2024 年中共網駭手法分析

我國網路空間迭遭中共網軍攻擊、竊資及侵擾，且手法日益翻新，範圍遍及政府、關鍵基礎設施與高科技製造產業等，試圖干擾我政府施政，牟取政治、軍事、科技與經濟利益。

壹、 趨勢發展

一、**威脅趨勢綜況**：依據政府網際服務網「入侵偵測指標」（**IoCs，Indicators of Compromise**）統計，我政府網際服務網 2024 年每日平均侵擾數為 240 萬次，較 2023 年日平均侵擾數 120 萬次增加逾 2 倍（**如圖 1**），且多數為中共網軍所為，雖多已有效偵阻，惟仍凸顯整體網駭侵擾態勢愈趨嚴峻。

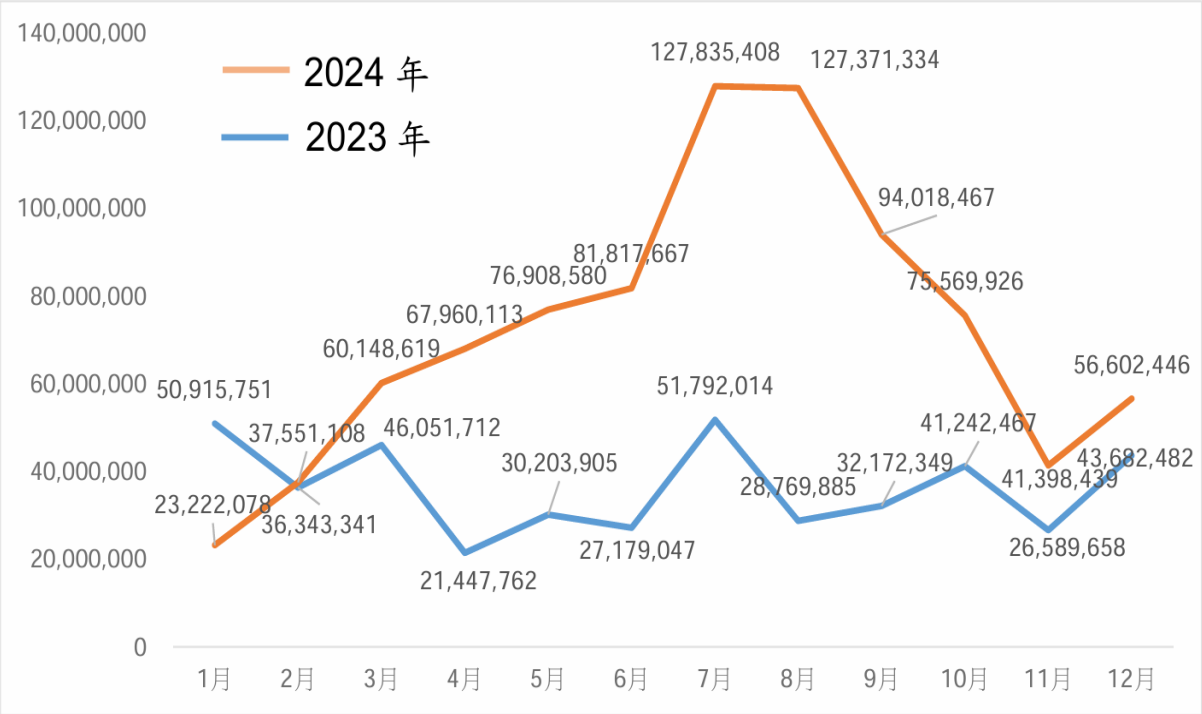


圖 1：2023 年-2024 年網駭威脅統計比較

二、**網軍駭侵目標**：2024 年國安情報團隊掌握我國政府及民間網駭案件計 906 案，相較 2023 年 752 案，增長比率逾二成，其中以政府機關比率最高，占整體總數逾八成。另分析中共網軍駭攻目標，以通訊傳播領域（**650%，主要為電信業**）、交通（**70%**）及國防供應鏈（**57%**）增長最為顯著，顯見該等領域已成為中共新興網駭重點（**如圖 2**）。

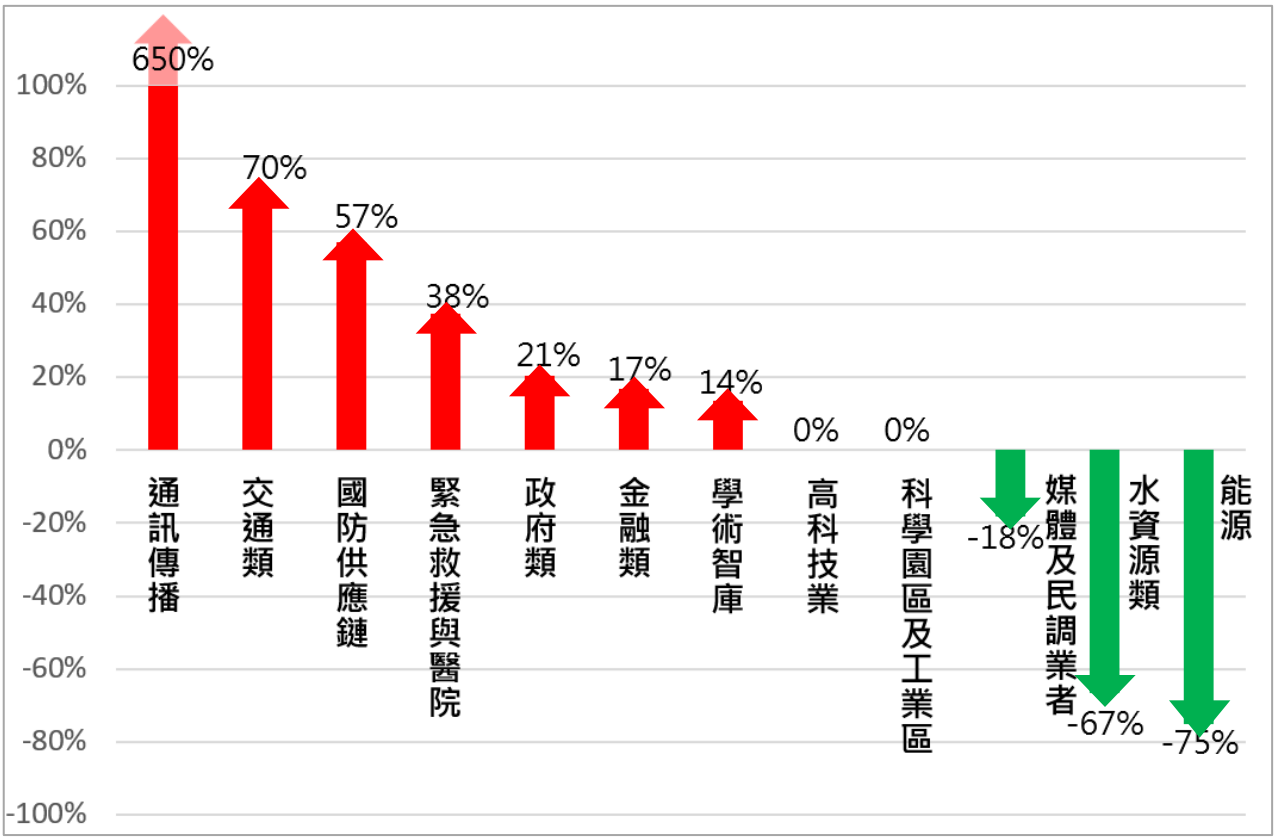


圖 2：2023 年-2024 年各領域遭網駭消長圖

貳、駭侵手法

一、**鎖定政府公務部門**：中共網軍鎖定我政府機關網通設備漏洞設伏竊資，以「離地攻擊」（**Living off-the-land**）手法，躲避網防系統偵察。如中共網軍利用電郵伺服器漏洞，對我政府機關發動駭侵，另針對我公職人員電子郵件，發動社交工程等攻擊，企圖竊取機敏資訊。

二、**瞄準資服業者及國防供應鏈**：中共網軍以多元手法對我國防供應鏈及資服業者駭侵竊資，尤側重電郵、公文書系統、密碼產製及差勤系統等供應商，並擴大攻擊範圍。

三、**設伏關鍵基礎設施**：中共網軍透過進階持續性滲透、釣魚郵件、零時差漏洞、木馬病毒、後門程式等手段，企圖駭攻設伏我公路、港務等關鍵基礎設施，謀影響我國交通運輸秩序。

四、**採取軍民融合犯罪手法**：中共結合民間駭客協力組織，運用勒索軟體等網路犯罪手法，對我製造業廠商遂行駭攻，獲取經濟利益。刑事局近期掌握中共駭侵部分學研單位，進行密碼破解，修改市話系統設定（**增加發話功能**），轉供電話詐騙使用。

五、**運用網駭匿蹤與暗網揭露**：中共以網駭手段竊取我國人個資，並於暗網及駭客論壇公開販售獲利，遂行「駭侵及洩漏」（**Hack & Leak**），同時藉由社群網路論壇發文批評網防不力，打擊我國家威信。

六、**結合軍演與網路襲擾**：中共網軍藉對臺軍演時機，結合網攻部署，包括利用邊緣網通設備，對我交通、金融等基礎設施，發動「分散式阻斷服務攻擊」（**DDoS**），期強化騷擾效果，擴大軍事威懾。

七、**部署新創產業竊取科技**：中共亦對各國高科技新創產業竊取專利技術，以獲取競爭優勢。思科公司（**Cisco**）2020 年曾告警，中共駭客組織（**APT41**）藉知名網通設備等公司（**Citrix 及 Cisco**）產品漏洞，攻擊全球企業，企圖竊取該等公司內部機敏技術資訊。

八、**構建全球匿蹤駭攻網路**：中共藉我物聯網（**IoT**）設備密碼漏洞進行駭侵，控制該等設備並進行加密串聯，組建匿蹤網路（**或稱殭屍網路**）遂行網攻活動。

參、結語

中共持續加大對我網路攻勢，並結合多元網路駭侵手法，對我政府、關鍵基礎設施及重要民企，進行偵查設伏及網駭竊資。我國政府透過資通安全聯防機制，運用多元情報來源管道，掌蒐網安威脅預警情資，即時分享權責部門應處；同時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。