網路戰的應用與未來發展趨勢—以烏俄戰爭為例

作者/陳明薇

提要

一、自2022年烏俄戰爭開打以來，至今有關戰爭的畫面及新聞不斷地透過網路傳遞而來，而這場戰爭也被稱為「無煙硝的戰爭」或「非砲火的戰爭」。

二、歷年來俄羅斯透過各式各樣的網路攻擊手段，並結合駭客組織勢力試圖破壞烏克蘭政府機構、基礎設施及電信網路等，而烏克蘭如何應對挑戰及可能衍生的資訊安全威脅加以探討。

三、國軍面臨共軍網路作戰能力日益增強及嚴峻軍事威脅之下，不對稱戰略的網路運用作為，是我國刻不容緩之議題，本文以烏俄戰爭為例，探討網路戰應用與未來發展趨勢，進而對我國網路戰提出具體建議。

關鍵詞：烏俄戰爭、網路戰、資訊安全、駭客組織

前言

烏克蘭和俄羅斯皆認為基輔羅斯是他們國家歷史的起源，自 1991 年蘇聯解體後，兩國雖於文化和經濟上都有密切往來，然俄羅斯認為烏克蘭在邊境擴展，對國家安全構成威脅，2014 年俄羅斯併吞克里米亞後，兩國關係急遽惡化，無論是地緣、政治、經濟以及民族文化等，多重因素導致爆發一場至今仍未結束的現代戰爭。

「網路戰」被視為現代戰爭中的前哨戰，運用誤導、複雜、阻擋、封鎖等手段，破壞通資指管中樞，導致對方無法動用武器，陷入「耳不聰、目不明」的劣勢，達到不戰而屈人之兵的效果，是一種新興的戰爭型態。

2022 年 2 月 23 日俄羅斯進攻烏克蘭邊界前一日就已揭開序幕，烏克蘭遭到前所未有的惡意軟體襲擊，俄羅斯鎖定烏克蘭政府機構、基礎建設、銀行資訊系統等進行破壞及竊取內容，而烏克蘭如何抵制網路攻擊與堅守不退的攻防作為，值得同樣面臨共軍網路作戰能力日益增加及嚴峻軍事威脅之下的我國借鏡。

本研究以「烏俄戰爭網路戰」作為主體，首先從烏俄兩國網路部隊特性及歷經的網路攻擊事件開始，其次針對網路戰運用手段探討，最後對我國提出發展策略與具體建議，以利未來網路建軍備戰之參考。

網路戰定義

「網路戰」通常被定義為針對一個國家的網路和系統進行一系列攻擊，導致目標機構和民生基礎設施嚴重破壞，[1]尤其是關鍵系統，導致被入侵的國家整體損害，甚至是造成生命損失，長久以來，網路攻擊一直被視為灰色地帶的衝突，是否符合戰爭行為的定義在國際法上存在爭議。

烏俄戰爭中，俄羅斯對烏克蘭基礎設施的入侵行為包括政府、銀行、能源系統、核能、電信業和衛星通訊系統的破壞，烏克蘭官方表示，這些導致關鍵民用服務中斷的網路攻擊應被定義為戰爭罪，並希望聯合國修改對「侵略」的法律定義，將「使用網路武器」納入其中，對此，烏克蘭也著手蒐集俄羅斯駭客網路攻擊的紀錄，擬提交給海牙國際刑事法院（International Criminal Court，ICC），作為俄羅斯犯下戰爭罪的證據。[2]

俄羅斯對網路作戰定義為在資訊領域的攻擊和防禦活動，包括位於網際網路環境的電腦對抗是「資訊戰」[3]形式之一，並認為基於網際網路的攻擊有以下數種形式，包含利用駭客通過網際網路用侮辱性或者煽動性的評論修改敵方網頁內容，此類言論傳送或是在其他網頁之內容中設置宣傳內容、入侵私人網頁或者伺服器以獲得機密資訊，或者將機密資訊替換成虛構，對其有利的訊息等方式。[4]

國軍「網路戰」定義係運用電腦系統、網際網路或通信網路之網路空間，藉網路情蒐等手段，獲取軍事所需情報，並掌握敵系統弱點，適時對敵實施破壞、阻絕、衰退或摧毀存在於電腦與網路空間上之資訊，甚至是電腦及網路空間本身的相關作為，以達成軍事目的。[5]

綜上所述，本研究將網路戰定義為可由國家或非國家(駭客組織)在網路空間，所採取的行動構成系統、設施或國家安全威脅之行為，輕則造成停擺、癱瘓或控制目標，重則影響社會、經濟或整個國家。

---

1 張玲玲，〈強化網路戰力 肆應新型態戰爭〉，《青年日報》，民國111年9月4日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1530306&type=forum，檢索日期2024年10月31日。

2 戴匡，〈俄羅斯網攻烏克蘭態勢分析及其啟示〉，《財團法人臺灣網路資訊中心》，民國112年4月24日，https://blog.twnic.tw/2023/04/24/26460/，檢索日期2024年10月31日。

3 「資訊戰為尋求在軍事及商業領域獲得優勢，採取攻擊及防禦之手段，使用計算機科學與資訊系統來利用、誤導以及摧毀敵人之資訊系統，同時亦保護自己之相關系統。」林宜昌，〈資訊戰對國軍防衛作戰重要性之研究〉，《海軍學術雙月刊》，第53卷第6期，頁117。

4 黃郁文，〈淺析俄羅斯「網路戰」-以2022年「俄烏戰爭」運用為例〉，《海軍學術雙月刊》(臺北中山)，第56卷第4期，海軍司令部，民國111年8月，頁90-91。

5 國防部，〈聯合作戰網電教則〉，民國111年12月8日，頁3-34。

烏俄戰爭網路戰應用與發展

一、烏克蘭與俄羅斯網路部隊特性

烏克蘭政府在戰爭初期就成立了「IT Army」，招募了許多志願者進行反擊，[6]利用全民國防力量，結合地方組織組成網路部隊，而俄羅斯為軍事機構編制，並下轄數個駭客組織進行網路行動，針對兩國網路部隊分述說明如下：

(一)烏克蘭網路部隊概述

烏克蘭政府與來自世界各地的駭客於2022年2月26日組成「烏克蘭資訊科技軍」（IT Army）」，由烏克蘭副總理米哈伊洛·費多羅夫(Mykhailo Fedorov)領導，[7]目標包括俄羅斯的基礎設施、政府機關、社群平台及各類民用電信服務業者，可以同時攻擊800個目標，實施有效的分散式阻斷服務（distributed denial-of-service, DDoS）[8]攻擊和防禦行動，入侵敵方網站和關鍵基礎設施(含管控系統)、建立釣魚網站及散播病毒，並進行網路間諜活動，對俄羅斯經濟和其他公共領域造成嚴重破壞，[9]且於官方網站宣達使命：「通過削弱侵略國家的經濟、干擾重要金融、基礎設施和政府服務的運作，將烏克蘭帶向勝利，並阻止敵方媒體宣傳，向他們人民傳達有關戰爭真相，希望侵略國家的居民都感受到他們國家正在進行之行為感到羞愧」。[10]

烏克蘭電腦緊急應變團隊（Computer Emergency Response Team of Ukraine，簡稱CERT-UA），隸屬於烏克蘭國家特殊通訊和資訊保護服務局，負責蒐集和分析網路事件、預防和偵測網路行為，並協助國家機構、軍事組織、企業等解決網路保護問題和應對網路威脅。[11]

(二)俄羅斯網路部隊概述

俄羅斯在其軍事安全單位架構下建立數個網路戰部隊，且經常針對共同目標執行任務，包含情報單位及駭客組織(如圖1)，分述說明如下：

1.俄羅斯網路戰之情報單位

---

6 〈俄烏戰爭周年回顧：俄羅斯網攻烏克蘭態勢分析及其啟示〉，《財團法人臺灣網路資訊中心》，西元2022年4月24日，https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1602，檢索日期2024年10月31日。

7 〈Ukraine war: Ukrainians announce the launch of an 'IT army' to fight off Russian cyberattacks〉，《euronews.next》，西元2022年2月27日，https://web.archive.org/web/20220424182133/https://www.euronews.com/next/2022/02/26/ukraine-war-ukrainians-announce-the-launch-of-an-it-army-to-fight-off-russian-cyberattacks，檢索日期2024年10月31日。

8 分散式阻斷服務（DDoS）攻擊是一種惡意嘗試，它利用大量的互聯網流量使目標伺服器或其周圍的基礎設施不堪重負，從而阻斷目標伺服器、服務或網路的正常流量。〈什麼是 DDoS 攻擊？〉，《Cloudflare》，https://www.cloudflare.com/zh-tw/learning/ddos/what-is-a-ddos-attack/，檢索日期2024年10月31日。

9 蕭長展，〈烏克蘭民間這樣做使俄軍付出代價：資訊科技力、破壞活動、訴諸國際〉，《WATchout》，西元2023年11月29日，https://watchout.tw/forum/IgH2vEjDy491NUfUlilM，檢索日期2023年12月22日。

10《IT ARMY OF UKRAINE》，https://itarmy.com.ua/，檢索日期2024年10月31日。

11〈Про CERT-UA〉，《Державні сайти України》，https://cert.gov.ua/about-us，檢索日期2024年10月31日。

(1)總參謀部「主要情報局」(Main Directorate of the Armed Forces)，以下簡稱GRU)，隸屬於俄羅斯武裝部隊總參謀部(前身為情報總局)，向國防部長和總參謀長報告，是最具破壞性的網路攻擊單位，由「54777部隊」及「網路特種技術中心」組成，下轄「26165部隊」、駭客組織「APT28」、「74455部隊」及「Sandworm」。

(2)「聯邦安全局」(Federal Security Service，以下簡稱FSB)，直接隸屬於俄羅斯總統，前身為俄羅斯聯邦反情報局(FSK)，負責俄羅斯內部安全及反情報，由「71330部隊」、「64829部隊」及駭客組織「Gamaredon」組成。

(3)「對外情報局」(Foreign Intelligence Service，以下簡稱SVR)，直接隸屬於俄羅斯總統，主要負責關於境外網路攻擊的情報蒐集，並與主要情報局(GRU)合作，下轄駭客組織「APT29」。

(4)「聯邦警察局」(Federal Protective Service，以下簡稱FSO)，直接隸屬於俄羅斯總統，由總統安全局、特種通信局及網路安全單位組成，負責保護政府單位、人員及通信安全。[12]

圖1 俄羅斯情報單位組織架構圖

資料來源：作者整理

12〈俄羅斯網軍研究簡報〉,《安全內參》，西元2021年1月6日，https://www.secrss.com/articles/28510，檢索日期2024年10月31日。

2.俄羅斯主要駭客組織(如表1)

(1)「APT28」也稱為Fancy Bear、STRONTIUM、Pawn Storm、Sednit Gang 和 Sofacy，歸屬俄羅斯總參謀部主要情報局(GRU)，編號由美國網路安全公司(FireEye)針對威脅行為或攻擊目標等提出命名，相較於一般駭客組織，進階持續性攻擊Advanced Persistent Threats(APT)組織更有策略與長遠的目標，通常由國家龐大資源支撐。

表 1 俄羅斯主要駭客組織表

駭客名稱	別名	成立時間	隸屬單位	主要攻擊目標
APT28	FancyBear、STRONTIUM、Pawn Storm、Sednit Gang 和 Sofacy	2004年	主要情報局(GRU)	軍隊、政府
Turla	Venomous Bear、Snake、Group 88、WhiteBear、Waterbug 及 Uroburos	2004 年	俄羅斯	政府、大使館、軍隊、教育、研究和製藥公司
APT29	Dukes、Cozy Bear	2008年	對外情報局(SVR)	政府、科技、電信、製藥
Sandworm	Telebots、Voodoo Bear、Iron Viking	2009 年	主要情報局(GRU)	政府、能源部門和關鍵基礎設施
Gamaredon	Armageddon、Shuckworm、Actinium	2014 年	聯邦安全局(FSB)	政府、軍隊及非營利組織

資料來源：作者整理。

知名APT組織計有「APT35」、「APT37」、「APT41」等駭客組織(如表2)，「APT28」經常在歐美國家進行，且以濫用「零時差漏洞」(0-day vulnerability、zero-day、vulnerability)[13]進行網路間諜活動，且於2021年10月利用基礎設施假

13零時差漏洞或零日漏洞（0-day vulnerability、zero-day vulnerability）是指軟體、韌體或硬體設計當中已被公開揭露但廠商卻仍未修補的缺失、弱點或錯誤。〈什麼是零時差漏洞 (Zero-Day Vulnerability)? 有哪些漏洞攻擊手法?〉，《趨勢科技》，西元2019年12月26日，https://blog.trendmicro.com.tw/?p=62238#more-62238，檢索日期

冒SNMP攻擊全球的思科路由器，其中大約250台路由器位於烏克蘭。[14]

表 2 知名進階持續性攻擊 Advanced Persistent Threats (APT)組織表

駭客名稱	隸屬地區	主要攻擊目標
APT28	俄羅斯	政府、國防、金融、航太
APT29	俄羅斯	政府、私人資訊
APT35	伊朗	政府、能源、科技
APT38	北韓	金融機構
APT41	中共	醫療、通訊、科技、電競遊戲

資料來源：作者整理。

(2)「Turla」也稱為Venomous Bear、Snake、Group 88、WhiteBear、Waterbug及Uroburos，從2004年開始活躍至今，為網路間諜組織以隱密戰術而聞名，與進階持續性滲透攻擊(APT)組織一樣擁有專屬複雜工具，以攻擊全球各地的政府機關、情報單位、軍事、教育、研究與醫藥產業，相較於其他駭客組織特別之處，攻擊後期使用衛星通訊幕後操蹤(C&C)機制與躲避偵測能力，攻擊全球各地政府機關、情報單位、軍事、教育、研究與醫藥產業，於2023年7月烏克蘭電腦緊急事件應變團隊(CERT-UA)，揭露 Turla 正在使用Capibar 惡意程式和 Kazuar 後門程式[15]對烏克蘭的國防設施發動間諜行動。[16]

(3)「APT29」也稱為Dukes、Cozy Bear，歸屬俄羅斯對外情報局(SVR)，主要目標針對政府機構、外交部門、醫療保健和能源系統來獲取情報，且於

2024年10月31日。

14〈APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers〉，《National Cyber Security Centre》，西元2023年4月18日，https://www.ncsc.gov.uk/news/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers，檢索日期2024年10月31日。

15CAPIBAR 惡意軟體(也稱為 Delivery Check 或 GAMEDAY)，應用 XSLT 語言和 COM 劫持，並可以透過特定的 PowerShell 實用程式偽裝成 MOF 檔案安裝在受感染的 MS Exchange 伺服器上，使攻擊者能夠將合法伺服器轉變為遠端惡意軟體管理工具；KAZUAR 後門程式能夠執行數十種惡意功能，包括透過 Chakra Core 啟動 JavaScript 程式碼、從作業系統登錄中收集事件日誌、憑證竊取(例如竊取使用者密碼、cookie、書籤和其他敏感資料)或竊取資料庫和軟體設定檔。〈CAPIBAR and KAZUAR Malware Detection: Turla Aka UAC-0024 or UAC-0003 Launches Targeted Cyber-Espionage Campaigns Against Ukraine〉，《SOC Prime》，https://socprime.com/blog/capibar-and-kazuar-malware-detection-turla-aka-uac-0024-or-uac-0003-launches-targeted-cyber-espionage-campaigns-against-ukraine/，檢索日期 2024 年 10 月 31 日。

16〈檢視 Turla APT 集團的活動〉，《Trend Micro》，西元2023年12月12日，https://www.trendmicro.com/zh_tw/research/23/i/examining-the-activities-of-the-turla-group.html，檢索日期2024年10月31日。

2020年以加拿大、美國和英國參與 COVID-19 疫苗開發的各種組織作為目標，意圖竊取與 COVID-19 疫苗開發和測試相關的資訊和智慧財產權。[17]

(4)「Sandworm」也稱為沙蟲，歸屬俄羅斯總參謀部主要情報局(GRU)，其製造的惡意軟體破壞力強，早在2022年6月之前，該組織就對烏克蘭實施網路入侵，透過「虛擬機管理程式」（Hypervisor）[18]取得變電站的「監控與資料擷取系統」（SCADA），進而控制「操作型科技系統」（OT），潛伏數個月之後，啟動已入侵電腦的惡意程式破壞「工業控制系統」（ICS），導致斷路器異常，爆發大規模停電。[19]

(5)「Gamaredon」也稱為Armageddon、Shuckworm、Actinium，根據美國安全公司(LookingGlass Cyber Solutions)報導了一場名為「世界末日」的活動，發現攻擊中使用多個Microsoft Word 文件，在文件的「最後保存者」和「作者」欄位中發現了「Armagedon」一詞（拼字錯誤的Armageddon），[20]這成為了該駭客組織的命名基礎，且微軟表示該組織早在2021年10月開始，已針對烏克蘭發動網路釣魚攻擊，包括政府、軍隊及非營利組織等。[21]

(三)小結

綜上所述，俄羅斯擁有龐大的網路部隊，包括政府資助的前台公司、被國家監視的私人企業、網絡犯罪分子和「愛國駭客」等，[22]長期進行資訊、宣傳、間諜和網路攻擊活動，且鎖定、癱瘓烏克蘭網站及重要戰略系統等目標。

烏克蘭政府面對俄羅斯的入侵過程，展現了卓越的應對能力和創新的解決方案，正式將「IT Army」納入後備網路部隊，由退伍的資訊科技技術人員及民間組織組成，在國家面臨網路威脅或衝突時，可以接受動員為國家保衛安全，這也顯示烏克蘭計畫將駭客力量制度化，並納入正式的軍事編制。

17〈APT29 targets COVID-19 vaccine development〉,《National Cyber Security Centre》, 西元2020年7月16日, https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development, 檢索日期2024年10月31日

18虛擬機管理程式(Hypervisor)可以用在單一實體機器上執行多個虛擬機器，每個虛擬機器都有各自的作業系統和應用程式，根據需要將基礎實體運算資源(例如CPU和記憶體) 配置給個別的虛擬機器。〈什麼是 Hypervisor?〉,《Amazon Web Services》, https://aws.amazon.com/tw/what-is/hypervisor/, 檢索日期2024年10月31日。

19汪哲仁,〈網攻威脅全球基建 資安防護刻不容緩〉,《青年日報》, 西元2023年11月22日, https://www.ydn.com.tw/news/newsInsidePage?chapterID=1631396, 檢索日期2024年10月31日。

20Eduard kovacs,〈 “Gamaredon” Group Uses Custom Malware in Ukraine Attacks〉,《SECURITYWEEK》, 西元2017年2月28日, https://www.securityweek.com/gamaredon-group-uses-custom-malware-ukraine-attacks/t, 檢索日期2024年10月31日。

21Sergiu Gatlan,〈Russian FSB hackers hitting Ukraine since October〉,《BLEEPINGCOMPUTER》, 西元2022年2月4日, https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development, 檢索日期2024年10月31日。

22〈Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior〉,《Atlanatic Council》, 西元2022年9月19日, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/, 檢索日期2024年10月31日。

二、烏俄戰爭網路戰事件概述

2014 年克里米亞衝突透過「NotPetya」惡意軟體及沙蟲侵略烏克蘭網站等網路攻擊事件，延續至 2022 年烏俄戰爭爆發前大規模分散式服務阻斷攻擊，2023 年則以癱瘓或破壞電力及電信等重要設施運作為主，因應各時期事件及發展，將其重點概略區分如下(如表 3)：

表 3 俄羅斯網路攻擊事件統計表

發生時間	事件名稱	攻擊型態	目標	影響範圍
2014 年	克里米亞西衝突	NotPetya	政府機構、銀行、郵局及支付系統。	併吞烏克蘭克里米亞半島。
2017 年	勒索軟體攻擊	NotPetya	烏克蘭近 1.3 萬台 IT 裝置、政府機構、銀行、郵局、報社、運輸及商業界。	電腦硬碟資料遭刪除或形成加密檔無法複製使用。
2021 年 7 月	海風 2021 攻擊	惡意軟體和假消息	烏克蘭海軍網站。	表達對黑海國家和北約盟國及合作夥伴參與「海風 2021」軍事演習不滿，並散播假消息。
2022 年 1 月	警告訊息攻擊	DDoS	烏克蘭外交部、國家安全與國防事務委員會等 70 個網站。	網站無法連線，停滯數小時後才恢復。
2022 年 2 月	雨刷攻擊	DDoS、Wiper	軍事、銀行網站。	以烏克蘭為主要區域，但迅速蔓延到美洲、歐洲和亞洲。
2022 年 11 月	斷電攻擊	DDoS	關閉變電所、破壞基礎設施。	烏克蘭大規模停電。
2023 年 5 月	斷網攻擊	Poemgate Poseidon Whitecat	烏克蘭 11 家網路和電信供應商。	導致烏克蘭數小時網路服務中斷。
2023 年 12 月	斷網攻擊	DDoS	烏克蘭最大電信業者 Kyivstar。	導致 Kyivstar 用戶數日沒有行動訊號和網路。

資料來源：作者整理。

(一)烏俄兩國衝突期間(2014 至 2021 年)：

1.克里米亞衝突

2014年俄羅斯以保護本國人民為由，結合當地勢力佔領與逕自宣布併吞克里米亞，並大力展開對烏克蘭的攻勢，遂引發克里米亞衝突危機，以漏洞檢測工具「Mimikatz」[23]竊得憑證，並透過「NotPetya」惡意軟體，使烏克蘭的政府機構、銀行、郵局及支付系統均受到嚴重打擊。

2.勒索軟體攻擊

2017年一種在許多方面類似於「Petya」的新型勒索軟體，網路安全公司(Kaspersky)將其稱為「NotPetya」，也有其他公司稱為「Petya 2.0」或「ExPetr」，該軟體透過遠端控制工具在電腦上執行惡意程式，受感染的文件將被完全清除(如圖2)，影響了世界各地包含美國、英國及德國等至少2,000個組織，國家銀行及民生大型基建行業無一倖免，而絕大多數受害組織都在烏克蘭。[24]

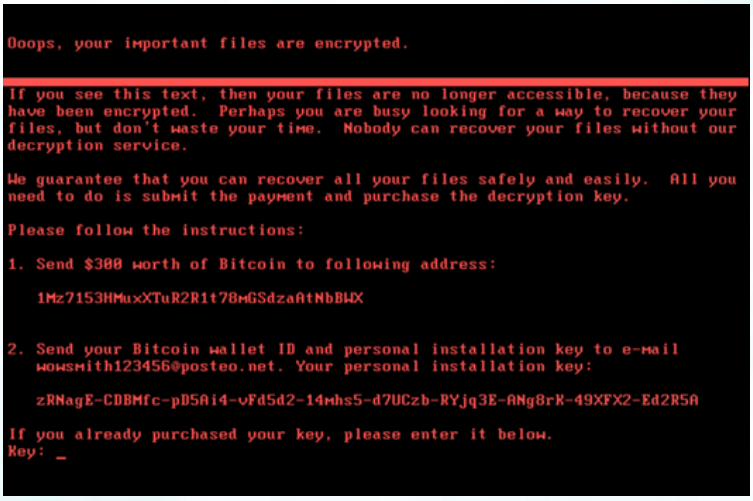

圖2 NotPetya勒索軟體警告訊息畫面

資料來源：〈NotPetya〉，《HYPR》，https://www.hypr.com/security-encyclopedia/notpetya，檢索日期2024年2月18日。

3.海風2021攻擊

2017年7月烏克蘭和美國在黑海舉辦年度多國聯合海上演習，俄羅斯公開要求取消該演習，數日後烏克蘭國防部表示，海軍網站遭俄羅斯入侵。

(二)烏俄戰爭開戰初期(2022 年)：

23Mimikatz原先是用來測試Windows安全性的小工具，可搜刮密碼、雜湊碼、PIN碼與Kerberos票證。趨勢科技，〈上膛的武器落入壞人中：合法工具變成勒索病毒的超級武器〉，《資安趨勢部落格》，西元2021年6月2日，https://blog.trendmicro.com.tw/?p=68278，檢索日期2024年10月31日。

24〈什麼是 Petya 與 NotPetya？〉，《Cloudflare》，https://www.cloudflare.com/zh-tw/learning/security/ransomware/petya-notpetya-ransomware/，檢索日期2024年10月31日。

1.警告訊息攻擊

2022年1月烏克蘭外交部、教育部及當地政府等70個網站遭大規模網路攻擊，網站上顯示烏克蘭語、俄語和波蘭語威脅警告訊息(如圖3)，如「烏克蘭!你的所有個人資料已上傳到公共網路，電腦裡所有資料將被銷毀且無法恢復」和「準備迎接最糟糕的情況吧，這是為了你的過去、現在和未來」。[25]

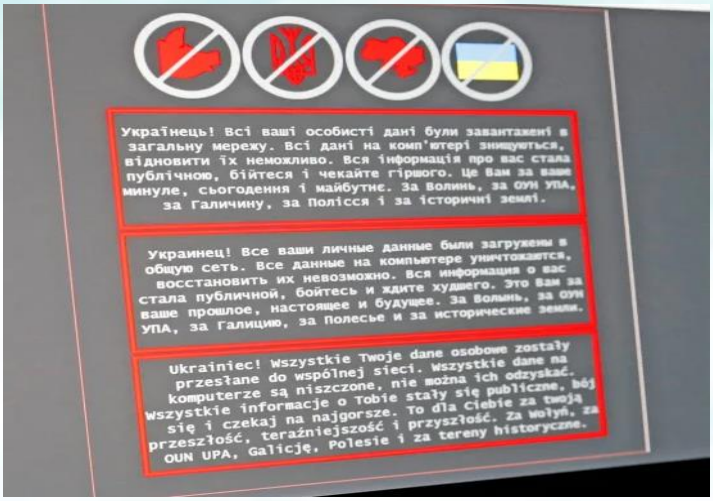

圖3烏克蘭語、俄語和波蘭語警告訊息畫面

資料來源：同註 25。

2.雨刷攻擊

2022年2月俄羅斯透過「DDoS」與「Wiper」破壞烏克蘭政府、銀行網站等，遭入侵的系統將無法正常使用，「Wiper」中文名為雨刷或擦拭器，透過系統漏洞或電子郵件攻擊，感染目標後刪除或毀損系統上的文件和資料。

3.斷電攻擊

2022年11月俄羅斯利用潛伏已久的「DDoS」與飛彈攻擊，透過打擊能源基礎設施，造成數百萬烏克蘭人民無電可用。

(三)烏俄戰爭開戰期間(2023 年)：

2023年兩件重大網路攻擊均為斷網攻擊，5月根據烏克蘭CERT-UA報告，俄羅斯駭客組織Sandworm針對烏克蘭至少11家網路和電信供應商發動攻擊，造成服務中斷數10小時，另使用Poemgate和 Poseidon竊取憑證並控制受感染的設備及Whitecat [26]來刪除任何取證痕跡。[27]

25Katharina Krebs、Jake Kwon，〈Cyberattack hits Ukraine government websites〉，《CNN》，西元2022年1月14日，https://edition.cnn.com/2022/01/14/europe/ukraine-cyber-attack-government-intl/index.html，檢索日期2024年10月31日。

26POEMGATE 是一個惡意模組，使用該模組靜態密碼進行身份驗證，並將身份驗證期間輸入的登入名稱和密碼

另12月烏克蘭最大電信供應商Kyivstar遭到重大網路攻擊，導致數百萬人無法使用手機和網路，而在烏克蘭更換到另一家電信供應商很容易，使許多人因工作等因素選擇使用其他電信供應商，間接造成Kyivstar營運損失。[28]

(四)小結

上述多起網路攻擊事件，歸納出過往俄羅斯針對烏克蘭之網路攻擊著重在電腦及資料破壞，企圖造成軍(民)網站及系統癱瘓，隨著烏俄兩國實體戰爭開打，網路空間的戰況更加激烈，俄羅斯以大量分散式阻斷服務攻擊烏克蘭各大網站，並散布警告訊息結合輿論戰與破壞電信、電力機房運作，企圖造成民眾恐慌，達成混合戰之策略，開戰期間則以斷網攻擊為重，阻斷烏克蘭軍隊及人民從網路、電視、廣播獲得資訊及宣傳效果。

俄羅斯看似擁有強大的網路部隊及駭客組織於戰爭中佔極大優勢，然烏克蘭確能長時間續戰及反制，並於各地持續提供網路服務，尤其是主要城市基輔，如何應處網路攻擊與防範作為值得我國探討。

烏俄戰爭網路戰手段探討

一、網路空間與法律規範

依照《聯合國憲章》的規定，在一個國家境內發生的武裝衝突中，使用武力不被視為非法行為，故俄羅斯從 2014 年克里米亞事件開始，便以保護國家人民為由，對烏克蘭發動武裝及無數次大規模網路攻擊，而烏克蘭透過國際社會宣傳自己的立場和行動，並不斷強調俄羅斯的侵略行為，維護自身領土完整和主權。

二、軍、民合作培育人才

自烏俄戰爭爆發以來，俄羅斯軍事、情報和政府機關與駭客組織建立了合作關係，共同擴張網路行動與資訊作戰能力，目的在於利用最小的成本達成極大影響力，並搭配武裝部隊展開一連串攻勢，烏克蘭則善用民間資源，使民眾產生抗敵意志並組成「IT Army」，運用社群媒體的力量號召全球駭客加入組織，

以 XOR 編碼形式保存在檔案中；Poseidon 是一個 Linux 後門程式，支援全系列的遠端電腦控制工具；Whitecat 是一個網路攻擊工具，可以干擾網路設備以及資料儲存系統。〈Russia-Linked APT Group Sandworm Has Hacked Eleven Telecommunication Service Providers in Ukraine between May and September 2023〉，《Securityaffairs》，https://securityaffairs.com/152617/apt/sandworm-ukraine-telecommunication-service.html，檢索日期 2024 年 10 月 31 日。

27Daryna Antoniuk，〈Russia’s Sandworm hacking unit targets Ukrainian telecom providers〉，《The Record》，西元2023年10月18日，https://therecord.media/russia-sandworm-hacking-ukraine-telecom-internet-providers，檢索日期2024年10月31日。

28Daryna Antoniuk，〈Ukraine's largest telecom operator shut down after cyberattack〉，《The Record》，西元2023年12月12日，https://therecord.media/kyivstar-cyberattack-telecom-shutdown-ukraine，檢索日期2024年10月31日

其網路攻擊方式主要針對俄羅斯國家經濟和公共領域。

三、網路作戰之戰果環境

對網路空間作戰環境而言，戰果評估自然也是每一場網路作戰重要的關鍵因素，其中「NotPetya」惡意軟體攻擊，讓烏克蘭幾乎變成數位荒漠，且 2022 年官方網站遭「DDoS」癱瘓，隨後「Wiper」[29]等病毒移除烏克蘭政府機關資料(常見攻擊手段如表 4)，意圖造成境內恐慌。

表 4 烏俄戰爭常見攻擊手段

攻擊方式	攻擊型態	影響範圍
阻斷攻擊	DDoS、NotPetya、Wiper	系統無法正常運作，造成政府、組織或團體系統癱瘓或中斷。
網路釣魚	NotPetya	偽裝成合法來源，向目標發送欺騙性的電子郵件或消息，誘導他們提供個人資料或機密資訊，
惡意軟體攻擊	Wiper、Poemgate、Poseidon、Whitecat	針對目標系統或網路，以獲取機密資訊或破壞系統，惡意刪除相關資訊。
網路封鎖	DDoS、Poemgate、Wiper、Poseidon、Whitecat	封鎖特定網站、服務或管道，限制人民檢索及通訊自由，以達到政治或軍事目的。
假消息	Deepfake	散布假消息或誇大訊息，以影響人民思想，造成社會輿論，並破壞敵方的形象或挑起社會紛爭。

資料來源：作者整理。

由於網路科技特性造成戰場能見度低，故實難以單靠網路空間來達成，例如以色列在 2007 年轟炸敘利亞核子反應的「果園行動」(Operation Orchard)[30]中，

29Wiper稱為擦拭器，使數據無法訪問和無法使用，然而，與勒索軟體不同的是，其目的並不是在支付贖金後恢復存取權限，而是永遠銷毀數據。〈What is Wiper Malware?〉，《Check Point》，https://www.checkpoint.com/tw/cyber-hub/threat-prevention/what-is-malware/what-is-wiper-malware/ =3，檢索日期2024年10月31日。

30以色列間諜衛星拍攝到已簽署反核子擴散條約的敘利亞在德愛祖爾附近有疑似核子製造工廠的設施出現，在

「據傳」就是由以色列先以電腦病毒破壞防護庫巴爾(Al-Kubar)核武設施的周邊防空飛彈系統，後續方能成功執行空襲行動。[31]現代戰爭已非傳統作戰使用望遠鏡和地圖，日益精進的演算法處理，可以從大量數據中找出關鍵資訊，意味著未來戰爭成敗取決於偵查能力，產生極具透明的戰場環境。

四、資訊網路之備援機制

烏克蘭為了防範俄羅斯的網路攻擊，積極推動數位韌性部署，以維持網路運作，平時不僅針對關鍵基礎設施，設置資料備份與系統備援機制，且對於資料傳輸的網路設備進行管理，並切斷對俄羅斯的電力來源依賴，轉為對其他國家的部署，在電力穩定之下，即使面對俄羅斯分散式阻斷服務攻擊也能維持低速傳輸，並在流量快速清理後恢復正常運作。[32]

五、科技對戰爭的重要性

戰爭開打後，俄羅斯透過網路及電視等數位平台，播放烏克蘭總統澤倫斯基投降演講的「深偽」（Deepfake）影片以假亂真，企圖達到網路戰、資訊作戰及認知戰的「混合威脅」（Hybrid Threats）效果，而烏克蘭也利用網路科技力量，獲得俄羅斯人民的手機號碼和電子郵件信箱，傳遞有關戰爭現實的訊息，這種心理戰和駭客攻擊，須經過更多具組織性及系統化的努力才能實現，烏克蘭副總理暨數位轉型部長則稱：「現代科技是回應戰車、火箭和飛彈的最好方法之一」，[33]可見烏克蘭將傳統戰爭加入新的科技元素，讓戰爭有了不一樣的打法。

對我國網路戰之省思

在烏俄戰爭模式下，我國面臨中共網路作戰能力日益增加及嚴峻軍事威脅，且共軍積極運用其網路灰色地帶、國力及政治影響力，以混合聯合作戰等方式達到解放臺灣之目的，對於網路戰應用及未來發展趨勢，我們應重視並瞭解其中之運用手段，扭轉局面獲取最後之勝利。

一、訂定網路安全防護規範

向美國情報單位求證後得知此訊息是正確的，而透過美國希望施壓敘利亞停止此核子設施建造無效後，以色列決定自行出擊，而作戰行動代號即為果園作戰 (Operation Orchard)。〈網路戰爭無國界，以俄烏網路戰為鏡提升全民資安防護意識〉，《International Fellowship of Christians and Jews》，西元2022年9月5日，https://www.ifcj.org/news/stand-for-israel-blog/operation-orchard，檢索日期2024年10月31日。

31姚宏旻，〈網路作戰的認知與迷思：從網路地理、科技能力與法律規範反思網路的攻擊與防禦〉，《國防雜誌》，第38卷1期，西元2023年3月，頁83。

32曾怡碩，〈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〉，《國防安全雙週報》，西元2022年4月14日，https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1629&typeid=3，檢索日期2024年10月31日。

33郭又華，〈【實體戰爭新手法：從虛擬世界號召全球同盟】烏克蘭運用2手科技策略對抗俄羅斯坦克〉，《iThome》，西元2023年3月18日，https://www.ithome.com.tw/news/149974，檢索日期2024年10月31日。

網路攻擊至今仍未有一致之國際條約就其特性加以規範，囿於缺乏全球普遍性共識，而無法直接將網路攻擊定義為戰爭行為，且網路攻擊是否構成武力攻擊，尚必須在「造成人員傷亡或重大財產損失」方面達到「相當嚴重性」的程度，才有可能構成「武力攻擊」，如此遭受攻擊之國家，也才得以援引「自衛權」實施反擊。

國內現行法規如中華民國刑法及資通安全管理法等，僅限於我國網路環境安全(如附錄)，並無針對軍隊之軍事行動訂有專法，盤點國內法可適用於網路行動者為國家安全法、國家情報工作法與國防法，而該三法主要均為原則性之規定，現行實務上有關軍隊之行動、範圍，仍以行政規則及命令為依歸。

建議我國對於遭受武裝攻擊時，應詳細制定計畫及想定作為實施反制之依據，並結合戰備訓練演練處置流程，訂定迅即反應的軍事行動教範或準則，俾面對外來各項網路威脅時，能對於不同層級、輕重、程序的狀況展開相對應反制措施，亦能提升整體國家安全防護。

儘管國際法意義上之網路戰並未真實發生，然而網路戰時代早已悄然到來，我國面對全球化網路新興議題，在現行體制架構下，除重視網路安全與網路戰之國際法與武裝衝突法之問題外，[34]應設法從歷史的教訓中找出原因，考量網路攻擊複雜性、隱匿性和隱密性等多項特徵，配合修訂新型態網路戰爭之防護措施，達成快速、反應、反制，建構安全可靠的國土防護網路。

二、培育網路人才平戰結合

臺灣每月遭受中共網路攻擊次數達 2,000 至 4,000 千萬次，尤其 2022 年美國眾議院院長斐洛西來訪期間更甚，臺灣數個政府網站遭受數位攻擊及入侵。

我國與烏克蘭同樣面臨強大鄰國威脅，如在衝突發生時達到與烏克蘭類似反制或更高的效果，應立即建立政府機關和民間組織之合作，設立協作機制和管道，並規劃進行相關演練。[35]烏克蘭之所以能夠抵抗俄羅斯的網路攻擊，絕大部分來自 2014 年克里米亞網路攻擊經驗教訓，多年來培育人才的教育環境，建立政府與人民間之網路安全意識及素養。

與我國同為小國的以色列，綜合國力可以撼動中東地區，其無形戰力 8200 部隊是一個極具代表性的例子，他們巧妙運用網路戰術，形成一種不對稱作戰優勢，這支部隊現役士兵服役時間比一般常態部隊多達 1 至 4 年，[36]從高中開始進行精挑細選，經過心理測試、體檢和學歷審核後進入為期半天的面試，而這

34李彥璋，〈國軍應對網路攻擊之法理框架〉，《國防雜誌》，第37卷3期，西元2022年9月，頁38-39。

35〈烏俄戰爭給臺灣的數位備戰啟示〉，《青平台》，西元2023年2月22日，https://future.org.tw/news/10346，檢索日期2024年10月31日。

36曾怡碩、洪嘉齡，〈平戰結合的以色列網路作戰部隊〉，《國防情勢特刊》，第13期，西元2021年11月9日，頁38-39

些面試由 8200 部隊的年輕成員進行，他們具備很高的動機主動尋找合適接班人，過程有助於挑選出高素質的新兵，通過初步篩選後，將接受長達 6 個月的訓練，每天 12 至 18 小時，包括網路戰術、密碼學、通訊電子工程、情報分析和資料挖掘等專業知識，訓練結束後，將被分發到 8200 部隊各單位服務，雖然職責不同但任務性質一致，後備役年齡可達 50 歲。

健全的制度累積了龐大而綿密的網路後備力量，不僅有助於建立優秀的資訊安全環境，在每年招募近千名新兵時，也為他們提供了良好的職業前景，此外，管制 8200 部隊退役之後備役人員每年返部，有助於部隊獲取最新知識和技能，同時也使業界人士了解部隊最新動態，促進軍民合作形成了雙贏局面。

烏克蘭、俄羅斯與以色列一連串的軍民整合與人才培育運用(如表 5)，值得我國效法應用於新兵召募、軍事訓練役、國軍志願役及每年透過後備教召與資通電軍共同執行網路攻擊、防護等任務，以強化我資安能量，另妥善規劃資安產業結合人力生涯發展，有助於吸引更多專業人士加入國軍。

表 5 人才培育對照表

國家名稱	教育方式	政府資源	優點	缺點
烏克蘭	傳統	少	穩定的基礎教育和知識	限制發展和缺乏創新
俄羅斯	廣泛	多	廣泛的學術教育和專業知識	易受政府政策和政治因素影響
以色列	創新	多 (包含私人企業)	有利培養創新和解決問題的能力	依賴私人企業可能導致資源分配不均

資料來源：作者整理。

三、強化網路資安作戰環境

目前國軍在資源共享和數位化指揮方面仍存在顯著差距，尤其在戰時面臨強烈的電子干擾和電子欺騙的環境下，有效掌握戰場態勢和及時作出決策將變

得困難，雖然各軍種已建立各自的資訊鏈，但相互之間通聯整合仍然不足，影響三軍統一指揮機制，也對聯合作戰效能造成影響，[37]因此，應從全面情、監、偵管理著手，掌握全軍資訊安全及網路傳輸，精進戰情、防空與戰管機制，結合國軍地面部隊 C4ISR 系統整合，發展共同作戰圖像平台、強化網路作戰及電子戰能量，以有效達成現代化作戰需求。

四、提升資安防護備援系統

俄羅斯軍事攻擊一開始就對烏克蘭的政府資訊中心和伺服器發動巡航導彈襲擊，並在前一天使用具破壞性的「wiper」惡意程式攻擊當地電腦網路。[38]

面對威脅的烏克蘭政府迅速決定將用戶端之數位基礎設施和資料轉移至位於歐洲的雲端資料中心，成功於戰爭期間保持與人民的溝通及進行軍事防護，這一行動顯示，一個國家在戰時實現數位韌性之關鍵，是能夠迅速將數據轉移到其他地方，並同時保持政府的數位運作。

我國具有高科技資訊人才、技術及網路防護實務經驗豐富，須透過數位發展部推動數位政策的創新與改革，整合電信、資訊、資訊安全、網路與傳播 5 大領域，全面規劃數位發展政策，統籌基礎建設、環境整備及資源運用相關業務，[39]落實公私部門與法治運作，建立商用衛星、數位化通訊、公共網路平臺，[40]並結合友軍單位增加資訊安全及科技交流，運用與整合中華電信及民營通資系統，納入國軍備援體系，常態化實施跨部會網路攻防實戰演練，強化整體資通戰力與應變能力。

另異地備援地點設立主要資訊作業系統、資料同步儲存及復原中心，[41]平時透過環島光纖與軍租網路，將資料同步完成備份，利於戰時迅速啟動備援機制。

五、發展科技結合網路作戰

俄羅斯政府在戰爭中透過人工智慧生成大量假影像，藉以擾亂外界對於烏俄戰爭的真實走向，打擊烏克蘭及邦交國之信心和士氣；烏克蘭利用先進網路威脅情報和端點保護技術，抵禦俄羅斯破壞性的網路攻擊，成功發揮關鍵作用。

微軟威脅情報中心運用人工智慧技術，及時偵測到俄羅斯軍方針對烏克蘭 48 個機構和企業發動多次破壞性網路攻擊，[42]其中包括「蠕蟲」[43]等惡意軟體，

37蔡志銓，〈國軍精進 C4ISR 系統之研析〉，《海軍軍官學校季刊》，第39卷4期，西元2020年12月24日，頁48

38施立成，〈網路戰爭無國界，以俄烏網路戰為鏡提升全民資安防護意識〉，《數位時代》，西元2022年8月26日，https://www.bnext.com.tw/article/71389/hacker%EF%BC%8Dinformation-security-mstic，檢索日期2024年10月31日。

39唐政務委員鳳辦公室，〈數位發展部—臺灣數位發展的馬達〉，《行政院》，西元2022年8月11日，https://www.ey.gov.tw/Page/448DE008087A1971/e03388cc-566c-4946-861b-2a1132c3c2cf，檢索日期2024年10月31日。

40張哲鐘、彭群堂，〈以色列8200網路間諜部隊對我國省思〉，《國防雜誌》，第37卷3期，西元2022年9月，頁48

41呂兆祥，〈共軍網路作戰對我資電作戰之影響〉，《國防雜誌》，第36卷6期，西元2015年11月，頁93。

42同註12。

然透過端點保護技術，快速將相關保護軟體的程式碼，傳送到雲端服務及其他連線設備，以有效識別和阻止惡意軟體之攻擊行為，在可預見的未來中，如何擴大人工智慧技術應用，俾能掌握相對優勢。

近年來「區塊鏈」作為一項新興的安全技術引起廣泛關注，其採用分散式系統架構，能夠顯著降低資料外洩風險，同時，網路攻擊日益頻繁，對系統安全構成嚴重威脅，為了應對這種挑戰，利用區塊鏈技術能夠有效抵禦駭客組織對網路的攻擊，透過區塊鏈之去中心化特性(如表 6)，可以建立一道堅固的網路安全防禦機制，保障訊息安全發送和接收，同時降低被駭客攻擊風險，因此，我國各系統如能夠導入區塊鏈技術，將可提升整體系統之網路安全。

表 6 區塊鏈主要功能

功能名稱	說明
去中心化	不依賴中央控制機構的系統架構，所有參與者（或稱為節點）共同維護系統運行，而不是由單一的中央實體來控制和管理。
不變性	一旦數據被寫入區塊鏈，且經過多數參與者（或稱為節點）確認後，就無法更改或刪除，以防有心人士竄改資料。
共識	所有參與者（或稱為節點）需要達成一致的共識，才能更新或修改資料。

資料來源：作者整理。

結論

自烏俄戰爭開打以來，烏克蘭展現出強大自我防衛決心與意志，並透過各種途徑尋求國際上的援助與支持，建立國家網路部隊及資安能量，並以小搏大抵抗俄羅斯侵略重要關鍵，網路安全防禦作為影響國家安全甚鉅。

現代戰爭誠如《孫子兵法》中《謀攻篇》，所敘述戰爭最高境界是通過非武力的方式使敵人屈服，武力則是最後的手段，換言之，動用一切手段，以最少代價贏得戰爭，然本研究分析認為「謀攻」是多層次、同時性的「伐謀」、「伐

43蠕蟲 (Worm)病毒再於可以自我複製，掌握電腦傳輸檔案或資訊的功能，系統一旦被蠕蟲感染會自動蔓延，最危險之處就是大量複製的能力。〈蠕蟲 Worm〉，《國立聯合大學》，https://isp.nuu.edu.tw/p/405-1074-1290,c633.php，檢索日期2024年10月31日。

交」與「伐兵」，同樣的原則也適用於中共，我們經常在各種網路社群平台及生活中，接收到似是而非的訊息，影響人民思想造成社會輿論。

戰爭中決勝關鍵即是結合戰術戰法的網路作戰，而網路作戰主要在戰力整合，網路空間使國家利益的邊界得以延伸和擴展，面對未來新型態戰爭及各種作戰環境，如果沒能從烏俄戰爭吸取教訓的軍隊，未來可能輸給從中學到一課的敵手。

參考文獻

一、中文書籍

(一)國防部，〈聯合作戰網電教則〉，民國 111 年 12 月 8 日修訂，頁 3-34。

(二)黃郁文，〈淺析俄羅斯「網路戰」-以 2022 年「俄烏戰爭」運用為例，《海軍學術雙月刊》(臺北市)，第 56 卷第 4 期，海軍司令部，民國 111 年 8 月，頁 90-91。

(三)李彥璋，〈國軍應對網路攻擊之法理框架〉，《國防雜誌》，第 37 卷 3 期，西元 2022 年 9 月，頁 38-39。

(四)曾怡碩、洪嘉齡，〈平戰結合的以色列網路作戰部隊〉，《國防情勢特刊》，第 13 期，西元 2021 年 11 月 9 日，頁 38-39。

(五)姚宏旻，〈網路作戰的認知與迷思：從網路地理、科技能力與法律規範反思網路的攻擊與防禦〉，《國防雜誌》，第 38 卷 1 期，西元 2023 年 3 月，頁 83。

(六)蔡志銓，〈國軍精進 C4ISR 系統之研析〉，《海軍軍官學校季刊》，第 39 卷 4 期，西元 2020 年 12 月 24 日，頁 48。

(七)張哲鐘、彭群堂，〈以色列 8200 網路間諜部隊對我國省思〉，《國防雜誌》，第 37 卷 3 期，西元 2022 年 9 月，頁 48。

(八)呂兆祥，〈共軍網路作戰對我資電作戰之影響〉，《國防雜誌》，第 36 卷 6 期，西元 2015 年 11 月，頁 93。

二、網路資料

(一)張玲玲，〈強化網路戰力 肆應新型態戰〉，《青年日報》，民國111年9月4日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1530306&type=forum，檢索日期2024年10月31日。

(二)戴匡，〈俄羅斯網攻烏克蘭態勢分析及其啟示〉，《財團法人臺灣網路資訊中心》，民國112年4月24日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1530306&type=forum，檢索日期2024年10月31日。

(三)〈俄烏戰爭周年回顧：俄羅斯網攻烏克蘭態勢分析及其啟示〉,《財團法人臺灣網路資訊中心》，西元2022年4月24日，https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1602，檢索日期2024年10月31日。

(四)蕭長展，〈烏克蘭民間這樣做使俄軍付出代價：資訊科技力、破壞活動、訴諸國際〉,《WATchout》，西元2023年11月29日，https://watchout.tw/forum/IgH2vEjDy491NUfUlilM，檢索日期2024年10月31日。

(五)〈什麼是零時差漏洞(Zero-Day Vulnerability)?有哪些漏洞攻擊手法?〉,《資安趨勢部落格》，西元2019年12月26日，https://blog.trendmicro.com.tw/?p=62238，檢索日期2024年10月31日。

(六)〈檢視Turla APT集團的活動〉,《Trend Micro》，西元2023年12月12日，https://www.trendmicro.com/zh_tw/research/23/i/examining-the-activities-of-the-turla-group.html，檢索日期2024年10月31日。

(七)汪哲仁，〈網攻威脅全球基建 資安防護刻不容緩〉,《青年日報》，西元2023年11月22日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1631396，檢索日期2024年10月31日。

(八)曾怡碩，〈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〉,《國防安全雙週報》，西元2022年4月14日，https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1629&typeid=3，檢索日期2024年10月31日

(九)〈烏俄戰爭給臺灣的數位備戰啟示〉,《青平台》，西元2023年2月22日，https://future.org.tw/news/10346，檢索日期2024年10月31日。

(十)施立成，〈網路戰爭無國界，以俄烏網路戰為鏡提升全民資安防護意識〉,《數位時代》，西元2022年8月26日，https://www.bnext.com.tw/article/71389/hacker%EF%BC%8Dinformation-security-mstic，檢索日期2024年10月31日

(十一)〈聯合國憲章〉,《植根法律網》，西元1965年12月20日，https://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040050070010800-0541220，檢索日期2024年10月31日。

(十二)〈中華民國刑法〉,《全國法規資料庫》，西元2023年12月27日，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=C0000001&kw=%e5%88%91%e6%b3%95，檢索日期2024年10月31日。

(十三)〈資通安全管理法〉,《全國法規資料庫》，西元2018年6月6日，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297&kw=%e8%b3%87%e9%80%9a%e5%ae%89%e5%85%a8%e7%ae%a1%e7%90%86%e6%b3%95，檢索日期2024年10月31日。

(十四)〈國家安全法〉,《全國法規資料庫》,西元2022年6月8日,https://law.moj.gov.tw/LawClass/LasWingleRela.aspx?medi=print&PCODE=A0030028&FLNO=6&ty=L,檢索日期2024年10月31日。

(十五)〈什麼是區塊鏈技術?〉,《AWS》,https://aws.amazon.com/tw/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc,檢索日期2024年10月31日。

(十六)〈國防法〉,《全國法規資料庫》,西元2012年6月6日,https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=F0010030&kw=%e5%9c%8b%e9%98%b2%e6%b3%95,檢索日期2024年10月31日。

(十七)〈國家情報工作法〉,《全國法規資料庫》,西元2020年1月15日,https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0020041&kw=%e5%9c%8b%e5%ae%b6%e6%83%85%e5%a0%b1%e5%b7%a5%e4%bd%9c%e6%b3%95,檢索日期2024年10月31日。

(十八)唐政務委員鳳辦公室,〈數位發展部一臺灣數位發展的馬達〉,《行政院》,西元2022年8月11日,https://www.ey.gov.tw/Page/448DE008087A1971/e03388cc-566c-4946-861b-2a1132c3c2cf,檢索日期2024年10月31日。

(十九)〈蠕蟲 Worm〉,《國立聯合大學》,https://isp.nuu.edu.tw/p/405-1074-1290,c633.php,檢索日期2024年10月31日。

(二十)郭又華,〈【實體戰爭新手法:從虛擬世界號召全球同盟】烏克蘭運用2手科技策略對抗俄羅斯坦克〉,《iThome》,西元2023年3月18日,https://www.ithome.com.tw/news/149974,檢索日期2024年10月31日。

(二一)〈Who Is KillNet?〉,《BlackBerry》,https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet,檢索日期2024年10月31日。

(二二)〈Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior〉,《Atlanatic Council》,西元2022年9月19日,https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/,檢索日期2024年10月31日。

(二三)〈APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers〉,《National Cyber Security Centre》,西元2023年4月18日,https://www.ncsc.gov.uk/news/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers,檢索日期2024年10月31日。

(二四)〈APT29 targets COVID-19 vaccine development〉,《National Cyber Security Centre》,西元2020年7月16日,https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development,檢索日期2024年10月31日。

(二五)Sergiu Gatlan,〈Russian FSB hackers hitting Ukraine since October〉,《BLEEPINGCOMPUTER》,西元2022年2月4日,https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development,檢索日期2024年10月31日

(二六)〈Russia’s war on Ukraine:Timeline of cyber-attacks〉,《EPRS》,西元2022年6月21日,https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549,檢索日期2024年10月31日。

(二七)〈Ukraine crisis: 'Wiper' discovered in latest cyber-attacks〉,《BBC》,西元2022年2月24日,https://www.bbc.com/news/technology-60500618,檢索日期2024年10月31日。

(二八)Daryna Antoniuk〈Russia’s Sandworm hacking unit targets Ukrainian telecom providers〉,《The Record》,西元2023年10月18日,https://therecord.media/russia-sandworm-hacking-ukraine-telecom-internet-providers,檢索日期2024年10月31日。

(二九)Daryna Antoniuk〈Ukraine telecom cyberattack one of highest-impact hacks of the war〉,《The Record》,西元2023年12月18日,https://therecord.media/ukraine-kyivstar-hack-high-impact,檢索日期2024年10月31日。

(三十)〈俄羅斯網軍研究簡報〉,《安全內參》,西元2021年1月6日,https://www.secrss.com/articles/28510,檢索日期2024年10月31日。

(三一)〈Ukraine war: Ukrainians announce the launch of an 'IT army' to fight off Russian cyberattacks〉,《euronews.next》,西元2022年2月27日,https://web.archive.org/web/20220424182133/https://www.euronews.com/next/2022/02/26/ukraine-war-ukrainians-announce-the-launch-of-an-it-army-to-fight-off-russian-cyber attacks,檢索日期2024年10月31日。

(三二)〈Про CERT-UA〉,《Державні сайти України》,https://cert.gov.ua/about-us,檢索日期2024年10月31日。

(三三)Katharina Krebs、Jake Kwon,〈Cyberattack hits Ukraine government websites〉,《CNN》,西元2022年1月14日,https://edition.cnn.com/2022/01/14/europe/ukraine-cyber-attack-government-intl/index.html,檢索日期2024年10月31日。

(三四)〈What is Wiper Malware?〉,《Check Point》,https://www.checkpoint.com/tw/cyber-hub/threat-prevention/what-is-malware/what-is-wiper-malware/=3,檢

索日期2024年10月31日。

(三五)〈Groups〉,《MITRE》,https://attack.mitre.org/versions/v10/groups/,檢索日期2024年10月31日。

(三六)〈Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure〉,《Cybersecurity and Infrastructure Security Agency》,https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a,檢索日期2024年10月31日。

(三七)Veronika telychko,〈CAPIBAR and KAZUAR Malware Detection: Turla Aka UAC-0024 or UAC-0003 Launches Targeted Cyber-Espionage Campaigns Against Ukraine〉,《SOC Prime》,https://socprime.com/blog/capibar-and-kazuar-malware-detection-turla-aka-uac-0024-or-uac-0003-launches-targeted-cyber-espionage-campaigns-against-ukraine/,檢索日期2024年10月31日。

作者簡介

陳明薇少校,專業軍官 104 年班、通訓中心通資電正規班 108 年班;曾任排長、資訊官、中隊長,現任職於通訓中心網路作戰組教官。

附錄

國內現行法規綜整表

法規名稱	條文	內容
中華民國刑法	第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
	第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
	第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
資通安全管理法	第 3 條	一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。 三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
國家安全法	第 6 條規定	為確保海防及軍事設施安全，並維護山地治安，得由國防部會同內政部指定海岸、山地或重要軍事設施地區劃為管制區，並公告之。

國家情報工作法	第 3 條第 2 款規定	二、情報工作：指情報機關基於職權，對足以影響國家安全或利益之資訊，所進行之蒐集、研析、處理及運用。國防部參謀本部通信電子資訊參謀次長室（以下簡稱通次室）及資通電軍指揮部（以下簡稱資通電軍）於平時主責為網路情蒐、網路防護及網路滲透等任務之執行與管制，性質上初步符合國際法所規範間諜之構成要件，而透過網路監視的行為，自然是屬於合法的軍事行動。
國防法	第 14 條規定	軍隊指揮事項如下： 一、軍隊人事管理與勤務。 二、軍事情報之蒐集及研判。 三、作戰序列、作戰計畫之策定及執行。 四、軍隊之部署運用及訓練。 五、軍隊動員整備及執行。 六、軍事準則之制頒及作戰研究發展。 七、獲得人員、裝備與補給品之分配及運用。 八、通信、資訊與電子戰之策劃及執行。 九、政治作戰之執行。 十、戰術及技術督察。 十一、災害防救之執行。 十二、其他有關軍隊指揮事項。

資料來源：作者整理