DOI:10.6237/NPJ.202208_56(4).0006

淺析俄羅斯「網路戰」－以2022年「俄烏戰爭」運用為例

Analyzing on Russia's Application of "Cyber Warfare" -An example of the Russia-Ukraine War in 2022

黃郁文　先生

提　　要：

一、「資訊作戰」在現代戰爭中至關重要，被視為取得決定性戰果的關鍵能力。戰爭中控制資訊被稱為「資訊封鎖」或「資訊優勢」；而「網路戰」為資訊作戰的一環，是一種駭客行為，它通過破壞對方的電腦網路和系統，刺探機密資訊，以達到政治目的。

二、俄羅斯已具備先進的網路能力，並在全球進行資訊、宣傳、間諜和網路攻擊活動，且於平時即鎖定或癱瘓他國的網站、重要戰略系統等目標，這類機構(公司)通常控制著國家重要基礎設施，如銀行、能源、水(電)力、通訊及衛星等；一旦戰爭伊始，即可提早掌握主動，獲取決定性的成功。

三、在2022年的「俄烏戰爭」中，俄國在攻擊烏克蘭前後，同樣也發動網路攻勢。「他山之石，可以攻玉」。未來我國除應防範敵對國家對我國之資料中心、網路、其他高度敏感資料進行網路或「分散式阻斷服務」(DDoS)等攻擊作為外，也需要有「快速分流、復原、重啟備份」等應對能力及機制，並透過國際合作及與建立聯防機制，以提升我國網路空間安全。

關鍵詞：俄羅斯、網路戰、烏克蘭

Abstract

1.Information warfare is crucial in modern war and is seen as a key capability for achieving decisive results, The necessity to control information in war is known as "information blockade" or "information dominance." Cyber warfare is an element of information warfare and is a form of hacking, which involves disrupting an opponent's computer network and systems to access confidential information for one's own political purposes.

2.Russia has developed advanced cyber capabilities to conduct information, propaganda, espionage and cyberattack activities around the world. Targets such as Ukrainian websites and important strategic corporate systems are locked on or neutralized in peacetime. Such corporations often control national key infrastructures such as banking, energy, water, power, communications, nuclear bombs and satellites in order to gain proactive control and decisive success.
3.The Russian attack on Ukraine was preceded and followed by cyberattacks. We will need to have the ability and mechanism to quickly divert, recover and restart backups in order to prevent cyberattacks and distributed denial of service(DDoS) attacks on data centers, networks and other highly sensitive data by our enemies in the future. Through international cooperation and information sharing, we can establish joint defense mechanisms with friendly countries and support our participation in international cyberspace. Cyber warfare is where our country can make a big play.
Keywords: Russia, cyber warfare, Ukraine

壹、前言

現代戰爭中，「資訊作戰」至關重要，而狹義的「資訊戰」亦可定義為「網路戰」，其內容包括針對敵對國家政府機關、軍事單位、金融機構，私人企業和社群等團體，利用開放性的網路平台與資訊技術，進行資料竊取、癱瘓系統服務與竄改他人資料等方式，以獲得戰場優勢，[1]且對打擊敵人具有非常高的效率。2022年2月24日，「烏俄戰爭」前，許多國際組織與新聞媒體就提出警告，俄羅斯正散布大量不實訊息，[2]並意圖發動「網路戰」，此正凸顯「網路戰」不僅是發動常規軍事攻擊的前置作業，亦為正式攻擊階段的輔助手段；而俄國此舉就是為對烏克蘭開戰前，形塑對其有利的戰場態勢。

回顧1991年烏克蘭脫離蘇聯後，即希望可以加入「北大西洋公約組織」(North Atlantic Treaty Organization，以下稱「NATO」或「北約」)。2008年，以美國為首的「北約」就曾考慮要把烏國納入成員，此舉卻觸動俄國總統普丁(Vladimir Putin)最敏感的安全神經；且長期以來，俄羅斯就有因烏克蘭持續親近西方而遠離俄國的焦慮，尤其一旦烏國加入「北約」，對俄國而言，西方敵人就會「近在咫尺」。[3]然烏克蘭為尋求加入「NATO」之舉措，不但招致俄羅斯於2月21日公開承認烏東地區尋求分離自治

註1：余政倫，〈淺談新型態「資訊戰」及網路攻防結合運用〉，《海軍學術雙月刊》(臺北市)第56卷，第2期，2022年4月1日，頁70。
註2：〈多方查證釐清來源 防範假訊息分化〉，《青年日報》，2021年3月3日，版5。
註3：劉威良，〈普亭第一時間的認知作戰很成功，德國回過神後才發現敵人近在眼前〉，關鍵評論，2022年3月3日，https://www.thenewslens.com/article/163417，檢索日期：2022年5月13日。

的「頓內茨克共和國」(Donetsk People´s Republic)與「盧甘斯克人民共和國」(Lugansk People´s Republic)之獨立地位，[4]並下令俄軍進入當地進行「維和行動」。普丁總統甚至表明，因烏克蘭拒不履行「明斯克協議」(Minsk Agreements)[5]，逕自宣布協議已不復存在；且不僅承認烏東兩個共和國，更於2月24日對烏克蘭採取「特別軍事行動」，戰火至此點燃。

因為俄羅斯發動對烏克蘭的戰爭，許多網路輿論的討論焦點，也都在檢討西方國家有無直接兵力援助，[6]也開始發想中共會發動對臺的侵略戰爭，並推測中共領導人習近平正關注國際對俄羅斯網路攻擊烏克蘭的反應，以做為未來入侵臺灣的評估準備。因此，撰文主要的目的在分析「俄烏戰爭」中的「網路戰」作為，並提供國軍高層借鑑，希望我國防範敵對我國資料中心、網路、其他高度敏感目標發動網路攻擊，或「分散式阻斷服務」(Distributed Denial of Service Attack，以下簡稱DDoS)[7]等攻擊方式時，能有相對應變機制及能力，同時提升我網路空間安全，以確保我國關鍵基礎設施安全。

貳、俄羅斯的網路戰思維及攻擊態樣

由於現代化必須具備經濟條件與工業技術實力，俄羅斯除持續對其軍事力量進行現代化改造，並企圖操縱全球資訊環境，以對周邊國家使用間接行動工具，[8]而網路攻擊對損壞資料、連接電腦的設備、重要戰略公司系統方面具有相當高的破壞性。而這類公司系統往往控制著國家重要的基礎設施，例如銀行、能源、供水、電力、通訊、水壩、核彈及衛星等等。因為網路攻擊最重要的特徵就是確定攻擊源頭的難度，而且這些攻擊可能會影響國家的利益，畢竟一小撮的高能力「駭客」(Hacker)，就可以做到整個軍隊做不到的事情；而莫斯科已從事實上證明，它有能力同時發動對網路空間和實地戰場產生重大影響的攻擊。[9]以下就俄羅斯對「網路戰」的定義、內容分述如下。

一、俄國網路作戰的定義及形式

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」形式之一；並認為

註4：洪美蘭，〈未能以優勢養實力「貿然選邊」烏克蘭招致「危機三部曲」〉，關鍵評論，2022年2月25日，https://forum.ettoday.net/news/2196297?fbclid=IwAR39gDCLBTpWizSd_CDm6sLhxnFXnYc6L6OtU9dqvZfBA5SQcFAz7vT1eqc，檢索日期：2022年5月13日。

註5：〈烏克蘭危機：解讀頓巴斯、明斯克協議、北溪二號等五個關鍵詞〉，BBC NEWS，2022年3月1日，https://www.bbc.com/zhongwen/trad/world-60555056，檢索日期：2022年5月13日。

註6：同註3。

註7：阻斷服務攻擊(Denial of Service Attack，DoS)是近年來常見的一種網路攻擊模式，其目的在於使被攻擊的目標網路或資訊系統的資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取網路及資訊系統的服務。當惡意攻擊者運用網路上大量被攻陷的電腦作為殭屍((Bot)向特定的目標發動攻擊時，稱為分散式阻斷服務攻擊(DDoS)。〈分散式阻斷服務攻擊防護策略探討〉，臺灣網路資訊中心，https://www.twnic.tw/NEWS4/165.php，檢索日期：2022年5月13日。

註8：它的終極威懾力量是強大的核力量，能夠在幾分鐘內對美國境內的目標，進行大規模核打擊。2017 Russia Military Power Report, Defense Intelligence Agency, June 23, 2017, p.6。

註9：〈如何能在俄烏危機中動用網路武器？〉，ALJAZEERA，2022年2月23日，https://chinese.aljazeera.net/opinions/2022/2/23/如何能在俄烏危機中動用網路武器，檢索日期：2022年5月13日。

基於網際網路的攻擊有以下數種形式，包含利用駭客(有官方授權的、合法)通過網際網路用侮辱性或者煽動性的評論修改敵方的網頁內容，此類言論的傳送或者是在其他網頁的內容中設置宣傳內容、入侵私人網頁或者伺服器以獲得秘密資訊，或者將秘密資訊替換成虛假、對其有利的信息等方式。[10]

二、取得決定性戰果的關鍵能力

俄羅斯認為資訊作戰被視為在作戰初期取得決定性結果的關鍵能力，重點是控制現代戰鬥空間各個維度的資訊頻譜。現代戰爭中控制資訊需要「資訊封鎖」及取得「資訊優勢」，並在戰役中儘早掌握主動權，並拒絕對手使用網路空間，從而獲得決定性的成功。俄國強調電子戰和其他資訊戰能力，包括滲透及欺騙等，做為應對戰爭各個方面的方法之一。[11]

三、軍事打擊前依賴進攻性的「網路戰」

俄羅斯是最早在軍事領域內利用網路空間的國家之一，並且一直重視研發，以提高其在該領域內的網路攻擊能力。在與烏克蘭的這場戰爭之中，俄國的戰略是依賴進攻性的「網路戰」，因為它們會使其在戰爭中的力量倍增；而這就意味著，如果能與其他的軍事能力配合使用，整體的戰鬥能力就能得到大大提升。此外，這項戰略還依賴於在開展軍事行動之前，嘗試破壞對手的資訊基礎設施及其民用和軍事通信，其中最突出的例子，就是莫斯科在2008年對「喬治亞共和國」(Georgia)發動軍事打擊之前，就遭指控涉嫌對喬國發動網路攻擊，[12]並造成該國網路癱瘓與重大損失。

四、以DDoS為主要網路攻擊型式

「分散式阻斷服務」(DDoS)攻擊目的是使電腦或網路無法提供正常的服務、干擾設備及攻擊控制民用或軍用設備工作的電腦，使電腦斷網或者損壞；或攻擊基礎設施，如保障城市日常生活基礎設施的電腦、供水、供電、消防、交通等。DDoS利用多個被破壞的電腦系統做為攻擊流量的來源，從而達成攻擊目的；而被利用的機器可能包括電腦及其他網路資源。自2014年烏克蘭東部地區發生戰爭以來，俄羅斯支持的駭客組織就持續對烏國軍隊採用各種電子和網路戰策略，以癱瘓烏國網路系統，並輔助作戰任務目標達成。[13]

五、「進階持續威脅」(Advanced Persistent Threat，簡稱APT)

APT並不只有單一形式的手段，而更像是複合的「網路戰」。典型的策略是從情報蒐集開始，到病毒或惡意程式植入，期間攻擊者可能會採取多種手法，如惡意軟體、弱點掃描，也包括利用內部間諜進行破壞。即便系統本身的防毒程式擋下其中一、兩次攻擊，也不代表威脅就被消滅，而是換個方式繼續攻擊。這一過程可能持續數天、數週、

註10：2017 Russia Military Power Report, Defense Intelligence Agency, June 23, 2017, p.32。
註11：同註10。
註12：同註9。
註13：Daniel Brown, Russian-backed separatists are using terrifying text messages to shock adversaries -and it's changing the face of warfare, INSIDER, Aug 15,2018, https://www.businessinsider.com/russians-use-creepy-text-messages-scare-ukrainians-changing-warfare-2018-8，檢索日期：2022年5月16日。

表一：俄羅斯主要安全單位的職責表

單位名稱	網路作戰	政治情報	經濟情報	軍事情報	行動支援	機構情報	政治安全	執法行動
主要情報局(GRU)	●	□	□	●	●	□		
聯邦安全局(FSB)	●	□	□	□	●	●	●	□
對外情報局(SVR)	●	●	●	□	●	□	□	
聯邦警衛局(FSO)	□					□	●	□
備註：●主要任務　□附屬任務								

資料來源：參考2017 Russia Military Power Report, Defense Intelligence Agency, June 23, 2017, p.73，由作者整理製表。

數月，甚至是以年為單位，不過一旦部署完成，最後發動攻擊可能只需數分鐘時間，就能達到大面積的傷害。[14]

參、俄羅斯網路戰攻擊單位

俄羅斯已經部署了先進網路能力，可在全球範圍內同時進行資訊宣傳、間諜活動和網路攻擊行動。該國設有許多單位並由各種安全和情報機構負責監督。[15]另因俄國的安全機構彼此相互競爭，且經常在同一個目標上開展秘密行動，使得具體的歸屬和動機評估變得更加困難(安全單位，如表一)。以下就其「網路戰」背後的情報單位及主要駭客組織，分段說明如后。

一、網路戰背後的情報單位

「進階持續威脅」(APT)是一種資安攻擊類型，簡單來說是針對特定對象所進行的多重、全方位網路攻擊；正因為需要長時間部署，發動APT攻擊也意味成本更高。俄羅斯主要進行網路「APT」之組織，其背後支持的單位，分項概述如下：

(一)聯邦武裝部隊總參謀部「主要情報局」(Russian General Main Staff Intelligence Directorate，以下簡稱GRU)[16]，該局隸屬於俄羅斯「軍事指揮部」，局長需向國防部長和總參謀長匯報，是該國最大的對外情報機構，因其願意執行風險更高的「複雜、高風險的行動」而從中脫穎而出。[17]該單位由「54777部隊」及「網路特種技術中心」組成，下轄「26165部隊」、「74455部隊」負責進行網路戰(如圖一)。[18]2018年10月美國賓州的一個大陪審團起訴了7名被告，他們都是GRU的成員，罪名是電腦駭客、電信欺詐、加重身分盜竊和洗錢；[19]2022年2

註14：林佳誼，〈總統府被駭，中了「最難防的這種」駭客目的是「震懾臺灣民心」？〉，《天下雜誌》(臺北市)，2020年5月18日，https://www.cw.com.tw/article/5100290?template=transformers&from_id=5120248&from_index=6&rec=k2i，檢索日期：2022年5月13日。

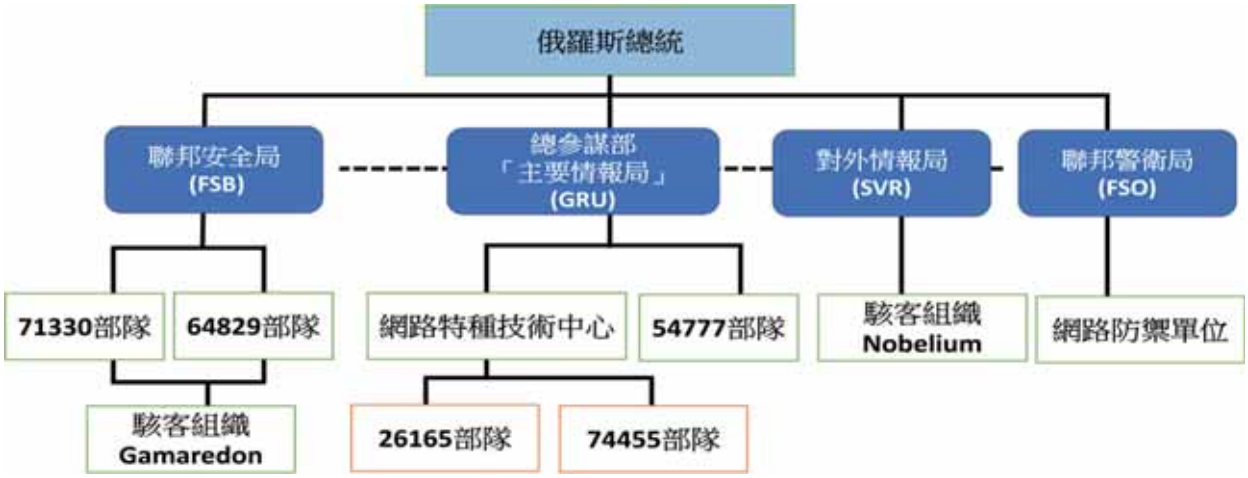
註15：Andrew S. Bowen, Russian Cyber Units, Congressional Research Service, February 2, 2022,p.1。

註16：U.S. Dept. Of Defense, Military And Security Developments Involving The People's Republic Of China 2021, November 2, 2021,p.147。

註17：格魯烏(俄語：Главное Разведывательное Управление，意思為「情報總局」，拉丁文轉寫為GRU)，為蘇聯與俄羅斯聯邦的軍事情報機構，是俄聯邦武裝部隊總參謀部的對外軍事情報機構，控制軍事情報部門並維持自己的特種部隊，與俄羅斯的其他安全和情報機構，如對外情報局(SVR)、聯邦安全局(FSB)和聯邦保護局(FSO)的負責人直接向總統匯報。該機構在國外部署的特工人數是SVR的6倍，指揮大約25,000名特種部隊。GRU , DBpedia, https://dbpedia.org/page/GRU，檢索日期：2022年5月16日。

註18：Andrew S. Bowen, Russian Military Intelligence: Background and Issues for Congress, November 15, 2021,p.18。

註19：該陰謀基於其戰略對美國個人、企業實體、國際組織及其各自位於世界各地的員工進行了持續而複雜的電腦入侵，從2014年12月或前後開始並至少持續到2018年5月。U.S. Charges Russian GRU Officers with International Hacking and



圖一：俄羅斯負責網路戰的情報單位圖

資料來源：參考Andrew S. Bowen, Russian Cyber Units, Congressional Research Service, February 2, 2022,p.1；Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, CISA, April 20, 2022,p3-5，由作者調整製圖。

月「俄烏戰爭」前，英國「國家網路安全中心」(National Cyber Security Centre，NCSC)即發出警告指出，由GRU控制的駭客團體「沙蟲」(Sandworm)，正集中對烏克蘭進行網路攻擊。[20]

(二)「聯邦安全局」(Federal Security Bureau，以下稱FSB)成立於1995年，前身是蘇聯「國家安全委員會」(又稱「格別烏」，以下稱KGB)的秘密警察系統，負責處理國家層級所面對的威脅，普丁在掌權前就曾擔任這個機構的負責人。[21]該局也是負責俄國內部安全和反情報的國內主要安全機構，任務包括保護國家免受外國網路攻擊和監視國內犯罪駭客，近年來，已將其使命擴大到包括外國情報蒐集和進攻性網路行動。[22]烏克蘭政府於2022年1月中旬在遭到大規模的網路攻擊後，即指控俄羅斯「FSB」(下轄「64829部隊」、「71300部隊」)與駭客組織「Gamaredon」有關。[23]

(三)「對外情報局」(Foreign Intel-

Related Influence and Disinformation Operations, The United States Department of Justice, October 4, 2018,https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and，檢索日期：2022年5月16日。

註20：「沙蟲」之前多次使用 VPNFilter 惡意軟體，瞄準企業網路上沒有防備的路由器或雲端硬碟，駭入後將檔案鎖死，先前已有多家歐美企業遭殃，並被沙蟲勒索贖金後才得以恢復資料。〈資訊戰同步開打，烏克蘭軍收大量心戰簡訊又遭DDoS 攻擊〉，科技新報，2022年2月24日，https://technews.tw/2022/02/24/ukrainian-is-under-massive-ddos-and-information-warfare-attacks/，檢索日期：2022年5月13日。

註21：〈普京、權力和毒藥：俄羅斯精英間諜俱樂部-俄羅斯聯邦安全局〉，BBC中文網，2022年2月5日，https://www.bbc.com/zhongwen/trad/world-42947727，檢索日期：2022年5月18日。

註22：同註15，p.2。26165部隊負責駭客攻擊民主黨國會競選委員會的兩個俄羅斯網路團體之一。74455部隊與俄羅斯一些破壞性的網路攻擊有關，曾參與2016年美國總統大選期間被盜的電子郵件和文件，具有顯著的攻擊性網路能力；54777部隊，又稱第72特別服務中心，負責心理戰，包括網路虛假訊息和資訊作戰。

註23：〈【資安月報】2022年2月〉，iThome，2022年3月6日，https://www.ithome.com.tw/news/149713，檢索日期：2022年5月13日。

表二：與俄羅斯相關的主要的駭客組織表

駭客名稱	別　　名	關聯單位	攻　擊　目　標
APT28	奇幻熊(Fancy Bear)、Sofacy Group、Pawn Storm、Sednit	總參謀部主要情報局	軍隊、安全部門、政府單位。
APT29	舒適熊(Cozy Bear)	聯邦安全局	電信、科技、製藥。
Gamaredon	Armageddon、Primitive Bear、ACTINIUM	聯邦安全局	政府部門、烏克蘭移民局、技術機敏單位、非營利組織(NGO)。
Turla	惡毒熊(Venomous Bear)、Uroburos 、KRYPTON、Snake	俄羅斯政府資助	政府、大使館和軍事單位。
worm	Voodoo Bear、TeleBots、Black Energy、Iron Viking、Quedagh、TEMP.Noble	俄羅斯政府資助	政府單位、關鍵系統能源、交通、醫療保健。

資料來源：參考The Top 5 Russian Cyber Threat Actors to Watch, Rapid, Mar 03, 2022,https://docs.publicnow.com/viewDoc?hash_primary=2D8B2C3D80F1D5EAACE3F65799717CECC69FF3EB；APT Gamaredon активно атакует украинские организации с октября 2021 года,8 февраля, SecurityLab.ru 2022,https://www.securitylab.ru/news/529611.php；〈世界著名駭客組織宣布發起網路戰爭〉，鳳凰網，2022年2月26日，https://tech.ifeng.com/c/8DwgC89heH1；〈俄羅斯駭客組織再次瞄準烏克蘭官員〉，360官網，2019年12月9日，http://www.360.cn/n/11390.html；檢索日期：2022年5月13日，由作者整理製表。

ligence Service of the Russian Federation，以下稱SVR)在前蘇聯時期是KGB的「第1總局」，負責國外情報的蒐集、分析，進攻性反間諜等；「聯邦安全局」(FSB)是「第2總局」，負責國內安全。蘇聯解體後，俄羅斯前總統葉爾欽(Boris Yeltsin)於1990年代把「KGB」分拆，目的是要削弱它的權力。[24]2020年駭客組織「Nobelium」曾攻擊美國資訊科技業者「Solar Winds」，導致使用該公司軟體的數千家企業及美國、英國政府機構受害，美國當時就指責SVR為幕後主使。[25]

(四)「聯邦警衛局」(FSO)，前身是「KGB」的「第9總局」，主要職能為保護總統及國家重要官員的人身安全，以及處理國家秘密通信相關的業務，擁有相當高水準的技術裝備，且武器、特殊手段、設備、通信和運輸都在不斷更新。[26]主要關注面向在俄羅斯政府網路的防禦。[27]

二、俄國主要的駭客組織

能夠發動「進階持續威脅」(APT)攻擊的駭客，通常都是組織性行為，背後甚至有國家力量支持；過去包含中共、北韓、俄羅斯等，都是經常被資安專家點名為APT攻擊背後的國家力量。[28]以下就俄國主要駭客組織，分述如後(如表二)。

(一)APT28

成立於2004年為，又被稱為「魔幻熊」

註24：〈俄兩大情報局 爆攻訐戰〉，《香港文匯報》，2010年12月28日，版A10。

註25：〈俄羅斯駭客集團發動網攻 鎖定美政府機構智庫等〉，中央廣播電台，2021年5月30日，https://www.rti.org.tw/news/view/id/2101096，檢索日期：2022年5月13日。

註26：Russian protective service uses unique domestic innovations, says official, Russian News Agency,16 SEP 2021,https://tass.com/defense/1338431?fr=operanews，檢索日期：2022年5月16日。

註27：同註23。

註28：同註14。

(Fancy Bear)或「Strontium」，主要的攻擊對象為各國政府、軍事及安全組織，受害者遍布全球。2014烏克蘭總統的選舉中，其就曾發起DDoS攻擊，干擾烏國「中央選舉委員會」；[29]另2016年亦曾攻擊「世界反禁藥組織」(World Anti-Doping Agency，WADA)，並公開當時奧運選手的個人機敏資料。[30]

(二)APT29

又名「舒適熊」，自2008年以來該組織即在俄羅斯境內經營網路間諜活動，其利用社會工程學和釣魚活動，入侵受害者的資料，且能夠執行複雜的技術和長期的攻擊，且可能有國家級別的資金支持。2013年，即運用帶有病毒的虛假「PDF」文檔，模擬在政治方面議題的官方文件攻擊烏克蘭，[31]並且一直在不斷改進和更新他們的駭客武器庫，以及對基礎設施的攻擊策略。該組織經常追求世界各地的高價值目標，最近的目標是從全球醫療機構竊取「COVID-19」疫苗數據。網路安全研究人員並強烈懷疑「APT29」與俄羅斯「聯邦安全局」(FSB)有密切聯繫。[32]

(三)Gamaredo

在2014年烏克蘭將親俄的總統亞努科維奇(Viktor Yanukovych)趕下台前，該組織就把攻擊目標朝向針對烏克蘭政府官員、反對黨成員和新聞工作者，之後進一步針對烏克蘭政府機構下手。[33]自2021年10月開始，該駭客組織就針對烏國包括政府及軍隊等單位組織發動網路釣魚郵件攻擊，戰事爆發迄今仍一直保持活躍。[34]

(四)Turla

係俄國的APT 駭客組織(又名Snake、Venomous Bear、Uroburos和White Bear)且至少從2004年以來就一直活躍迄今。多年來，該組織以美國、烏克蘭或阿拉伯國家為目標，開發了一套龐大的網路攻擊工具，如其中的惡意軟體「Kazuar」，因為功能有限且編碼高效，致一般防毒軟體很難偵測。[35]

(五)沙蟲組織(Sandworm)

該組織成立於2009年，是一個與俄羅斯政府密切有關的駭客小組。其製造的惡意軟體破壞力強，目的是攻擊不同國家的電網，

註29：〈美國防情報局評估俄羅斯網路作戰實力：CyberBerkut發動新一輪「輿論攻擊」〉，E安全，2017年7月17日，https://posts.careerengine.us/p/5ecb6a758e09df08009922ba，檢索日期：2022年5月13日。

註30：陳曉莉，〈微軟：新一波網路攻擊鎖定運動及反禁藥組織〉，iThome，2019年10月29日，https://www.ithome.com.tw/news/133879，檢索日期：2022年5月25日。

註31：〈美國評估俄羅斯網路實力：CyberBerkut輿論攻擊〉，搜狐，2017年7月18日，https://www.sohu.com/a/157998836_257305，檢索日期：2022年5月13日。

註32 ：APT29,Enigma Soft, https://www.enigmasoftware.com/zh-hant/apt29-removal/，檢索日期：2022年5月13日。

註33：〈APT 駭客集團利用 Covid19 新冠肺炎作為誘餌〉，趨勢科技，2020年4月22日，https://blog.trendmicro.com.tw/?p=64059，檢索日期：2022年5月13日。

註34 ：〈俄羅斯駭客組織Gamaredon鎖定烏克蘭下手，資安業者提出更多發現〉，IThome，2022年2月8日，https://www.ithome.com.tw/news/149253，檢索日期：2022年5月13日。

註35：這個後門程式偽裝成一個無害但虛假的微軟 Windows 時間服務程式，能夠上傳、執行或竊取檔案，被編排以註冊自身與攻擊者控制的伺服器建立通信，以接收進一步的指令，範圍從下載和執行任意進程到將命令的結果上傳回伺服器，所以儘管攻擊者從2020年就開始部署它，但是一直沒有被發現。〈研究人員發現，俄羅斯APT駭客組織Turla 在攻擊目標系統上部署新型的second-chance後門程式〉，竣盟科技，2021年9月29日，https://blog.billows.com.tw/?p=1404，檢索日期：2022年5月13日。

曾開發「Send Energy3」病毒在2015年襲擊烏克蘭的電網，2016年12月再度攻擊烏國首都基輔(Kyiv)附近的變電站。[36]2017年「Not Petya」駭客事件、及對美國和法國選舉的干預，還有2018年冬季奧運會開幕式駭客襲擊事件等，都有「Sandworm」的影子。[37]

肆、俄國「網路戰」攻擊手段

俄羅斯在2014年併吞烏克蘭「克里米亞半島」(Crimea)之前，網路攻擊就一直是俄國入侵他國的關鍵工具。2007年及2008年俄國也分別對喬治亞及愛沙尼亞(Republic of Estonia)使用過類似手段，其意圖當然是散播恐慌、造成混亂、分散注意力。長期以來，外界預期俄國的網路攻擊將先於軍事入侵，或與軍事入侵同時發生。透過大量使用DDoS攻擊或以大流量攻擊對方目標伺服器，[38]致使政府官網崩壞、民眾無法連線，造成民心不安。以下就2022年「俄烏戰爭」中俄國使用之「網路戰」攻擊手段(網路攻擊事件，如表三)，分析說明如后：

一、2月24日開戰前

(一)自2015年起，烏克蘭就已多次遭遇駭客攻擊，曾導致上百萬居民斷電6小時；[39]隔年冬天駭客又針對烏國電網植入惡意軟體，致首都基輔供電、供暖遭斷，導致俄羅斯備受國際譴責。此次戰前烏克蘭遭受的「Wiper」網攻，就被發現已預先埋藏3個月以後才啟動。因俄國駭客在平日就已預先計畫發送各式假消息、假影片，連日常寄送電子郵件都附帶埋藏病毒碼的假Word、Excel等文件潛伏至民間企業、政府網站、金融公司等多個地點，靜待時機發動，[40]就如同2014年陸續對烏國進行的斷電、斷網攻擊。因此，俄國駭客被認定為在戰事前，即已長期埋入惡意病毒伺機發動。

(二)基於漏洞和人性弱點的植入係「網路戰」準備重點，因此俄國利用惡意軟體，使用竊取的憑證利用遠端存取資料，同時部署到被攻擊目標的電腦。此番結合2022年前後針對烏克蘭的APT攻擊，這些勒索病毒透過漏洞和社交網路關係，以釣魚信件的形式來進行滲透；這種部署工作為網路攻擊前重要的步驟，屬於戰前準備階段的重點。畢竟俄國對「網路戰」的傾向是有據可查的，過去被可信地指責或證明需對烏克蘭及其周邊

註36：〈美國防情報局評估俄羅斯網路作戰實力：CyberBerkut發動新一輪「輿論攻擊」〉，字媒體，2021年12月15日，https://zi.media/@twpetsearcharlinksnet/post/amyAw7，檢索日期：2022年5月13日。

註37：〈沒有炸彈或武器 這就是俄羅斯可以摧毀烏克蘭基礎設施的方式〉，ALJAZEERA，2022年2月12日，https://chinese.aljazeera.net/news/2022/2/12/沒有炸彈或武器這就是俄羅斯可以摧毀烏克蘭基礎，檢索日期：2022年5月13日。

註38：〈俄羅斯同步發動網路攻擊 烏克蘭政府部門與金融機構網站遭癱瘓〉，風傳媒，2022年2月24日，https://www.storm.mg/article/4210608，檢索日期：2022年5月13日。

註39：指2015年12月對烏克蘭電網的攻擊，當時烏國西部的「伊萬諾-弗蘭科夫斯克」地區完全被駭客入侵，此前，駭客操縱整個系統中大約60個斷路器和變電站，導致超過25萬人電力供應被切斷；與此同時，駭客還對電力公司電話網路發起協同攻擊，這使得與客戶的交流變得更加困難。此外，駭客破壞該公司的備用發電機，這使技術人員自己也陷入黑暗之中。〈招募惡魔 俄羅斯通過互聯網控制世界的計畫〉，ALJAZEERA，2021年4月8日，https://chinese.aljazeera.net/opinions/long-reads/2021/4/8/招募惡魔俄羅斯通過互聯網控制世界的計畫，檢索日期：2022年5月13日。

註40：鍾張涵，〈烏俄網路大戰　專家：中國駭客也在臺灣埋了「數位定時炸彈」〉，《天下雜誌》(臺北市)，2022年3月2日，https://www.cw.com.tw/article/5120248，檢索日期：2022年5月13日。

表三：2021年至2022年2月俄羅斯網路攻擊事件一覽表

日　期	攻擊形態	目　　標	影　　響
2021/2	大規模DDoS 攻擊	烏克蘭安全和國防網站、其他國家機構和企業	網站遭破壞，攻擊結束後仍無法登錄。
2021/7	惡意軟體和發布假文件	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，並傳播有關軍事演習的虛假資訊。
2022 0114	DDoS 攻擊	烏國外交部、國家安全與國防事務委員會等70個網站	全數網站無法連線、幾小時後才恢復。
2022 0215-16	DDoS 攻擊	烏克蘭國防部及武裝部隊網站、兩家銀行	網站無法連線、服務中斷。
2022 0223	DDoS、Wiper攻擊	烏國外交、內政、國防部、國家安全局等多部門網站；兩大國營銀行及其他金融網站	1. 基輔、第二大城哈爾科夫、港口馬利烏波爾(Mariupol)等城市網路陸續斷線、網站無法連線、服務中斷。 2. 惡意程式「HermeticaWiper」在3個多月前即植入烏國電腦。
2022 0224	DDoS 攻擊	烏國首都基輔、哈爾克夫及烏克蘭部隊	1. 基輔的網路流量下降了六成；包括哈爾科夫在內居民遭停電或斷網，約70個政府網站癱瘓。 2. 烏軍個人手機接收到訊息。

資料來源：參考Great-Power Offensive Cyber Campaigns: Experiments in Strategy, International Institute For Strategic Studies,24 February,2022,p57；Andrew S. Bowen, Russian Military Intelligence: Background and Issues for Congress, November 15, 2021, p.18；鍾張涵 ，〈烏俄網路大戰 專家：中國駭客也在臺灣埋了「數位定時炸彈」〉，《天下雜誌》(臺北市)，2022年3月2日，https://www.cw.com.tw/article/5120248，檢索日期：2022年5月13日，由作者整理製表。

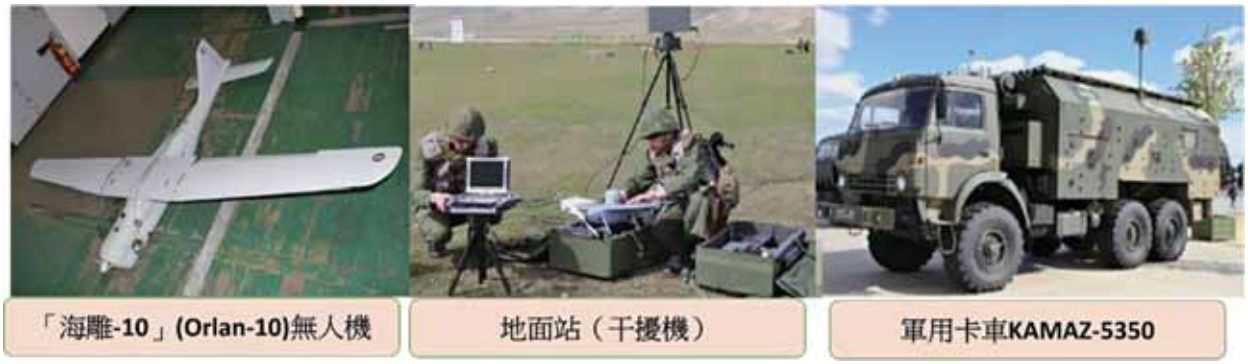
鄰國的多次網路攻擊負責，包括2007年愛沙尼亞、2008年喬治亞，和2009年吉爾吉斯(Kyrgyz Republic)的DDoS攻擊。[41]

(三)2022年1月15日，微軟公司的「威脅情報中心」(Microsoft Security Response Center，MSTIC)即已發現針對烏國政府和多個組織的破壞性惡意軟體「耳語門」(Whisper Gate)操作的證據，該軟體於該月13日首次出現在烏克蘭的被攻擊電腦系統上，[42]到了14日，烏國外交、教育、內政及能源部等多個政府網站因遭到大規模網路攻擊而關閉；[43]15日，烏國國防部、武裝部隊等多個軍方網站和銀行的網站同樣遭到大規模網路攻擊而關閉。23日，該國外交、國防、內政、安全局等政府機構及兩家大型銀行(包括最大的商業銀行Privat bank及國家儲蓄銀行Oschad bank)的網站，再次成為DDoS攻擊的目標，到了晚間22時52分，烏國數百台電腦上發現新型惡意資料刪除軟體「Hermetic Wiper」，涉及目標包括金融及政府

註41：2015、2017年，烏克蘭的電網因惡意軟體變種BlackEnergy和Industroyer/CrashOverride 而遭受兩次單獨關閉時，大部分證據也都指向俄羅斯。David Ruiz, Potential cybersecurity impacts of Russia’ s invasion of Ukraine, February 25, Malwarebytes LABS,2022,https://blog.malwarebytes.com/malwarebytes-news/2022/02/potential-cybersecurity-impacts-of-russias-invasion-of-ukraine/，檢索日期：2022年5月13日。

註42：WhisperGate惡意軟體 具有破壞性，能使目標設備無法運行。Destructive Malware Targeting Organizations in Ukraine, CISA, March 01,2022,https://www.cisa.gov/uscert/ncas/alerts/aa22-057a，檢索日期：2022年5月13日。

註43：〈深度剖析-俄烏衝突中網路攻擊的五大特徵〉，搜狐，2022年2月26日，https://www.sohu.com/a/525634068_327908，檢索日期：2022年5月13日。



圖二：俄軍「里爾-3」電子戰系統組成

資料來源：參考〈資訊戰同步開打，烏克蘭軍收大量心戰簡訊又遭DDoS攻擊〉，科技新報，2022年2月24日，https://technews.tw/2022/02/24/ukrainian-is-under-massive-ddos-and-information-warfare-attacks/，檢索日期：2022年5月13日，由作者綜整製圖。

承包商。到24日清晨，俄羅斯正式對烏克蘭開戰，顯見攻擊前的準備均「按部就班」。[44]

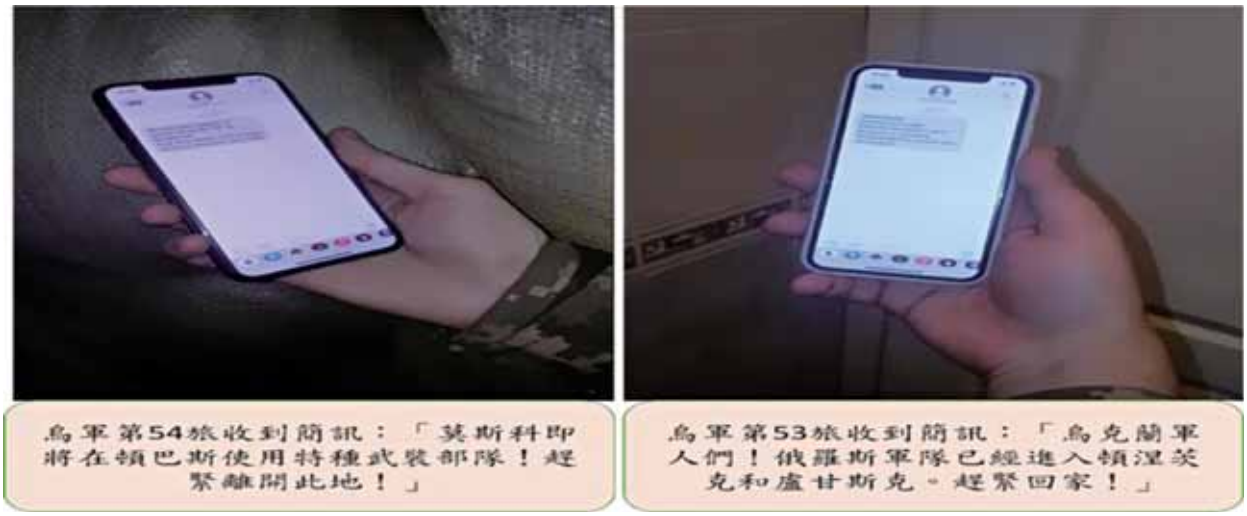
二、2月24日開戰後

(一)網路作戰不分平時和戰時，戰前準備具有較高的隱蔽性，操作在「平時」，運用於「戰時」；看得到的是作戰效果，看不到的是作戰準備，而作戰過程可在短時間內甚至瞬間完成。如網路攻擊中的惡意軟體「耳語門」就在紛爭前已經完成植入；[45]部分惡意軟體甚至提前3個月就準備完成，並在開戰日之前植入。網路攻擊已成為開戰首要選擇武器，並結合傳統作戰力量和作戰方式，有效實現多維領域作戰。

(二)此次戰爭爆發前，俄國駭客大規模的網路攻擊早在1月中旬便開始發動，再次攻擊行動出現在2月中、下旬，對象都是烏國政府機關與國營銀行，他們的網站遭到DDoS攻擊而癱瘓；再者，駭客也透過資料破壞軟體「Wiper」來對這些機關的電腦下手。[46]儘管每個波次攻擊的重點都不同，但總體而言，軍、政安全機制、能源、金融秩序已成為主要的目標，透過影響政府運作、擾亂經濟秩序等方式，其警示的意味非常明顯。戰爭開始後，除協同傳統作戰力量外，各組織亦根據前期網路偵察，對烏國重要電腦實施資料刪除之網路攻擊。

(三)俄國也使用無人駕駛飛行器(UAV)和地面系統對衛星、蜂窩和無線電通信系統進行電磁偵察和干擾，並對烏克蘭無人機進行GPS欺騙和電子戰攻擊。[47]「里爾-3」電子戰系統(RB-341V)載台由干擾機和「海鵰10」(Orlan-10)無人機構成(如圖二)，能夠破壞目標網路，並能向網路用戶發送虛假信息。由於俄羅斯有較為先進的電子戰設備，可以快速對烏克蘭士兵的手機進行定位發送簡訊，例如先向烏軍官兵手機發送「離開，不

註44：同註39。
註45：同註30。
註46：同註23。
註47：同註13。



圖三：俄軍傳訊息至烏克蘭軍隊手機

資料來源：參考〈資訊戰同步開打，烏克蘭軍收大量心戰簡訊又遭DDoS攻擊〉，科技新報，2022年2月24日，https://technews.tw/2022/02/24/ukrainian-is-under-massive-ddos-and-information-warfare-attacks/，檢索日期：2022年5月13日，由作者綜整製圖。

然就等死！」然後傳訊給士兵家屬，告訴他們「你們的兒子(丈夫)已經死了」，再打電話到士兵手機占線，或是馬上砲擊手機訊號所在位置(如圖三)。[48]

(四)從2月24日開始，俄國網軍已對烏國政府和軍方網路進行一連串DDoS攻擊，藉由瞬間大規模的流量湧入，造成網路癱瘓，使得烏國外交部、國防部和許多企業、銀行網站無法使用。[49]首都基輔的網路流量下降六成，第二大城哈爾科夫(Kharkiv)在內，都遭受停電或斷網，即使烏克蘭的網路供應商在官方「Instagram」頻道中不斷更新修復訊息，仍有許多居民無法順利連網。[50]

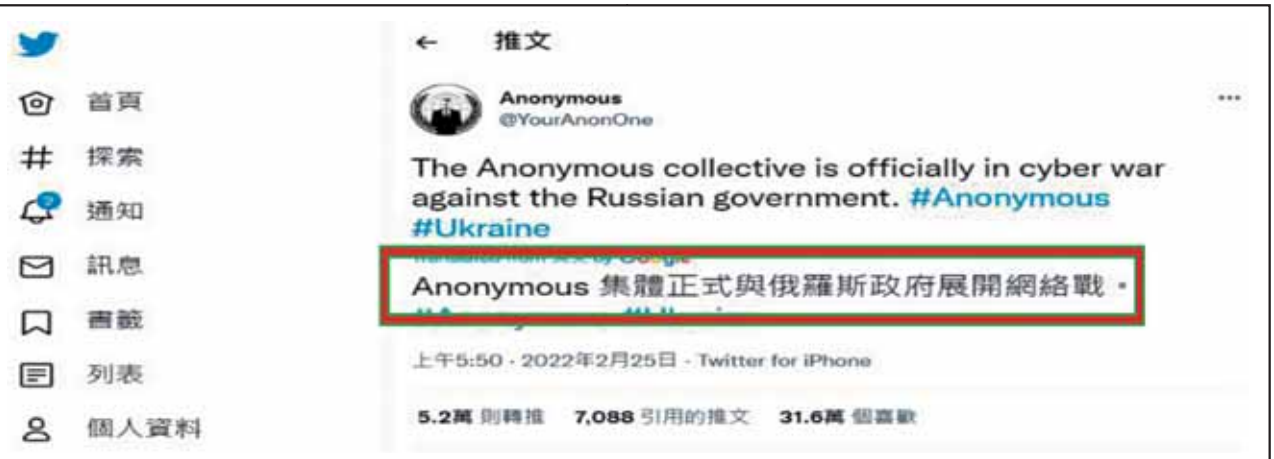
俄羅斯有鑑於網路如果癱瘓，將嚴重影響內部金融、軍事等領域，所以長期以來一直對網路威脅保持警惕，[51]俄國政府並準備啟動自己的「主權互聯網」(Runet)，目前正在與「國家電腦事故協調中心」(National Computer Incident Response & Coordination Center)進行研究，以應付駭客對關鍵資訊基礎設施的攻擊，同時做好啟用「Runet」的準備。因為俄羅斯長期以來即認為，在社交媒體影響力和網路攻擊日益增加的背景下，建立「主權互聯網」是必不可少

註48：同註20。

註49：同註20。

註50：〈烏克蘭被「禁言」！幕僚建議拜登：對俄羅斯進行網路攻擊〉，《遠見雜誌》(臺北市)，2022年2月26日，https://www.gvm.com.tw/article/87464，檢索日期：2022年5月28日。

註51：「Rubnet」是俄羅斯出於國家網路防禦目的, 而構建的一個脫離全球互聯網的內部局域網。俄國為維護國內網路安全，2019年11月即進行大規模「斷網」，以測試內部網絡「Rubnet」，檢測是否可在沒有全球互聯網的情況下正常運作。黃郁文，〈俄羅斯「斷網」測試：擺脫西方網絡威脅〉，三策智庫，2019年11月1日，http://www.senstrat.com/Article/s247.html，檢索日期：2022年5月28日。



圖四：駭客組織「匿名者」於社群媒體上向俄羅斯宣戰

資料來源：參考Anonymous@YourAnonOne, Twitter, February 25, 2022 ,https://twitter.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw，檢索日期：2022年5月28日，由作者調整製圖。

的作法。[52]即便如此，開戰迄今俄國除網路攻擊成效明顯外，至於在其他軍事行動上，似乎進展並不順利，此次戰場最終結果如何，恐仍有待觀察。

伍、烏克蘭與盟友的反制作為

在俄羅斯以軍事行動進攻烏克蘭的同時也發動網路攻擊，而烏國政府也呼籲國內的駭客，一同協助抵禦；除保護國內基礎設施不再受駭客襲擊外，也針對俄國軍隊進行網路情蒐與反擊。以下就烏克蘭與盟友的反制作為，概要說明如后：

一、招募民間志願者參與

面對大規模、多波次的DDoS攻擊，烏克蘭網路力量於初期缺乏有效的應對之策，為改善這種形勢，該國「數位轉型部長」號召自願者協助組織「IT軍隊」，[53]以網路安全公司「Cyber Unit Technologies」為其核心，政府則透過該公司在社交媒體上鼓勵其他網路專家加入，透過成員豐富的網路安全經驗，蒐集有關俄國境內戰爭和潛在目標的情報，並與烏國政府分享。[54]烏國政府也招募民間志願者以網路攻擊做為反擊，連全球最大駭客組織「匿名者」(Anonymous)都回應招募令，同時對俄國開展DDoS攻擊，並於2月25日在社群媒體「推特」(Twitter)上發文，正式對俄羅斯發動「網路戰」(如圖四)，儘管主要攻擊對象是俄國政府，不過也會

註52：俄總統普丁在2019年5月就簽署《互聯網主權法》，根據這一法律，俄國互聯網基礎設施將逐步擺脫對境外網路的依賴，尤其是在遭受外部攻擊時，俄羅斯可以獨立運行國內互聯網；此前，俄國相關部門多次進行過互聯網斷網測試並取得成功。〈俄媒：俄準備啟用本國互聯網〉，環球網，2022年3月2日，https://world.huanqiu.com/article/471U8axR0MX，檢索日期：2022年5月28日。

註53：已有超過31.1萬人已經在社交媒體平台Telegram加入一個名為烏克蘭「IT軍隊」的組織，共同目標是攻擊俄羅斯。〈要讓俄羅斯回到石器時代！揭密烏克蘭31萬人「IT大軍」〉，蘋果新聞網，2022年3月25日，檢索日期：2022年5月8日。

註54：〈襲擊俄羅斯的網絡游擊隊：烏克蘭IT軍隊的真實身份〉，Yahoo，2022年2月25日，https://tw.stock.yahoo.com/news/襲擊俄羅斯的網絡游擊隊-烏克蘭it軍隊的真實身份-151300546.html，檢索日期：2022年5月28日。

涵蓋該國的私人企業。[55]

二、由多國共同協助進行網路攻防

由美國微軟(Microsoft)公開對全世界發布的訊息表示，在俄羅斯發動攻擊前數小時，一項被指稱為「FoxBlade」的網路惡意行動，已針對烏克蘭政府各組織，金融機構發動攻勢，該惡意行動被微軟的「情報中心」發現，馬上進行反制措施、拆解病毒，並提供防禦軟體成功攔截這項攻擊。[56]2月22日由「立陶宛」領導的12人團隊，成員包括來自愛沙尼亞、荷蘭、立陶宛、克羅埃西亞、羅馬尼亞和波蘭等國，儘管當時仍在烏克蘭訪問，也立即幫助抵禦俄羅斯對烏國的遠程和戰場網路攻擊。[57]烏國政府也呼籲國內的駭客，一同協助保護國內基礎設施不受外國襲擊外，也針對俄羅斯軍隊進行網路情蒐。

三、組織「網路戰」反制俄軍

烏國共列出包括俄國政府單位IP位址(Internet Protocol Address)、政府儲存設備及郵件伺服器，其他如國營銀行、支持基礎架構的業者，甚至俄羅斯搜尋引擎「Yandex」等31個網路攻擊目標。[58]另一方面，基於參與戰爭的軍人個資若落入敵營，很有可能影響該部隊士氣戰志。根據烏國新聞網站的報導，「烏克蘭國防戰略中心」已取得部分俄國參戰軍人的名冊，當中包含姓名、護照號碼及所屬單位等資料，共約12萬名軍人名列其中；該網站同時公布這份名單，咸信已對俄國軍隊士氣造成影響。[59]前美國國務卿希拉蕊(Hillary Diane Rodham Clinton)甚至呼籲美國駭客也對俄羅斯發動網路攻擊，同時烏國政府也向韓國提出請求，希望提供網路安全方面的援助，以提升應對俄國網路攻擊的能力。[60]

四、國外民間企業投入網路通訊

美國民間企業「馬薩爾科技」(Maxar Technologies)則出動商用衛星影像，打破傳統衛星影像被軍事衛星壟斷局面，讓俄軍動態屢屢曝光。[61]此外，受到俄國入侵影響，烏克蘭部分地區網路中斷，若烏國網路設施繼續遭到破壞，毫無疑問受益者是俄羅斯。從以往戰爭經驗檢視，如果戰爭地區發生

註55：曾凡芸，〈向俄羅斯網路攻擊宣戰：烏克蘭呼籲國內駭客「協助抵禦攻擊」、全球最大駭客團體對俄進行網路戰〉，關鍵評論，2022年2月25日，https://www.thenewslens.com/article/163306，檢索日期：2022年5月28日。

註56：〈郭台銘：資安即國安 整合組織全面防禦網路戰〉，中央社，2022年3月6日，https://www.cna.com.tw/news/aopl/202203060139.aspx，檢索日期：2022年5月8日。

註57：Gareth Corfield,Ukraine hit by DDoS attacks, Russia deploys malware,The Register,23 Feb,2022,https://www.theregister.com/2022/02/23/ukraine_ddos_russia_malware/，檢索日期：2022年5月8日。

註58：Yandex是一家俄羅斯網際網路企業，旗下的搜尋引擎在俄國內擁有逾60%的市場占有率。林妍溱，〈駭客組織分別加入俄、烏陣營開戰〉，IThome，2022年2月28日，https://www.ithome.com.tw/news/149578，檢索日期：2022年5月8日。

註59：周峻佑，〈【資安日報】2022年3月〉，IThome，2022年3月4日，https://www.ithome.com.tw/news/149704，檢索日期：2022年5月8日。

註60：〈俄烏衝突網空態勢研判：關基成網攻重點 俄方克制使用高級能力〉，互聯網安全內參，2022年2月28日，https://mp.weixin.qq.com/s/uAitou40B8ebiFJfSwJh2Q，檢索日期：2022年5月28日。

註61：傳統光學影像衛星利用可見光與紅外線感測器產生圖像，缺點是無法穿透雲層或拍攝夜間清晰影響；新世代影像衛星則搭配合成孔徑雷達(SAR)，既能穿透雲層，也能在夜間使用，還需要透過檔案調整成為具情報價值之照片；而衛星公司雖擅長技術層面，卻需要更多有效情報與指導，方能「讓衛星拍攝正確的位置」。美國「國家偵察辦公室」(NRO)以每年3億美元(約新臺幣84億元)合約，優先存取「Maxar Technologies」的4枚遙測衛星拍攝資訊。〈商用衛星影像 讓俄軍動態全都露〉，《青年日報》，2021年3月1日，版9。

網路中斷，通常代表侵犯人權事件的風險大幅提高；[62]據此，美國「太空探索科技公司」(SpaceX)執行長馬斯克(Elon Musk)，隨即於2月26日宣布旗下「星鏈」(Starlink)衛星寬頻網路服務已在烏克蘭啟用，衛星網路由於不需要建設實體線路，[63]有助於在當地網路因戰火而阻斷時，仍能繼續提供資訊流通，有助烏國對外聯繫及訊息收送。

五、社群媒體發揮重要作用

「輿論戰」、「心理戰」做為網路攻擊的一部分，也在這本次戰場中發揮重要作用，並成為重點關注對象。通過網路空間發布有利於己方和不利於對方的虛實資訊，既可以試探對手反應，也可以起到震懾的作用，最終達到瓦解人心、改變作戰進程的意圖。例如，影片平臺「You Tube」於3月1日宣布封鎖「今日俄羅斯」與「俄羅斯衛星通訊社」的傳播頻道；而「臉書」(Face book)集團母公司也宣布封鎖在歐洲登錄的這兩家媒體在「臉書」以及子公司「Instagram」的官方帳號。同日「谷歌」(Google)也將這兩家媒體軟體從其應用軟體商店下架；甚至「微軟」集團也做出了同樣舉措，並表示正調整相關演算法，以增加這兩家媒體在搜索結果中出現的難度，[64]此正凸顯社群媒體已在現代網路作戰中占有重要的一席之地。

「烏俄戰事」迄今仍未結束，烏克蘭總統澤倫斯基(Volodymyr Zelensky)為贏得支持者聲援，不僅通過視訊向西方國家爭取重型武器援助，在其他國家國會演講，呼籲國際加強制裁俄羅斯，還指責俄軍侵略犯下的各種「罪狀和暴行」，激發國民同仇敵愾心理與抗敵意志，希望繼續吸引世界各國的聲援與支持，烏國並在網路世界、社群媒體持續展開全面的進攻，究竟能否協助烏國獲勝，目前「鹿死誰手」尚未可知；但此刻烏國各大城焦土一片、而逃難人數更已突破600萬人以上，仔細深究這場戰爭勝負或許早已出現端倪，而這才是輕忽戰爭所帶來的慘痛代價。

陸、省思-代結語

「他山之石，可以攻玉」。在「資安即國安」的前提下，網路安全已經成為全民共識。此次對「烏俄戰爭」中的「網路戰」作為，謹提供以下幾點省思，提供國人及政府單位參考：

一、俄羅斯以軍事行動進攻烏克蘭的前後，也同時發動網路攻擊，而烏國也有相關反制作為，例如總統澤倫斯基每天發表附上英文字幕的談話影片在網路瘋傳，國防和外交部長則圖文並茂地強調該國如何奮力的進行軍事抵抗。與此同時，烏國人民也展示反擊成功的影片也在網路流傳，其中包括飛彈擊落俄軍直升機，以及農民用拖拉機拖走俄國武器裝備等等，[65]均展現出奮戰到底的決

註62：〈禁言的戰爭：烏克蘭網路搖搖欲墜，幕僚建議拜登執行網路攻擊〉，科技新報，2022年2月25日，https://technews.tw/2022/02/25/ukraine-internet-outages-spark-concerns-of-broader-blackout/，檢索日期：2022年5月8日。

註63：〈馬斯克啟動「星鏈」助烏網路不中斷〉，《青年日報》，2022年2月28日，版6。

註64：這些網路平台並非新聞媒體，其本質原是傳播盈利，但大都選擇參加抵制俄羅斯的行動。〈俄烏衝突信息戰：俄對外宣傳機器在歐洲遭遇全面阻擊〉，FRI，2022年3月2日，https://www.rfi.fr/cn/專欄檢索/今日經濟/20220302-俄烏衝突資訊戰-俄對外宣傳機器在歐洲遭遇全面阻擊，檢索日期：2022年5月8日。

註65：〈烏克蘭強打資訊戰 網路火力更勝俄羅斯〉，中央社，2022年3月6日，https://www.cna.com.tw/news/aopl/202203060139.aspx，檢索日期：2022年5月8日。

心，但亦有西方學者認為，烏克蘭不僅應在輿論上創造英雄事蹟及民眾的痛苦資訊，更要整合全般「網路戰」反制作為，方有機會贏得戰爭。[66]觀察目前戰場上發出的訊息內容確實真偽難辨，但至少已達到影響輿論風向之目的，致多數國家一致譴責俄羅斯；然對戰場勝負是否真有助益，尚待時間驗證。

二、「網路戰」為先戰之戰，網路攻擊則成為一種新型武器。部分國家透過駭客攻擊敵國的電力網路、金融市場和政府電腦系統，所帶來的毀滅性後果並不亞於有形武器及炸彈的威力。網路被破壞或中斷是戰爭全程均會發生的狀況，而現代戰爭網路設施關閉或被攻擊，通常代表會引發更嚴重的後果，如2022年2月沙烏地阿拉伯就曾空襲葉門電信基礎設施，成功控制訊息傳播且更容易達成戰略目標就是一例；另一方面，網路關閉代表媒體更難獲得重要消息，甚至連當地人也難取得安全保障的消息。所以相關網路備援計畫及方案也需要在平時即先行策訂，才能在訊息萬變的資訊戰場上「防範未然」。

三、中共對我網路作戰練兵從未間斷，在科技日益高度化的世界中，「網路戰」將在破壞我國防禦系統、指揮控制中心和國家基礎設施方面，發揮關鍵作用；我國除需防範來路不明的惡意程式外，更應高度關注與提高警覺。因為「網路戰」具有多樣性及多變性的攻擊方式與手段，尤其攻者「形於無形」，守者往往「防不勝防」。故就資訊安全領域而言，唯有建構多層之安全防護機制，主動提供技術支援服務，才能提升我國資訊優勢與網路安全。當前臺海局勢嚴峻，爆發大規模戰爭的疑慮正不斷升溫，勢必連帶推升更多資安預算支出。我國政經情勢特殊，目前除已積極推動各項網路安全政策外，並應提高資安人才培訓能量、開發資安產業創新技術，藉以強化國家對於各種網路安全事件的緊急應變與協調能力，也才能在第一時間解決突發的資安、網路攻勢。

四、我國為全球重要供應鏈之一環，也處於地緣政治的關鍵角色，在資通安全的風險管控上，更不容掉以輕心。科技發展和資通安全相關的進步立法，也應與時俱進，跟上世界的脈動；[67]因為網路安全不僅是我國的挑戰，也是機會。尤其我國半導體產業居全球供應鏈重要角色，如何在政府的整體政策下，結合公、私部門組織與法制的協力運作，全力打造獲世界信賴的資安系統及產業鏈，未來透過持續強化資安聯防能量，並與友好國家增進資安科技交流及情資分享，才能落實防範及反制國際網路駭侵與惡意攻擊，[68]確保我國網路安全。

當前「網路戰」正對我國整體安全，形成長期性的威脅，如何因應已成為國家安全的當務之急，在面對敵人「無時無刻」且「無所不用其極」地意圖侵犯我國的同時，國

註66：Stuart A. Thompson and Davey Alba, “Fact and Mythmaking Blend in Ukraine’s Information War,” The New York Times, March 3, 2022, https://www.nytimes.com/2022/03/03/technology/ukraine-war-misinfo.html. Visited date: April 13, 2022，檢索日期：2022年5月18日。

註67：同註56。

註68：國防報告書編纂委員會，《中華民國110年國防報告書》(臺北市：國防部，2021年10月)，頁33。

軍更需要強化我網路戰防護作為，增加抵抗能力。「俄烏戰爭」期間，儘管俄軍在網路戰及軍事作戰層面相對於烏軍仍占優勢，但在包括認知戰、輿論戰、心理戰、法律戰和宣傳戰等廣義的資訊作戰領域上，與烏克蘭相比，似乎「相形見拙」。但這場戰爭之禍未見盡頭，且全球仍處在戰爭風險與危機中，但誰是戰爭中的真正獲利者，猶待時間驗證。

面對中共迄未放棄武力解決臺海問題、面對軍事力量數倍於我國的中共，「網路戰」等資訊作戰領域將是我國可以大加發揮之處，國軍各單位平時即可勤於耕耘網路作戰領域，厚植網路攻防能量，且除「通資電軍」持續擔負國軍網路及電子戰的戰力整合的角色外，對資訊安全教育亦需要高度重視，透過激發學校的教育和研究能量，引導國內產業的升級轉型，並強化學術和產業界密切的交流，俾在資訊安全的技術水準與全球市場競爭力上，繼續「頭角崢嶸」、奠基實力、補強戰力。再透過國際合作、情資傳遞共享，與友好國家建立聯防機制及協助我參與國際網路空間之支持；如此多管齊下，咸信在我國「上下一心」的充分準備下，定能無懼敵人網路攻勢，克敵致勝。 ⚓

作者簡介：

黃郁文先生，備役陸軍上校，中正理工學院專科83年班、政治作戰學校93年班、國防大學陸軍指揮參謀學院96年班、國防大學政治研究所102年班、國防大學戰爭學院104年班。曾任政戰主任、國防大學教官、退輔會專員，現為淡江大學整合戰略與科技中心副研究員暨國際事務與戰略研究所博士候選人。

老軍艦的故事

廬山軍艦 PF-836

廬山軍艦原為美海軍BULL號，編號APD-78，由美國丹佛造船廠建造，1943年8月12日成軍服役。

民國55年美國依據軍援政策將該艦售予我國，於同年12月19日拖抵左營港，12月22日由總司令馮啟聰中將主持升旗典禮，命名為「廬山軍艦」，隸屬驅逐艦隊。

廬山軍艦成軍後，主要執行海峽偵巡及外島運補護航，民國57年曾與壽山軍艦納編敦睦遠航支隊，前往關島、中途島、夏威夷及沖繩等地訪問，於民國84年10月1日功成除役。(取材自老軍艦的故事)