鍵基礎設施係遭中共駭客組織 APT31 攻擊。
0827	美國、英國、加拿大、澳洲、紐西蘭、德國、義大利、日本、荷蘭、波蘭、芬蘭、捷克、西班牙等 13 國 23 個情報與安全機構發布聯合資安公告。	指控中共國家級駭客組織滲透全球關鍵基礎設施與系統。

表 2：2025 年國際示警中共網駭威脅情形

中共已全面結合軍事、情報、產業與科技等公、私部門，透過各種網駭手段與技術，提升對外網攻的穿透性及隱蔽性。面對中共網駭威脅，本局將持續與國安情報團隊、政府相關機關，透由資安聯防及通報機制，即時通報並應處中共對臺駭侵活動。

本局在 2025 年已與全球 30 多個國家推展網安合作，並召開資安對話及技術會議，機先掌握中共網軍攻擊態樣，同時透過跨國資安合作網路，聯合查察惡意中繼站，以襄助政府決策及應變整備，提升我國關鍵基礎設施整體防護韌性及量能。

本局提醒國人重視資安防護，警覺中共對我網駭威脅，共維我國整體網路安全。