從俄羅斯網路戰發展對我陸軍資電作戰構建之啓示

作者簡介

黃基禎上校，理工學院78年班、美國大學資訊研究所碩士、英國大學政治學博士；曾任排長、連長、人參官、教參官、編譯官、研究教官、外連官，現任國防大學助理教授。

王清安中校，中正理工學院88年班、通資電正規班175期、陸院98年班；曾任排長、連長、營長、群參謀主任，現任戰爭學院學員。

提要

一、2016年美國總統大選前，俄羅斯運用網路攻擊以影響該國選舉結果。回顧俄羅斯十年來網路戰運用，從癱瘓敵國網路到運用網路影響他國民主機制，網路戰的作戰型態已向多元、複雜型態發展。

二、為因應網路作戰型態的改變，俄羅斯國防部於2016年新編「資訊和大眾傳播部」。同時，對外承認已建制網路部隊。另外，透由資訊產業自主及網路科技國際合作，以強化網路戰整體戰力。

三、面對中共解放軍資電作戰之威脅，借鏡俄羅斯網路戰發展經驗，本文提出強化網路安全演練機制、爭取網路聯合作戰，及建構網路科技自主能量等3建議，以利我陸軍因應未來網路戰之挑戰。

關鍵詞：網路戰、網路部隊、駭客、病毒

前　言

2017年5月9日，美國國安局長兼網路司令部司令羅傑斯(Mike Rogers)上將於國會報告時表示，2016年底美國大選期間，俄羅斯運用網路駭客攻擊民主黨總統候選人希拉蕊(Hillary Clinton)電子郵件，企圖干涉美國民主運作。[1]回顧2007、2008年，俄羅斯分別針對愛沙尼亞及喬治亞共和國網路、通訊等關鍵基礎設施實施網路攻擊，進而癱瘓其銀行、交通等設施；其中令人注意的是，於2008年對喬治亞共和國發動軍事攻擊前，運用網路媒體宣傳手段，以獲取發動戰爭的正當性，最後贏得戰爭勝利。[2]雖然，俄羅斯矢口否認美國對其網路攻擊行為的指控，但根據2017年10月底Facebook提供美國聽證會的資料表示：從2015年6月～2017年8月間，俄羅斯特工人員申請假帳號，透過Facebook發出約8萬多則有關種族問題在內的分裂社會之消息。[3]隨著網路戰攻擊對象的改變，其意味著未來網路戰的作戰型態，也將隨之發生變化。

事實上，自2017年起，我國已有專家學者呼籲，針對複合式網路戰爭型態，國軍必須儘早完成整備。根據2017年9月13日，我國中華戰略暨兵棋研究會理事長黃介正博士出席國防部研討會時表示：未來戰爭的發展趨勢，不能僅侷限於「制空、制海、反登陸」的思維；而是要將敵、我間對於網路、通訊可能的攻防，及透過社群網路傳播的真、假資訊，納入軍事戰略思維。[4]同年10月，我國國防大學副校長丘樹華中將出席「第11屆軍事新聞學術研討會」更強調，數位傳播時代的來臨，對國軍將是一項重大的考驗。[5]因此，準備打贏複合式的網路戰，對我陸軍建軍備戰將是愈來愈重要。

俄羅斯網路戰之概述

遂行任何軍事行動，必須在統一思想上，建立合作無間的行動準繩。而定義

1　Dan Boylan, "NSA chief, to Senate: Cyberattack on infrastructure worst-case scenario," The Washington Times, https://translate.google.com.tw/translate?hl=zh-TW&sl=en&u=http://www.washingtontimes.com/news/2017/may/9/mike-rogers-nsa-chief-senate-cyberattack-infrastru/&prev=search, May 9, 2017.

2　東鳥，《鍵盤狙擊手 ── 不見硝煙的網路戰爭，殺傷力卻更為驚人》(臺北：上奇資訊，2015)，頁50～52。

3　Mary Clare Jalonick? and Barbara Ortutay,"Tech companies find more signs of Russian election activity", Fox business, http://www.foxbusiness.com/features/2017/10/30/facebook-russia-linked-posts-distributed-to-126m-users.html, October 30, 2017.

4　黃德潔，〈整評司講座 探討國防戰略新思維〉《青年日報》(臺北)，2017年9月14日，版4。

5　鄭豪，〈新媒體傳播 創新肆應挑戰〉《青年日報》(臺北)，2017年10月6日，版3。

與目的，即為賦予部隊遂行任務的行動指南。

一、網路戰之定義

隨著網路、通訊技術的提升，網路空間的範圍已由實體線路，擴及至資訊終端用戶。根據2013年，于忠杰研究指出：俄羅斯網路戰即對敵指揮所通資系統發動攻擊，或阻止敵方使用網路資訊，最終癱瘓敵方整體運作。[6]另外，根據2016年北約國防大學副教授Keir Giles表示，俄羅斯的網路戰，除包括實體基礎設施的物理層，如實體電路，還包含影響人類資訊處理的認知領域層。[7]因此，俄羅斯的網路戰戰略構想，為運用網路於平、戰時造成敵國內部政治動亂，進而影響政府運用機制。戰時，再輔以癱瘓敵國通資系統，影響敵國聯合作戰效能。簡言之，俄羅斯所發展出的網路戰即為「不戰而屈人之兵」最佳作戰型態。

二、網路戰之目的

明確的作戰目標，有利指揮官統合戰力贏得勝利。根據2010年，馬建光研究表示，俄羅斯的網路戰運用構想，與傳統火力制壓運用極為相似，於攻擊前，運用網路攻擊癱瘓敵國網路，以達擾亂敵國社會秩序。戰時，運用軟、硬殺手段，破壞敵方通資系統，以降低敵軍聯合作戰反應能力。[8]此外，2016年2月，俄羅斯國防部長史久(Sergei Shoigu)出席俄羅斯「杜馬議會」(Russian parliament ,Duma)時強調：俄羅斯的網路部隊，將以聰明、準確、有效的運用網路宣傳及反宣傳，以分散敵國活動，獲取戰爭勝利。[9]不僅如此，根據2016年Keir Giles指出，俄羅斯的網路戰為實現政治或外交為主要目的。和平時期採取網路偵察，掌握敵國重要資訊；戰時，配合網路攻擊，發布虛、假資訊，煽動敵國內部人民政治意識形態分化，取得有利於自身的戰爭面及國際話語權。[10]因此，運用網路平台散布謠言，瓦解敵國內部抗敵意志。同時，運用網路攻擊癱瘓敵國網際網路，進而影響敵國政治、經濟、

6 于忠杰，〈俄羅斯網路與信息安全的做法與啟示〉，黃藝主編，《網路空間安全戰略研究》(北京：國防大學出版社，西元2013年)，頁336。

7 Keir Giles, Handbook of Russian Information Warfare (ROMA:NATO Defense College Cataloguing, 西元2016), P. 9.

8 馬建光、李宗源，〈俄軍網路戰能力不可小覷〉《環球軍事》(北京)，22期，新世界出版社，西元2010年9月，頁46。

9 Sergey Sukhankin, "Russian Cyber Troops: A Weapon of Aggression, "Real clear defense, https://www.realcleardefense.com/articles/2017/05/12/russian_cyber_troops_a_weapon_of_aggression_111368.html, May 12, 2017.

10 同註7, pp.10-11.

交通及軍事等安全，將成為未來網路戰發展新趨勢。

俄羅斯網路部隊與預算

要捍衛網路空間的安全與利益，必須編組網路部隊及挹注經費。

一、網路部隊編組

隨著網路安全威脅日益增加，構建網路空間的安全體系，必須整合國防、國安及內政等三大體系。故俄羅斯網路空間安全部門，為「俄聯邦資訊政策委員會」統籌運用國防部網路部隊、俄聯邦安全局及俄聯邦保衛局(國務院)所構建而成。[11]各部門責任，分述如後：

(一)俄聯邦資訊政策委員會

要確保網路安全，必須避免多頭馬車的行政部門出現。俄羅斯網路安全政策制定，由俄聯邦資訊政策委員負責，其委員會主席由總統擔任。下設網路安全委員會設有「國家網路安全回應中心」，以協調聯邦各部門，與民營企業資訊共享。[12]另外，為強化網路防護能力，由俄聯邦「通信部」負責評估國內網路穩定性，並針對網路演習所暴露缺點，制定有效措施；「媒體與文化管理局」負責監控新聞媒體。[13]因此，在統一領導推動網路安全下，各項資源獲得最好的分配。

(二)國防部

為確保網路空間利益不受侵犯。2014年，俄羅斯「聯邦委員會」提出利用「白色駭客」(無犯罪前科的網路專家)組成網路部隊；其任務為對國家境內發動網路攻擊，以加強化政府、企業網路安全防護能力。[14]同年，為保護俄羅斯國防網路安全，在其國防部內部設立「資訊作戰總局」(information warfare directorate)，從事網路戰攻、防演練。[15]另外，在網路防護特種分隊包括網路監測中心、資訊安全評估中心、應急處理中心、資訊安全研究中心等。[16]此外，俄羅斯國防部所屬軍種

11 惠志斌，《全球網路空間信息安全戰略研究》(上海：上海世界國企出版公司:2015年4月)，頁96。

12 王舒毅，〈俄羅斯網路安全戰略的主要特點〉《保密工作》(北京)，2016年第8期，保密工作雜誌社，2016年8月，頁45。

13 劉勃然，〈俄羅斯網路安全治理機制探析〉《西伯利亞研究》(黑龍江)，第43卷第6期，西伯利亞研究雜誌社，2016年12月，頁31。

14 周季禮，〈2014 年俄羅斯網路空間安全發展舉措綜述〉《中國資訊安全》(北京)，2015年10期，國家資訊技術安全研究中心，2015年8月，頁101。

15 Pavel Felgenhauer, " Defense Minister Shoigu Promotes Russian Cyber Warfare Troops and Declares Victory in Syria," Eurasia Daily Monitor Volume: 14 Issue: 23, https://jamestown.org/program/defense-minister-shoigu-promotes-russian-cyber-warfare-troops-declares-victory-syria/, February 23, 2017.

16 同註11，頁97。

內編組通信部隊，強化遂行軍事作戰任務。[17]不僅如此，為強化網路心理作戰效能，2016年俄羅斯國防部新增「資訊和大眾傳播部」(Department of Information and Mass Communication)，與聯邦安全局及情報局(Foreign Intelligence Service, SVR)共同負責網路攻擊。[18]由俄羅斯網路部隊編組透露出，未來網路戰的作戰型態，將著眼於瓦解敵國內部抗敵意志，及癱瘓敵國指管通資系統使其網路空間隔離於世界之外。

不僅如此，為強化網路科技研發能量，國防部成立獨立部門－科技部，以負責監測和處理網路威脅資訊。[19]根據2010年中共《環球軍事》指出，俄羅斯國防部與民間網路安全公司(Dr.web)及「卡巴斯基實驗室」等合作。[20]另外，根據2017年Sergey Sukhankin研究指出，自2001年起，俄羅斯的一家軟體公司已配合國防部，成立「秘密網路部隊」(secretive cyber troops)，以強化其網路戰能力。[21]故從俄羅斯國防部籌建科技部凸顯出，影響網路戰勝敗的關鍵在於科技是否取得優勢。簡言之，網路戰力即建構在正規部隊與民間網路能量的整合。

總之，俄羅斯國防部的網路部隊，在組織上幕僚單位為「資訊和大眾傳播部」及「科技部」。執行單位為資訊作戰總局(含直屬網路部隊)納編民間網路科技公司與實驗室。此外，各軍種的通信部隊負責指管通資系統作業與維護(網路部隊編組，如圖1)。

(三)俄聯邦安全局

隨著網路安全已危害到國家安全，運用國安體系預先掌握網路資訊，即可預防網路威脅及對敵發動網路攻擊。2013年初，俄羅斯總統普丁簽署《關於建立查明、預防和消除對俄羅斯資訊資源電腦攻擊後果的國家系統》命令，責成「俄聯邦安全局」(Federal Security Service ,FSB)建立國家網路安全系統，負責檢測駭客入侵和預先掌握國家遭攻擊之資訊。[22]俄羅斯聯邦安全局下屬的一個「網路作戰部門」(Cyber operation divisions)，負責聯繫、運

17 "Information Warfare: The New Russian Cyber War Force", strategy page , https://www.strategypage.com/htmw/htiw/20130908.aspx, September 8,2013.

18 同註9。

19 同註12，頁45。

20 同註8，頁42。

21 同註9。

22 朱峰、王麗、譚立新，〈俄羅斯的自主可控網路空間安全體系〉《資訊安全與通信保密》(北京)，2014年9期，資訊安全與通信保密雜誌社，2014年9月，頁72。

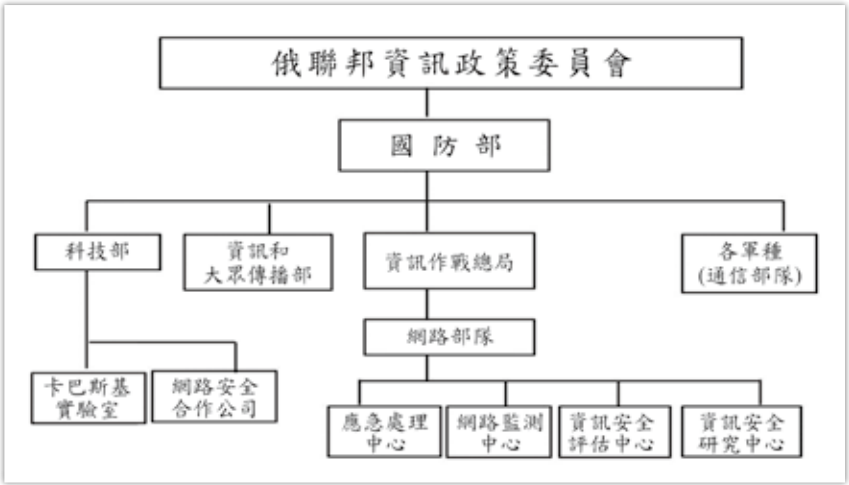

圖1　俄羅斯國防部網路部隊編組

資料來源：惠志斌，《全球網路空間信息安全戰略研究》，(上海：上海世界國企出版公司：2015年4月)，頁97；周季禮，〈2014年俄羅斯網路空間安全發展舉措綜述〉《中國資訊安全》(北京)，2015年10期，國家資訊技術安全研究中心，2015年8月，頁101；Defense intelligence agency," Russia military power-building a military to support great power aspirations", Committed to Excellence In Defense of the Nation,2017, pp.39〈http：//www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf〉

用網路駭客；其原因為駭客不隸屬於俄羅斯政府，故駭客遭查獲後，與政府無相關；另外，也無須負擔駭客成本。[23]此外，據2017年美國情報局揭露：俄羅斯情報部門已經被認為是選擇或偽裝成其他駭客主要團體。2015年對法國電視台TV5等網路攻擊，即為俄羅斯通過愛國主義號召一個名為「Cyber Caliphate」的駭客組織所為。[24]

(四)國務院

為強化國家境內網路安全管理，國務院(State Council)設有專門局，負責調查境內網路犯罪活動。[25]國務院下屬的「特種技術局」被稱為網警K部，負責網路安全工作。[26]此外，在俄聯邦中央及各地方的安全機構也設立相應的網路安全部門。[27]故為強化網路言論管理，俄羅斯有別於民主國家網路警察職責，除調查網路犯罪行為外，還必須監控網民言論。

總體而言，俄羅斯的網路空間安全體系，即由俄聯邦資訊政策委員會，直接指揮國防、國安及內政等部門所建構而成。並依網路空間的威脅源及管控方式，

23　"Chinese and Russian spies have reportedly stepped up their cyber attacks on Australian government networks, http://www.news.com.au/technology/online/hacking/steep-rise-of-cyber-attacks-in-australia/news-story/8ddf56cdd2189e2a9802b9abe5c6efb0, FEBRUARY 17 2016.

24　同註19。

25　賈易飛、梅占軍，〈俄羅斯網路安全機制的構建〉《軍事文摘》(北京)，第3期，解放軍出版社，2017年3月，頁22。

26　同註12，頁45。

27　同註11，頁97。

區分為戰時負責網路戰攻擊的國防部，及平、戰時負責網路監控的安全局，及掌握國家境內網路安全的網路警察(俄羅斯網路空間作戰任務編組，如圖2)。

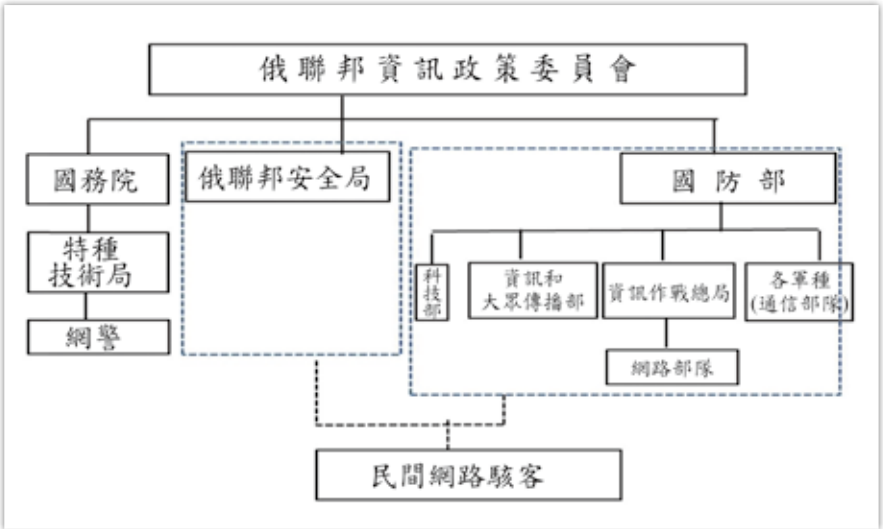

圖2　俄羅斯網路空間作戰任務編組

資料來源：朱峰、王麗、譚立新，〈俄羅斯的自主可控網路空間安全體系〉《資訊安全與通信保密》(北京)，2014年9期，資訊安全與通信保密雜誌社，2014年9月，頁72；賈易飛、梅占軍，〈俄羅斯網路安全機制的構建〉《軍事文摘》(北京)，第3期，解放軍出版社，2017年3月，頁22。

(二)網路部隊預算

要贏得網路戰爭，必須挹注國防經費培養高素質網路人才。據2013年，于忠杰指出，俄羅斯為提升網路戰能力，已挹注經費400億美元，以培養網路部隊；同時，預估俄羅斯網路部隊編制有7,300員。[28]另外，2014年4月17日，俄羅斯國防出口公司安全司管理局局長尤裡・西多林曾表示，為預防網路駭客入侵，國防部已投資290萬美元，提升網路科技能量。[29]此外，根據2017年Sergey Sukhankin表示，俄羅斯的網路部隊預估為1,000員，財務支出每年約3億美元。[30]因此，從俄羅斯網路部隊編組發展推測出，2014年前網路部隊7,300員，應為遂行俄羅斯國家整體網路安全的部隊(國防、國安及內政)。而2017年Sergey Sukhankin研究數據，則為俄羅斯國防部網路部隊1,000人，3億美元則用於國防部網路空間內。

除此之外，厚植國內網路科技發展，提升國家網路安全整體戰力。於2012年10月，俄羅斯投資60億盧布(約合1.84億美元)成立「網路創新發展基金會」，以提升晶片和作業系統的研發。隔年，俄羅斯政府公布《2018年前資訊技術產業發展規劃》。規劃於2018年前，投入40億盧

28　同註6，頁336。

29　楊國輝，〈2014年俄羅斯網路資訊安全建設觀察〉《中國信息安全》(北京)，2014年10期，中國信息安全出版社，頁104、105。

30　同註9。

布(約1.2億美金)建設50個資訊技術領域的創新研發中心，以改善IT基礎設施。[31]因此提升網路戰能力，除成立網路部隊外，還須挹注經費發展網路科技自主化。

評估俄羅斯網路戰能力

要發揮網路戰作戰效能，必須運用網路病毒及駭客，癱瘓敵國政治、經濟、軍事。反之，須防範敵人運用同樣手段，對本國的攻擊。

一、網路攻擊

使敵無法獲取正確資訊，依攻擊方式區分電腦病毒及網路駭客。

(一)電腦病毒

由於資訊設備是由電腦晶片所組成，透由電腦病毒植入晶片中，使其無法正常運作，即可達到網路攻擊目的。2015年底，俄羅斯對烏克蘭西部大部分地區發動網路攻擊，透由網路散播病毒，癱瘓烏克蘭西部資訊、通信等關鍵基礎設施，致使電力網中斷，造成約有140萬家庭和企業停電。[32]此外，為避免在美國境內的電腦，因使它國軟體而遭電腦病毒植入。2017年9月3日美國「國土安全部」要求，美國聯邦政府所屬部門，於90天內全面移除已安裝俄羅斯防毒軟體「卡巴斯基」(Kaspersky)；其原因為俄羅斯法律規定允許俄羅斯情報機構可以要求或強迫「卡巴斯基」，提供所需的數據資料。[33]因此，誰擁有網路科技優勢，誰就掌握網路戰的主動權。

(二)網路駭客

遂行網路攻擊，除利用電腦病毒外；另外，可透由網路駭客針對系統漏洞實施網路攻擊。根據2017年2月底，美國國防科學委員會出版的一份報告《網路嚇阻任務力量》(Task Force on Cyber Deterrence)指出，美國正處於日益嚴重的網路攻擊風險當中，且俄羅斯和中共正增加對美國關鍵基礎設施的工業控制系統進行網路攻擊的實質性能力。在過去的幾年中，美國企業界遭俄羅斯、中共等網路駭客攻擊，已造成數十億美元的損失。[34]不僅如此，根據2017年5月美國「戰略之頁」網站報導：俄羅斯的網路駭客能力，已威脅到美國部署在南韓薩德

31 同註31。

32 "Information Warfare: Russian Cyber War Training Can Be A Killer,"strategy page, https://www.strategypage.com/htmw/htiw/20160310.aspx, March 10, 2016.

33 Homeland security, "DHS Statement on the Issuance of Binding Operational Directive 17-01, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01, September 13, 2017.

34 "Task Force on cyber deterrence," DoD Defense Science Board,http://cdn.defensedaily.com/wp-content/uploads/post_attachment/158081.pdf, February 28,2017.

(Thaad)[35]的網路系統。[36]從俄羅斯網路駭客能力凸顯出，隨著網路駭客能力愈來愈強，網路安全防護也相對困難。

二、網路防禦

網路防禦，不僅須防範來自外部的侵犯，也須做好內部監控。

(一)對內審查

要防範網路安全威脅，必須確保國家境內的網路節點不遭敵國網路攻擊。2014年，俄羅斯政府立法通過，要求所有網路公司須保存使用者相關數據資料在俄羅斯境內保存6個月以上。[37]此外，俄羅斯聯邦安全局等8家政府機構，已安裝名為「行動偵查系統」的軟體(System for Operative Investigative Activities, SORM)。該項系統可自動追蹤據有IP的資訊設備，如電話、路邊攝影機。[38]不僅如此，俄羅斯利用網路審查員，使不受政府歡迎的文章停留在網頁後面，如果只是用關鍵詞搜尋，將很難搜尋到。[39]故在俄羅斯境內的網路中，任何數據資料將受到監控，也意味著網路安全擴及到具有IP的資設設備上。

(二)對外防護

要落實網路安全管理，必須防範國家境外的網路駭客入侵。2013年，俄羅斯國防部建設獨立的內部網路，以保障其網路安全。[40]此外，2014年為加強對國際媒體的監控，直接參股管控社群媒體。如俄羅斯DST公司，已擁有臉書10%的股份。另外，蘋果公司產品源代碼必須交由俄羅斯政府監管。同時，扶持本國自行研發軟體，如「觸摸網」已超過2.1億用戶，成為俄羅斯最大社交媒體網站。[41]不僅如此，2014年俄羅斯「卡巴斯基」網路安全公司，已研發出「網路威脅即時地圖」。

35 「薩德」系統為終端高空防禦飛彈(英語：Terminal High Altitude Area Defense，THAAD，音譯)。為美國為強化聯合防空所設計的系統。薩德飛彈防禦系統，包括4輛發射車、雷達、冷卻車、控制站、指揮艙、通訊單元、發電車等。

36 "Information Warfare: THAAD The Hack Attack Magnet,"strategy page, https://www.strategypage.com/htmw/htiw/articles/20170611.aspx, June 11, 2017.

37 同註12，頁46。

38 樂蓓、石紅梅、陳桂香、鐘鑫，〈俄羅斯與印度的網路監控系統概覽〉《中國安防》(北京)，第10期，漢斯出版社，2014年10月，頁89、90。

39 Frederic Martel著，林幼嵐譯，《全球網路戰爭：全球化vs在地化》(SMART. Enquete sur les internets)(新臺市：稻田出版有限公司，2016 年)，頁103、104。

40 同註12，頁46。

41 朱峰、王麗、譚立新，〈俄羅斯的自主可控網路 空間安全體系〉《資訊安全與通信保密》(北京)，2014年9期，資訊安全與通信保密雜誌社，2014年9月，頁73。

該系統採用類似谷歌地球(Google Earth)的方式，能從網路中提取資料，並顯示出世界範圍內不同類型的網路攻擊條紋，以利掌握網路攻擊情況。[42]因此，防範網路攻擊，不能消極的依靠網路人員監控、應變處置。而須建構資訊化系統，主動掌握網路攻擊者IP位址，以達嚇阻之效。

三、網路戰特、弱點

要構建可恃的網路戰力，必須要有素質精良的網路部隊及科技自主的通資系統。故從組織面、技術面及政策面，以評估其網路戰力。

(一)特點

1.增設資訊和大眾傳播部，因應網路戰作戰型態改變

隨著網路科技及智慧型手機的普及，網路戰的攻擊對象已從癱瘓敵國關鍵基礎設施的物理層，擴及到使用者決策領域。2016年俄羅斯國防部新增「資訊和大眾傳播部」，即因應此威脅所增編。回顧從2008年俄羅斯利用網路攻擊破壞喬治亞共和國的資訊基礎設施。同時，運用網路媒體以獲取俄羅斯人民的輿論支持。再至2016年，俄羅斯運用網路社群媒體直接影響美國選情結果。即證明網路戰的作戰型態已發生變化(俄羅斯網路攻擊統計，如表1)。不僅如此，據2017年9月26日，美國參謀總長聯席會主席鄧福德將軍(Dunford)出席參議院武裝委員會時表示：為因應俄羅斯多樣且複雜的運用網路執行混合作戰(hybrid warfare)，必須改變以往作戰計畫的傳統0、1階段。[43]因此，未

表1　俄羅斯網路攻擊統計

年份	攻擊行為
2007年 (愛沙尼亞)	俄羅斯運用駭客，針對愛沙尼亞政府機構、銀行和媒體網站實施網路攻擊，癱瘓該國關鍵基礎建設。
2008年 (喬治亞共和國)	俄羅斯運用網路攻擊，癱瘓喬治亞共和國的指、管、通、資、情、監、偵等系統。同時，以網路媒體，爭取國內輿論支持。
2014年 (烏克蘭)	烏克蘭衝突中，俄羅斯運用網路攻擊，同時，癱瘓該國部分電網，及使用網路社群媒體增加其國際輿論支持。
2015年 (美國)	2015年，俄羅斯運用網路攻擊，關閉美國國防部部分電子郵件系統，及竊取美國白宮重要資訊。
2016年 (美國)	美國總統大選期間，俄羅斯駭客組織推出Tumblr頁面的遊獻比賽，鼓勵美國黑人反抗政府；同時利用YouTube等社群平台操控美國民意流向。
2017年	2015年6月到2017年8月間，俄國特工透過臉書發出約8萬則貼文，以影響美國政治。

資料來源：作者自行彙整。

42　同註14，頁101。

43　Colin Clark,"Dunford Says White House Nixes Refueling For New Air Force One ," /breakingdefense, https://breakingdefense.com/2017/09/dunford-says-white-house-nixes-refueling-for-new-air-force-one/, September 26, 2017.

來網路戰、心理戰、宣傳戰將不再分開，而是結合為一種新型態的作戰力量，並以支持軍事作戰任務達成。

2.培養網路科技自主能力，提升網路戰攻、防戰力

沒有網路安全，就沒有國家安全。要建構安全的網路環境，必須使用自行研發的軟、體系統。根據2013年，于忠杰研究指出：俄羅斯國防部已意識到，沒有自行研製的資訊、通訊等關鍵基礎設施，就等同於沒有生命線；儘管自行研發的技術，可能落後歐、美等國家，但為確保網路安全及可信任的資訊系統，俄羅斯軍方所構連的聯戰系統使用的軟體，必須為自行研製。[44]此外，2014年6月，俄羅斯政府為強化研製的能力，同意俄羅斯國產軟體定價可高於國外產品金額的15%。同時，俄羅斯政府機構和國營企業，在資訊系統核心元件，將不再對外採購，如美國Intel或AMD為處理器。軟體方面，俄羅斯已開發出Linux作業系統，供國內電腦使用。不僅如此，俄羅斯國防部已採購由俄羅斯民間電腦公司所自行研製的Rupad平板電腦(含移動作業系統)。[45]因此，由俄羅斯決心發展網路科技的過程中，凸顯出網路科技自主化對網路戰攻、防之重要。

3.強化國際合作，提升網路空間影響力

無邊疆的虛擬網路空間，極易遭到網路駭客攻擊。透由國際合作，將可確保國家境內的數據資料不被竊取。2016年6月25日，中、俄兩國元首習近平與普丁已共同簽署《中華人民共和國主席和俄羅斯聯邦總統關於協作推進信息網絡空間發展的聯合聲明》。透過網路合作，共同打擊利用網路進行恐怖及犯罪活動，以加強跨境網路安全威脅治理。[46]另外，為提升網路安全技術發展，俄羅斯已與巴西、印度等國展開雙邊合作，以保障網路安全協定制定。[47]除此之外，據2016年美國外交政策委員研究報告指出：2009年美國電網遭網路攻擊，即為中國網路間諜與俄羅斯合作所為。[48]因此，俄羅斯為提升網路戰整體實力，除強化科技自主研發能力外，並透過國際合作方式，以提升自身的網路研發實力。

44 同註6，頁336。

45 同註26，頁21～23。

46 〈中華人民共和國主席和俄羅斯聯邦總統關於協作推進資訊網路空間發展的聯合聲明〉《解放軍報》(北京)，西元2016年6月26日，版3。

47 同註12，頁46。

48 "STRATEGIC PRIMER:2016 CYBERSECURITY," American Foreign Policy Council , Volume 2, Spring,2016,pp.6-7

(二)弱點

1.抵觸西方民主價值，易成為網路攻擊對象

隨著智慧型手機普及，傳播網路文化、顛覆他國政權，已成為最簡單、成本低的網路戰手段。根據2016年劉勃然研究表示，俄羅斯的網際網路已成為西方國家破壞俄政治、文化安全的重要平台。以美國為首的西方國家曾借助Google、Facebook等社群媒體，在俄羅斯境內策劃了多次大型示威活動，與俄政府唱反調。2015年1月，為俄羅斯反對派領導人阿列克謝．納瓦利內，就利用Facebook和Twitter等社群媒體，鼓動民眾呈現大規模請願活動。[49]此外，2017年俄羅斯遭假資訊網路攻擊。該資訊慌報有炸彈引起民眾恐慌。調查後，由於犯罪者身分難以查明。但俄媒推測謊報電話可能由鄰國烏克蘭、或其他仇俄分子所為。[50]故從俄羅斯遭網路攻擊行為凸顯出網路防護能力不足之處。

2.網路人才缺乏，網路科技無法超越敵國

網路戰力來自網路人才及科技自主。要厚植網路人才，首先要有素質精良的網民可供挑選。據2015年周季禮研究表示，俄羅斯於2015～2018年，預劃撥款640億盧布購買430萬台資訊通信技術設備，以提升中學生學習網路的條件。[51]此舉意味著俄羅斯人民的網路素質不夠普及。除此之外，據2016年Frederic Martel研究指出：在俄羅斯境內大部分的企業家，為確保智慧財產權能受司法安全保護，已將他們的品牌轉移至歐洲國家，如在美國一間網路公司只有5個人，很多工作都外包，但在俄國則須100人，都不委外。[52]因此，俄羅斯政府為擔心網路技術遭外國技術入侵，正加緊俄羅斯境內的網路科技限制。

對我陸軍資電作戰之啟示及策進作為

預防戰爭、準備戰爭、打贏戰爭，是建軍備戰最高宗旨。借鏡俄羅斯網路戰的發展，據以檢視我陸軍資電作戰現況，策進未來進步空間。

一、對我陸軍資電作戰之啟示

作戰型態改變，作戰思維須與時俱進。但盲目的跟隨別人僅會浪費國防資源，惟結合作戰實需，才能建構出符合我陸

49 同註13，頁30。

50 〈「詐彈」威脅－莫斯科10萬人疏散〉《青年日報》(臺北)，西元2017年10月8日，版6。

51 同註14，頁98。

52 同註42，頁106

軍資電作戰需求。

(一)我陸軍資電作戰任務概述

「作戰靠指揮、指揮靠通信」。為確保國軍戰時野戰通資電路暢通，2017年9月26日，我國參謀總長李喜明上將視導第〇作戰區「野戰通資系統開設實況驗證」時表示：整合運用軍、民資源，提升戰時機動通資指管能量，將是因應未來作戰所需。[53]同年，我陸軍司令王信龍上將主持「年度重大演訓通資電驗證成效專報」時表示：面對未來作戰威脅，通資系統須強化備援措施，以確保任務達成。[54]在各作戰區(防衛部)負有統合運用我陸軍聯兵旅、營通資能量、資通電軍所轄部隊及公、民營資源，以建構指管通資系統責任的情況下，其凸顯出我陸軍資電作戰所面臨的問題，為確保聯合網路環境安全及整合公、民營通資能量。

(二)對我陸軍資電作戰啟示

承上述面臨的問題。借鏡俄羅斯網路戰之作戰思維、網路科技自主及網路戰攻、防等特點，將有助我陸軍資電作戰能力之增長。

1.擴大網路空間作戰範圍，強化不對稱作戰效益

隨著智慧型手機深入到民眾日常生活，影響敵國決策判斷，獲取有利於我國的網路主導權，取得國際輿論支持，已成為網路戰的戰略目標。根據2015年，英國倫敦國王學院Rod Thornton博士表示：俄羅斯的網路戰著眼於網路和心理戰併用；其目的為減少軍事力量必要性投入。同時，使敵國軍事和民間力量支持他們國家利益。[55]另外，據2016年Keir Giles表示，俄羅斯運用網路和心理行動作戰，具有及時、秘密及意想不到的原則。另外為管制傳統及數位媒體宣傳，也積極強化電子戰干擾能力。並針對網路空間實體線路的脆弱性，責由深水研究總局(GUGI)對海底通信電纜實施調查，必要時予以破壞。[56]從俄羅斯直接攻擊目標到直接影響決策的改變，意味著網路戰將朝向多元、複雜的作戰型態發展。

值得注意的是，2015年12月底，中共解放軍新成立的「戰略支援部隊」即為打贏網路戰、電子戰、太空戰及心理戰。根據2017年12月10日，德國聯邦憲法保護局揭露：中共情報單位利用「領英」

53 黃一翔，〈李總長肯定野戰通資指管效能〉《青年日報》(臺北)，2017年9月27日，版3。

54 黃庭，〈王信龍驗證陸軍通資系統〉《青年日報》(臺北)，2017年12月13日，版5。

55 Rod Thornton," The Changing Nature of Modern Warfare," The RUSI Journal, VOL.160NO.4,AUGUST/SEPTEMBER, 2015, P.43

56 同註7, pp.64-66

(LinkedIn)交友平台，申請假帳號扮演成顧問公司、智庫或學者，以獲取個人資料。經發現，已超過1萬名德國公民與之接觸，其中還包括歐洲數個國家的高階外交官和政治人物[57](中共與俄羅斯網路戰運用同、異比較，如表2)。因此，未來攻臺戰役中，中共解放軍其可能參考俄羅斯網路戰模式，利用網路媒體宣傳，造成我國社會動亂、顛覆政權。同時，運用網路攻擊，癱瘓我國軍、民網際網路，影響我國政治、經濟、軍事等戰爭潛力。反之，我國亦可利用同文化優勢，運用網路、心理作戰，以策動中共內部反共運動，獲取有利於我國的戰爭面。

2.沒有自主的網路國防，將無法遂行聯合作戰

聯合作戰成功的關鍵，在於互連、互通的網路平台。2014年俄羅斯為強化網

表2　中共與俄羅斯網路戰運用比較

項目＼區分		中國	俄羅斯
同	戰略目的	運用網路戰癱瘓敵國關鍵基礎設施，爭取話語權，贏得戰爭面。	
	指揮權責	成立「資訊委員會」(中共為中央網絡安全和資訊化領導小組)，直接向國家主席負責，統合運用國防部網路部隊、國安局、公安部(網警)。	
	手段	網電一體戰	混合戰爭
	防護	對外：立法審查，要求外國網路公司交出密鑰，使用人實名制；對內：利用網路審查員，嚴格管制網路言論(中國：五毛黨、俄羅斯：巨魔)。	
	資訊系統自主發展	銀河電腦 微信、微博	Dr.web 網路安全公司 卡巴斯基實驗證
異	攻擊	攻、偵一體	攻、防一體
	網路部隊編組	戰略支援部隊：將電戰部隊、網路部隊及原總政治部整合。 另外，政治委員會成立輿論管制組。	2016年新增宣傳及通信部，負責宣傳、反宣傳、顛覆它國政權。
	網路部隊任務	負責網路戰攻擊及保障指管通資系統構連。	擔任國家網路戰假想敵，及保障指管通資系統構連。
	對象	它國軍事、個人資訊 如：2014年中共5員遭美國司法起訴；2017年澳洲F-35遭駭客攻擊。	關鍵基礎設施 (2007年愛沙尼亞、喬治亞共和國、2015年美國電腦)。 使用人：2016年底美國選舉。
	駭客運手	由解放軍、企業及大學整合。 (軍民融合)	由國安局下轄研究機構，運用網路駭客。

資料來源：作者自行整理。

57　German intelligence unmasks alleged covert Chinese social media profiles, https://www.reuters.com/article/us-germany-security-china/german-intelligence-unmasks-alleged-covert-chinese-social-media-profiles-idUSKBN1E40CA, DECEMBER 10, 2017.

路安全防護，針對所需的電腦軟、硬體，責由國防部與民間網路公司、實驗室共同開發，確保系統不遭受網路病毒植入。此外，為能有效管制社群媒體新聞傳播，嚴禁美國google、facebook等在境內使用，並研制系統供國人上網。反觀，我陸軍所建構的通資系統，無論是個人使用的作業系統，如windows，或野戰指管通資平台，仍以美國資訊系統為主。須知，近年來，俄羅斯及中共網路戰發展，已將美國資訊系統納入網路戰攻擊首要目標。在我陸軍尚無自製的作業系統下，未來臺海戰役中我陸軍通資系統極可能遭網路攻擊而癱瘓。簡言之，無自製的網路科技能力，我陸軍將無法遂行聯合作戰。

3.網路空間的攻、防能力，建構於合作模式

隨著網際網路的出現，國與國的天然屏障在網路空間中已消失。但由於網路攻擊具有匿名性與複雜性，以2007年俄羅斯網路攻擊愛沙尼亞為例，其入侵IP地址為美國而非俄羅斯。經調查後，為俄羅斯網路駭客透由美國IP向愛沙尼亞發動攻擊。為此，2016年俄羅斯與中共簽訂網路互不侵犯協定，並與巴西、印度加強網路科技合作。事實上，網路戰的演練合作，不僅僅是俄羅斯與中共，在美國與南韓的「網路風爆」、北約盟國等17個國家的「網路之盾」，均投射出網路空間的軍事實力，絕非以單一國家行為者可以獨自發展、單打獨鬥；而是朝向網路安全集體合作，構建安全的網路空間戰力為發展目標。

二、建議具體作為

(一)強化網路安全演練機制，重新檢視教育內容

隨著中共解放軍「戰略支援部」的成立，及太空科技性能不斷更新，對我陸軍網路安全已造成極大的威脅。以往各作戰區(防衛部)可藉由基地訓練、災防演練等時機，整合驗證資電群及聯兵旅、營通資戰力。然而，隨著陸軍資電部隊於2017年7月底，移編到國軍資通電軍後，作戰區(防衛部)如何整合資電戰力，便有待考驗。故建議未來我軍資電部隊基地流路，須考量與國軍資通電軍基地流路。否則，一旦出現衝突，將影響訓練成效。不僅如此，我陸軍網路安全教育的授課內容，絕不可還停留在網路安全防護宣教，須隨著攻擊型態的改變，從法律、政戰思想等加強教育，以利未來網路戰之挑戰。

(二)改變作戰思維，爭取網路聯合作戰

掌握網路話語權，即掌握戰爭優勢。隨著網路戰攻擊目標已從資訊、通訊等關鍵設施轉換為網路使用者，作戰思維就須跟著改變。然而，檢視我陸軍重大演習兵推課題，及聯電操演資電作戰思考框架後，發現其想定仍停留在線路中斷、伺服器遭攻擊的行動、反應、反制。而忽略了資電作戰還包含心理、宣傳及反宣傳，

法律等。基此，我陸軍資電作戰思維，是否參照美陸軍倡議的「多領域作戰」而做調整，便值得探討。此外，各國為強化網路安全防護機制，透過同盟聯合網路演習，以強化集體安全。故建議我陸軍應向國防部爭取員額，納編我陸軍網路人才參與跨國網路演習，提升網路整體戰力。

(三)建構網路科技自主能量，確保網路空間無漏洞

沒有網路安全，就沒有國家安全。綜觀我陸軍在網路空間扮演角色，即為陸上網路空間的捍衛者，故確保實體線路、網路協定的安全，即為我陸軍重責大任。然而，近年來我陸軍通資系統，無論從作業系統、硬體設施，僅消極拒絕購置中國大陸產品，而忽略了美國的網路科技早已成為中共網路攻擊的主要目標之既定事實，如F-35資訊遭竊。為此，我陸軍應優先將軟體作業系統納入建案中，以強化我陸軍網路安全防線。不可諱言，推動國防資訊產業自主化，必然會遇到成本過高、市場不大的投資風險。根據2017年12月12日，我國立法院所舉辦「振興國防產業條例」公聽會時廠商表示：希望可以降低投資門檻及軍事產品規格，讓廠商可以投入國防產業。[58]因此，在我陸軍建構網路科技自主化的過度期間，是否建議國防部向部會提出，參考俄羅斯網路科技自主化經驗(競標價格比市場高15%)，以建全我國資安產業。

結　　語

2016年，俄羅斯運用網路社群媒體，如臉書(Facebook)、推特(Twitter)，影響美國民主選舉，此舉已投射出未來網路作戰的新模式。但以往電腦病毒、網路駭客癱瘓政、經、軍等的攻擊手段並非宣告中止，而是意味著未來網路戰將是更加多元且複雜。從俄羅斯組建網路戰力發現，為強化網路空間攻、防能力，是由俄羅斯「聯邦政府」直接掌握國安、國防及內政體系，以落實網路空間各司其職之功能。在職責定位方面，發動境外網路攻擊是由國安局下轄的研究機構所策動，而非國防部。而國防部的網路部隊，則擔任俄羅斯網路空間的假想敵，透由實際演練以檢測其境內政府機關、民間企業等網路安全有無漏洞。但令人值得注意的是，中共發展網路戰型態，與俄羅斯有著許多相同之處，如利用網路戰、心理戰，瓦解敵國的抗敵意志，這是與美國所建構的網路部隊不同。總之，面對未來網路戰的挑戰，我陸軍應以前瞻的思維、突破以往的作法，參考美、俄等軍事強國的網路發展，並因應中共解放軍資電作戰威脅下，建構出可捍衛我國數位空間的資電戰力。

58　王明達，〈推國防產業－我逐步建立自有軍規〉《青年日報》(臺北)，西元2017年12月13日，版2。