中共網路攻擊與國軍資安防護作為之研析

作者/張思瑩

提要

一、隨著中共網路科技的進步，其網路攻擊手段，已從分散式阻斷式服務攻擊(DDoS)拒止他國網路正常使用，到運用先進持續攻擊手段(APT)，已對國軍安全產生嚴重威脅，而網路戰在現代戰爭中扮演的是一個強而有力的助攻，其重要性不容小覷。

二、中共從在國家主席習近平的帶動下，其網路戰發展的規模日趨強勢，而當局更是將網路戰結合至政治層面，運用網路戰手段對國軍造成各種影響，間接達成所期望的政治環境

三、國軍防衛作戰中，網路戰已成為極具重要的一環，且網路戰已逐步走向實體利益及政治面向；加上中共運用網路癱瘓、攻擊關鍵基礎設施之作戰思維已確立。強化資訊安全防護並納入軍事戰略思維，才能面對複合式的資訊戰爭，將是國軍面對的嚴峻挑戰。

關鍵詞：網路戰、網路攻擊、資訊戰、不對稱作戰

前言

隨著科技的進步戰爭型態從最開始的陸、海、空戰轉為現在的太空戰、資訊戰及網路戰，已經跳脫以往戰爭的固有型態，朝向嶄新的格局及更新穎的作戰思維，從早期的冷兵器、中期的熱兵器等都是講究兵力、火力以及武器技術的對抗，而現在探討的「不對稱作戰」也漸漸成為了現代各國的作戰主流方式，網路戰便是其中之一。

而中共深知發展網路作戰的重要性，於1997年成立國家信息化領導小組，致力發展網路作戰已20餘年，且於2015年12月31日將網路戰、電子戰、太空戰及心理戰等專業部隊整併成「戰略支援部隊」，其目的在於優先掌握戰場空間主動權，爭取網路空間及電磁頻譜之優勢進而開創陸、海、空軍有利作戰態勢。

此外，2017年曾擔任美國雷根總統的國防特別顧問艾利森(Graham Allison)亦揭露出：中共網路攻擊能力，已具備可暫時削弱美國在網路空間的反擊能力；其攻擊目標更包含了關鍵的指、管、通、資、情、監、偵(C4ISR)等系統。[1]

既然中共已有短暫癱瘓美國C4ISR系統的能力，其勢必對我國政、經、軍及各項重要關鍵設施同樣具有癱瘓能力，面對中共資訊戰優勢，國軍如何確保我指管通資情監偵系統(C4ISR)暢通及各項防護作為，已然成為近年重要課題之一，本文將針對中共歷年網路戰相關發展與

[1]Graham Allison,“How America and China Could Stumble to War,” NationalInterest,http://nationalinterest.org/feature/how-america-china-could-stumble-war-20150,URL Year，(2017/April/12)。

作為結合國軍現有之網路防護機制進而探討其網路攻擊對我資通安全防禦威脅評估，最後提出建議事項。

現行網路的威脅

一、網路戰威脅之特性

網路攻擊已經成為全球國家安全最嚴重的挑戰，行政院曾統計，境外對我國攻擊次數在2019年每月平均有2億次的掃瞄、3千萬次的攻擊，由此可見有心人士對我國試探攻擊不曾減少，顯示我國正不斷的面臨嚴峻的網路攻擊威脅，且中共對我國軍在每月統計中，高達10萬2298次的攻擊，若系統漏洞一再的被發現且利用，因此，資訊安全防護是由內而外的，以確保國軍機敏資訊獲得完整之防護，況且「網路戰」是不分平、戰時的，且完全未有煙硝的戰爭，因此，國軍每一位電腦使用者都應該隨時提高警覺，保持已身即處於戰場，且面臨嚴峻的網路攻擊，除了持續落實軍、民網的實體隔離及專網專用政策，建置嚴密資安防護機制外，亦應針對資訊科技快速發展所衍生的新形態威脅，發展適切之防護措施，提升官兵的資安防護意識，以防護國軍網路安全，確保部隊戰力。

二、國軍所面臨網路戰威脅

中共戰略支援部隊戰時將納編網路作戰部隊、電子偵蒐、干擾部隊與無人機部隊編成為「資訊作戰群」。2018年6月中共網路部隊已在上海、北京完成史上最大規模的擴編。同時，該部隊配備了最新的硬體和軟體等網路作戰裝備，其作戰能力已可掌握全球特定目標，對敵實施從Gbps到高達Tbps高頻率「分散式阻斷式服務攻擊(Distributed Denial of Service, DDoS)」，其效益將使敵國網站全面癱瘓。另外，2020年6月經專家協助追蹤與分析，發現逾17萬帳號透過彼此轉貼散播中共防疫、扭曲香港示威及有關「臺灣問題」等假消息，並有利中共輿論，企圖達到不斷重複意見的媒體「迴音效應」。不僅如此，2021年5月美國受到勒索軟體攻擊，駭客透過非法軟體控制其電腦系統及資料，Colonial Pipeline被迫關閉其美國東部沿海各州供油的關鍵燃油網路，使國家進入緊急狀態。[2]因此，中共網路作戰部隊併入戰略支援部隊後，將使原建制不同部門的網路部隊與電子戰部隊整併為「資訊作戰群」後，其網路空間作戰能力將對國軍網路、通信等系統產生極大威脅。若國軍遭受中共網路戰攻擊，中共將可竊取我國機密並掌握行動藉由癱瘓關鍵設施；不僅如此，國軍通資備援系統的陸區系統也將面臨更大的威脅，由於該系統天線網極易成為電子戰及太空偵照目標，到戰時存活率將非常低。換言之，未來臺海戰役中，國軍的固定資訊機房及具有無線電信號源的高山站臺，或備援指管通資系統，亦將受到更為嚴重的威脅。

[2]林穎佑，〈中共戰略支援部隊的任務與規模〉《陸軍學術月刊》，第 15 卷 10 期，民國 106 年 10 月，頁 107-108。

中共網路戰現況

一、中共網軍特色及作為

中共軍事研究者認為，「電腦、通信、網路」這三者是相互通聯且密不可分的技術，現在通信技術也結合了網路，構成了一個複雜的信息網路，也創造出一種新的作戰技術手段，對戰爭產生極大的影響，中共當前對於建立網軍可說是不遺餘力，不僅於解放軍中正式將網路作戰武力部隊納入正規行列作戰，並且更在民兵部隊以及人民武警部隊中成立專職使用網路作戰的網路部隊，企圖將此作為中共網軍的主角；1992至1995年，共軍效法美國在波灣戰爭中對伊拉克所實施的資訊戰法，總結出了約十種作戰模式，經過三年由下至上、由部隊及機關院校，逐級討論，在1996至1999年解放軍將其精減為六種樣式。1997年中共成立國家信息化領導小組，[3]召開全國信息化工作會議，1998年國務院成立「工業和信息化部」，對全國各相關部門進行分工。至2002年開始，中共規劃全國性國家戰略級的資訊戰分工，在解放軍階層僅負責電子戰及網路戰(如表一)，由參四部負責規劃成軍，網軍部隊由解放軍結合民間IT產、官、學界的信息民兵共同組成。[4]

表一:中共網軍作戰構想與手段

區分		目的
作戰構想		整合網路空間及電磁頻譜等作戰能量，擴大多領域偵蒐範圍，獲取軍事決策優勢，提升聯合作戰能力。同時，反制敵國對自身 C4ISR 等網路、通信節點攻擊進而達到確保整體安全。
作戰手段與目標	偵察	整合網路空間及電磁頻譜等偵察能量，對敵國實體電子設備、網路節點，擴及至數位資料庫及個人電子信箱，提升軍事行動決策優勢。
	攻擊	同步運用網路戰及電子戰，攻擊敵國軍事指管通情系統及國家網路、通信等關鍵基礎設施，加速癱瘓敵國指管通資鏈路中斷，掌握戰爭主動權。
	防禦	防護自身指管通資系統遭定位、干擾，確保在網路空間及電磁頻譜等作戰領域自由活動，以確保通資系統及數據資料正常運作，強化整體安全防護能力。

資料來源：王清安〈從中共「網電一體戰」探討共軍戰略支援部隊作戰能力〉《海軍學術雙月刊第五十四卷第三期》，第84頁。

2014年2月27日，中共國家主席習近平主持「中央網絡安全和信息化領導小組第一次會議」，強調統籌布局各方創新發展，努力將中國大陸建設成為網路強國。故中共已經將網路空間視為與美國戰略競逐要項的重要一環。且似乎已經認定，就是因為握有網路優勢，美軍才能在

[3]江蔚，〈中央網路安全和信息化領導小組成立:從網路大國邁向網路強國〉，《新華網》，https://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html，(檢索日期：2020年11月27日)。

[4]郁智隆，〈中共網軍兵力結構與戰力評估〉，《陸軍學院畢業論文集》，https://edts.lib.tku.edu.tw/etdservice/view_metadata?etdun=U0002-0102201803140000&start=61&end=80&from=CATEcateid=B006，(檢索日期：2020年11月28日)。

情報蒐集、指揮管制和軍事行動上無往不利。同時，中共領導階層也很忌憚美國以開放的網際空間和網路，威脅到共產黨統治的正當性。[5]

根據報告顯示，中共的網路諜報活動，在技術層面上已經轉向偷竊智慧財產跟專利權資訊。美國一家民營網路安全公司「曼迪安特」(Mandiant)發表針對共軍61398部隊的報告，不過只讓該部隊更加精進其「工具與基礎設施」，使爾後的入侵更難偵測。共軍大約有16個(信號情報)技術偵察單位和局處，和至少7個電子作戰／電子反制單位。中共各大軍區，都各自編配了一個電子反制團；二砲部隊，應該也有其電子支援單位。這些組織的任務，就是進行網路滲透、網路諜報及電子作戰。[6]

中共戰略資訊戰是利用非殺傷性技術而秘密實施的，不需要公開宣戰。它利用了國家力量的所有手段在國家戰略形成可競爭的優勢，把戰爭的範圍擴大到經濟、政治和社會的各個方面。這種網路資訊戰無論在平時、危機時刻還是戰爭狀態下都可能發生。例如:組織駭客通過網際網路與直接或間接相連的其他私人網路入侵另一個國家的交通、銀行、電力、石油等重要經濟部門或政府辦公系統，造成另一個國家交通癱瘓，金融混亂，電網停電，煉油廠爆炸，政府的電腦系統減速、失去聯繫、崩潰。用這種資訊攻擊的形成達到控制另一個國家為目標。[7]

二、現今策略

中共駭客利用電腦佈建的方式，將微軟最新作業系統破解後，順道植入木馬病毒及惡意程式，並公開於網站供人下載，許多資安意識薄弱的使用者若安裝破解版之作業系統，每臺電腦都有可能成為中共駭客進入臺灣竊取隱私資料的跳板，此為另類的資訊戰，因為大部分的破解版作業系統皆為中共駭客所發行，中共網軍若以此作為資訊戰前的布局，伺機利用作業系統之普及以悄悄進入臺灣內部，中共即能輕而易舉的掌握臺灣各種以電腦控制的系統，如果其發動戰爭，中共網軍即可輕易的癱瘓或掌握臺灣電腦系統，舉凡國軍塔臺、電達系統、飛彈系統等，其可不戰而勝，恐對我國產生威脅。[8]

三、攻擊方式

隨著網路成熟發展，網路科技也深入人類生活中，特別是對中共來說，從最早的數據機及傳統電話進行撥接的上網模式，逐漸進步到新型的通訊協定，從網軍歷年最常攻擊的目標對象，筆者將其區分為「設備及服務」、「關鍵基礎建設」，以及不分對象的「環境」等三個面向實施說明：

(一)設備及服務

[5]江國顯、于成森〈中共網路發展暨威脅之研究〉(陸軍學術雙月刊，第544期，2015年12月)，第1頁。
[6]鄧炘傑〈中共軍事現代化及網路作為〉《陸軍學術月刊》，第五十二卷第544期，第138頁。
[7]湯瑪士,詹森篇。(網路安全-捍衛網路時代中的關鍵基礎設施)，(國防部編印，2017年8月)，頁63。
[8]吳祥億，資訊時代對國家安全的挑戰，《行政院農業委員會》，https://www.coa.gov.tw/ws.php?id=13849，(檢索日期：2021年8月27日)。

隨著網路成熟發展，網路科技也深入人類生活中，特別是對中共來說，從最早的數據機及傳統電話進行撥接的上網模式，逐漸進步到新型的通訊協定，以下列舉網軍歷年最常用的攻擊，主要包括：

1.分散式阻斷服務攻擊(Distributed Denial-of-service attack, DDoS)：

攻擊者會製造大量的封包，最終使目標系統無法負荷，或者使用多個盜用或受控的來源來產生攻擊，藉以消耗被攻擊者的網路頻寬與系統資源，導致網路癱瘓，無法提供正常的服務，此種攻擊主要是利用分散於不同地方的多部電腦主機，發送大量的偽造封包，進而達成癱瘓網路電腦主機伺服器為目的。[9]

2.隱碼攻擊(SQL Injection)：

隱碼攻擊是一種網戰弱點，能讓攻擊者使用資料庫查詢語法(Structure Query Language，SQL)入侵網站的資料庫，一般都是正常查詢指令夾雜著 SQL 的惡意指令，在未過濾 SQL 惡意指令的情況下，資料庫伺服器會接收到攻擊代碼啟動執行，使攻擊者能擅自更動、刪除或竊取資料；隱碼攻擊仍是目前最常見的攻擊手段，因不需要太多撰寫該網頁程式知識或是存取原始碼便可執行，只要懂 SQL 指令操作即可攻擊，有點類似〝盲注〞攻擊，輸入 SQL 指令試試看能不能得到資料。[10]

3.進階持續性滲透攻擊（Advanced Persistant Threat, APT）：

進階持續性滲透攻擊手段是近幾年較常見的網路攻擊型態，攻擊者往往都是相當龐大且有組織的駭客集團，並非像一般駭客事件可由單一駭客所為，駭客集團會針對特定的攻擊對象設計一套專屬的攻擊策略，攻擊手段除了以電腦入侵方式外，也會透過其他傳統的手段達到竊取資料的目的。[11]

4.韌體攻擊：

近年物聯網發展迅速，且人員資安防護觀念增強，以往針對特定目標所進行的社交工程，便開始轉變針對特定網路設備，如網路路由器、交換器、無線基地臺等，透過韌體的入侵以控制整個網路的流量，亦可結合國內生產線，在初賞時就已完成韌體上之修改，在藉由產品銷售，進而獲取更多情報與資訊，這也就是我國行政院資通安全處於 109 年 10 月公告要求各公務機關禁用中國大陸資通訊設備。

(二)關鍵基礎設施

網際網路是國家建設之基礎設施，也是推動經濟發展和社會進步的重要支撐。如果

[9]〈什麼是DDoS攻擊?〉,《aws網站》, https://aws.amazon.com/tw/shield/ddos-attack-protestion/，(檢索日期：2020年11月27日)。

[10]Gordon Fang，〈資安滲透攻防筆記〉,《Gordon Fang網站》, https://gordonfang-850054.medium.com/資安滲透攻防筆記-1-c9a6b8ada5fa，(檢索日期：2020年11月28日)。

[11]小茶，〈進階持續性滲透攻擊APT〉,《IT邦幫忙網站》, https://ithelp.ithome.com.tw/m/aeticles/10188821，(檢索日期：2020年11月29日)。

提升國家經濟競爭的實力，就必須藉由網路發展，加快產業的增值服務、現代物流、專業諮詢服務等，並研發技術及擴展戰略，才能增加國家實力。所以越是開發中的國家，其國內基礎設施安全就越難以保證，最主要的原因是國內基礎設施的資訊化工程及各基礎設施之間的緊密依賴關係，以我國行政院公布「前瞻基礎建設計畫」[12]可以看出網際網路與經濟產能的相互關聯。據趨勢科技的一篇研究報告[13]指出 2016 年遭駭客入侵及不知名的病毒造成全球企業損失金額高達近 10 億美元(約新臺幣 300 億元)，這正是基礎設施脆弱性的一個例證。國家未來的網路戰雖以軍事作戰為主軸，但網絡攻擊的目標並不僅限於軍事設施。凡能藉由破壞敵國國內的硬體工程或民生設施，以達到損害其經濟層面、降低其人民反抗意志及減少交戰時敵人之反擊能力，都會是戰爭進行前網路戰攻擊的目標。[14]

(三)環境

1.散播假訊息

現在資訊的取得管道，大多從行動裝置上網際網路搜尋取得，隨時隨地即可獲得龐大資訊，掌握國內外，社會、政治、經濟等相關即時動態，並對相關議題實施參與並提出個人意見，此種方法大大提升其便利性及即時性，但因無法正確辨識資訊來源及內容是否屬實，使資訊的正確性及可信度卻相對較低，可是內容卻可以輕易造成羊群效應，使國人對議題產生共鳴並討論；中共可能於國人習慣使用之社群媒體上如 FB、Twitter 及 google 瀏覽器等相關論壇上散播假議題，易造成瀏覽者對現今時勢錯誤的認知，影響公民和國家的行為，進而影響社會或政治安全。

2.網路身分及名譽破壞

在網路普及後，人們會在網路上經營屬於自己網路上的線上身分及虛擬生活，對於多數人來說即時分享自己的生活動態，並受到大眾關注，是件了不起的事情，故也可以看成屬於個人的另一項虛擬人格。所以組織團體、大眾任務、政府官員及公家機關會藉由網路來實施線上宣傳並與群眾互動，建立組織形象，獲取群眾對個人、團體或政策上的認同。故中共可能藉由對特定人事或組織散布醜聞，惡意破壞網路身分及名譽，透過資訊的便利性，迅速傳遞至瀏覽者，造成三人成虎，不論其真實與否，亦會對當事人造成影響，如政治人物或重要政府官員，就會對造成群眾對其抨擊或不認同，影響其公信力並進而下臺。

現今社會只要將資料儲存在電腦上，而同時該臺電腦又擁有上網的功能，就有可能

[12]〈前瞻基礎建設計畫〉，《國家發展委員會》，https://www.ndc.gov.tw/cp.aspx?n=608FE9340FE6990D，(檢索日期：2020年11月29日)。

[13]Techtion科技行動派，〈趨勢科技2016年資安全總評報告出爐，勒索病毒家族數量飆升7倍!臺灣受勒索遍讀攻擊排名全球前20%〉，《T客邦》，https://www.techbang.com/posts/49804-trend-micro-2016-information-security-rating-report-blackmail-families-number-soared-7-times-taiwan-ransomware-virus-attack-times-ranked-the-worlds-top-20，(檢索日期：2020年11月29日)。

[14]呂俊儀，〈企業成為網路犯罪來源〉，《Media信傳媒》，https://www.cmmedia.com.tw/home/articles/3037，(檢索日期：2020年12月1日)。

遭遇到攻擊的可能，雖然現在有很多單位都採用實體隔離的方式來區分內網及外網，但也應工作的需要，需將機密資料拷貝至私人電腦中，便有可能流出的疑慮，或若任何可以存取數位資料及上網功能的設備，都有可能遭到攻擊的可能，所以，網路世界中，更該提倡或是透過不斷的演練來達到效果，像是來路不明的郵件不要開啟或是在社群網站中不要透漏太多個人資訊，同時慎選網路朋友等，這些不只是保護自己的隱私，更重要的是避免中共網軍進行社交工程學的參考依據，綜整上述攻擊手段又可區分為下列方式。(如表二)

表二：近年中共網軍常見網路攻擊手段[15]

項目 / 面向	常見攻擊	攻擊前兆	利用弱點
設備及服務	分散式阻斷服務	利用各國伺服器跳板或中木馬病毒電腦，同時連線網站意圖癱瘓系統。	網路頻寬不足與系統效能負荷過大。
	隱碼攻擊	先進行系統掃描動作。	網站程式撰寫弱點。
	進階持續性滲透攻擊	無聲無息，僅能綜合判斷。	各種方式。
	韌體攻擊	安全性機構或有心人士發現軟體或硬體上存在的缺陷，進入弱點侵入期，開始形成潛在威脅。	不當設計、實作、組態設定。
關鍵基礎設施	金融業、電力設施等	無聲無息，僅能綜合判斷。	相關金融、電力、用水等均屬民生應用，當這些設施遭駭無法正常運作，易使民眾對政府信心造成打擊。
環境	散播假訊息	使用誇張、聳動等標題或是明顯經過刻意修圖的圖片引人注目。	利用民眾對資訊正確性的質疑，進而衍生對政府、網路及人際互動等產生不信任感。
	網路身分及名譽破壞		

資料來源：〈國家資通安全戰略報告-資安即國安〉，總統府網站，2018年10月，作者彙整

國軍防護手段及強化作為

近年中共網軍常見網路攻擊層出不窮，針對前述「設備及服務」、「關鍵基礎設施」與「環境」等三個面向，提出國軍防護手段，並藉此建議國軍應有的強化作為：

一、防護手段

(一)設備及服務

1.分散式阻斷服務攻擊：

此攻擊手段為利用各國伺服器跳板或木馬電腦同時連線網站，意圖癱瘓系統；國軍

[15]〈國家資通安全戰略報告-資安即國安〉，《總統府網站》，https://www.president.gov.tw/Page/317/969/，(檢索日期：2020年12月5日)。

防護手段可有建置防火牆、入侵防禦系統與阻斷服務防禦系統等防護措施，強化我方服務之可用性，說明如下：

(1)防火牆(Firewall)：防火牆可以設定簡單的規則來允許或阻擋特定的通訊協定及 IP 位址等，複雜且混合性的攻擊方式將無法透過簡單的防火牆規則來做防禦，過程中可阻擋正常合法的封包流量進而影響服務的可能性。

(2)入侵防禦系統(Intrusion Prevention System, IPS)：對於特徵明顯攻擊是可以有效防禦的，雖攻擊趨勢已轉向為以合法流量掩飾非法行為的攻擊，也就是檢視分析的對象來源是網路上傳輸的封包，透過檢查網路封包內容的方式來防範是否有入侵行為[16]。

(3)阻斷服務防禦系統(DoS Defense System, DDS)：相較於入侵防禦系統更專注於 DDoS 攻擊上，具備阻擋以連線方式形成的 DDoS 攻擊，且阻斷服務防禦系統也能夠辨識來自通訊協定的攻擊。

(4)人為資安管控：

利用監控網路流量技術監測網路流量有無高於平常值（5Mbit/s)、連線數量有無高於平常值(如監測設定為 10,000 筆)並監控系統掃描情形，從中進行分析判斷，若發現以上行為，即進行過濾與封鎖。

2.隱碼攻擊：

運用網站程式撰寫弱點，進行惡意語法的注入，藉以取得網站控制權；面對此種攻擊手段，則應強化我方資料庫服務的安全作為，如嚴格管控並限縮權限、複雜的資料表名稱，或是部署封包防火牆等設備，使這類攻擊手段不易進行，說明如下：

(1)嚴格管控並限縮權限：將資料庫預設的帳號及密碼關閉，並確實把關資料庫管理員帳號，藉以提高資料庫的存取權限，限制攻擊者透過某些通道存取資料。

(2)複雜的資料表名稱：盡可能不要設定容易猜取的資料庫或資料表的名稱，避免入侵者使用預設名稱竊取資料庫或資料表資料。

(3)封包過濾防火牆：部署封包過濾防火牆（如 Web 應用程式防火牆），過濾掉 OSI 應用層的威脅，一般防火牆址會顧慮到網路層及傳輸層間的威脅，故對於應用層較為忽略。

(4)人為資安管控：

利用監控系統掃描技術，監控入侵偵測系統，若發現有掃描行為進行自動化行為阻擋，即利用監控警訊監控網頁有無跳出警訊，在利用增修阻擋規則，將重複掃描行為 IP 納入防火牆黑名單。

3.進階持續性滲透攻擊：持續且潛伏運用新型攻擊手段，說明如下：

(1)提高防備心：切勿點取與自身無關的釣魚郵件等資訊。

[16]陳毓璋、李俊毅、高志孝、楊陳俊，〈入侵式防禦系統設計之研究〉，《TANET2007 臺灣網際網路研討會論文集(一)》，http://itech.ntcu.edu.tw/tanet%202007/5%5C137.pdf，(檢索日期:2021 年 7 月 8 日)。

(2)定期更新軟體:每項軟體均有安全性之漏洞,定期更新軟體有助於安全性提升。

(3)安裝防毒軟體:確實安裝防毒軟體,以有效降低惡意軟體襲擾。

(4)人為資安管控:

利用監控系統紀錄,進行監控入侵防禦系統、APT 防禦資安設備、高階網頁型防火牆,綜合分析攻擊型式技術,以掌握資安情資,主動瞭解該攻擊入侵目標,隨時參考相關國際資安網頁消息,掌握最新資安情資,若發現異狀,則利用增修阻擋規則,以資安防禦設備發現該行為模式,將行為封包阻斷,並納入防火牆黑名單。

4.韌體攻擊:

(1)縮短半衰期:縮短發佈修正檔至組織所有機器均完成應用修正檔的期間。

(2)制定有效的弱點稽核機制:設定定期弱點掃描機制,找出是否存在未更新之修正檔、安全性組態設定不當或其他潛在弱點。

(3)管控製造國家(中共)之資訊設備:國軍現行規範嚴禁使用中共製造之相關設備,其目的為有效提升資訊安全,確保國家軍機。

(4)人為資安管控:制定有效修正檔管理策略:即時取得修正檔→測試修正檔→集中強制應用修正檔→檢查應用確認結果。

(二)關鍵基礎設施

國軍近年來持續建立指揮、通信等多重備援系統,以分散遭到癱瘓的風險,國防部在「五年兵力整建計畫」報告中指出,在戰力保存的部分,國軍將持續整建強化可抵抗和降低敵人第一擊傷害、提升戰場存活率並進而發揮有效戰力的設施,包括建構地下化、洞庫化和機動化的防護能力,同時提升備援和戰場存活能力、建立備援中心或機動指管設備,以及強化聯合指管通電設施的存活率,以達跨領域間資訊分享效率。另應建立告警機制,於危機或緊急狀況發生時,即時向民眾發出告警。此外,因應資訊戰攻擊的備援部分,國軍也開始分散作戰區資料中心,並進行「異地備援系統」的整建,全臺含外島以先後建立 9 套備援系統,以避免作戰資訊中心遭襲擊後資料全毀。

(三)環境

1.散播假訊息

此攻擊手段多以各種合法、非法手段,大量生產文章,原創性少,致真實性難以判斷,意圖造成民心動搖。

(1)落實網路安全的監管:監管的標準與機構由政府認可,監管者有權驅逐不遵守之人員。

(2)成立事實查核中心:檢驗消息真實性,以達到破除謠言。

(3)人為資安管控:

確認資訊的來源,對可疑網站及其連絡方式進行驗證,並檢查發佈日期,重新發

佈舊的新聞，但並不代表它們與現今事件相關，應詳細閱讀，檢驗消息真實性，避免造成恐慌。

2.網路身分及名譽破壞

此攻擊手段多以組織團體、大眾任務、政府官員及公家機關會藉由網路來實施線上宣傳並與群眾互動，建立組織形象，獲取群眾對個人、團體或政策上的認同。

(1)透過蒐集與分析現有網路隱匿與竄改身分之各項行為與技術，研提防制技術。

(2)規範網路業者應採用查核機制，確保資訊真實性。

(3)人為資安管控：

培養國人對於媒體及網路資訊的識別能力，係為提升國人對於資訊正確性識別能力，避免遭不實訊息干擾，並啟動自我防禦工程，推行相關法制規範，以提升自我防護機制並熟悉相關法律規範，避免遭有心人士侵襲。

正俗謂「兵來將擋，水來土掩」，每種攻擊方式，必有其對應的防護手段，但防護作為仍會受限於其他不確定因素而造成攻擊無法阻擋或是防護手段的強度不足，綜整國軍針對中共攻擊手段提出防護手段(如表三)。

表三：國軍防護手段

面向 項目	設備及服務	關鍵基礎設施	環境
攻擊手段	1.利用各國伺服器跳板，意圖癱瘓系統。 2.運用網站程式撰寫弱點，取得網站控制權。	逐步蒐集民間政黨規劃、經貿分析、學術著作，以及電信網路、關鍵基礎設施系統等隱性資訊，或是經由網路攻擊癱瘓我國運作。	多以各種合法、非法手段，大量生產文章，原創性少，致真實性難以判斷。
防護手段	1.安裝防毒軟體並定期更新。 2.封包過濾防火牆。 3.阻斷服務防禦系統。	1.建立橫向與縱向通報機制並提升跨領域間資訊分享效率。 2.建立告警機制，於危機或緊急狀況發生時，即時向民眾發出告警。	1.落實網路的安全監管。 2.研提現有網路相關服務供業者因應隱匿與名譽破壞之防制技術。
防禦步驟	1.監測網路流量及系統掃描情形並進行過濾與封鎖。 2.增修阻擋規則。 3.即時獲取最新的弱點資訊。	1.監控警訊。 2.啟動電腦緊急應變團隊。	1.確認資訊來源並檢查發佈日期。 2.培養國人對於媒體及網路資訊的識別能力。
窒礙問題	1.若遇國際大規模攻擊，將難以阻擋。 2.須增加監控人員、時常進行軟體版本升級。 3.發佈修正檔與發生攻擊程式的間隔數越來越短。	須增加資安教育訓練與人員的投資，培養專才人員多角度判斷。	1.若國人對於判斷資料正確性觀念淡薄，易造成社會動盪。 2.若非專業人事較不易察覺異狀，故具有複雜性及隱匿性。

資料來源：作者彙整

二、強化作為

由於資訊科技不斷更新，國軍的防衛作戰構想中，資訊戰已從配角轉換成重要角色，且資訊戰已從駭客利用網路來竊取機密資料，演進至由網路虛擬空間走向實體利益面向，進而破壞關鍵資訊設施，而現今作戰無論陸、海、空及資通電軍，皆離不開中共網電一體戰的範疇內，然而作戰靠指管，指管靠通資，若我國在戰爭中先期失去制資訊權，將可能造成難以計算的傷害與損失，美國國家安全、情報等單位更高層曾在國會諮詢中發表聯合聲明，表示以目前全球發展網路作戰能力而言至少有30個國家，其中也包含我國的假想敵中共，故針對國軍強化作為列舉現階段可加強之事項：

(一)資安防護作為標準程序化

資訊戰的重點乃在資訊安全防護，國軍雖在內部網路及實體隔離方面發展較為完善，但再堅強的防護體系及系統還是有遭受突破的可能，因此我仍需將發展安全防護機制與系統裝備朝向構建自動化、系統化以及資訊化之安全防護系統為重要目標。由被動性的防護(如：防火牆)進而建立主動性的監偵能量及加強我反制作為(如：IDS、IPS)以建立關聯防護機制，才能在防衛作戰中，確保我資訊鏈路之完整，進而有效支援作戰，以貫徹「實體隔離、專網專用」之政策。

(二)持續培訓人才並增加誘因

現今科技日新月異，網路世界的知識亦需要持續學習，因此建議編列相關預算並提高待遇，將國軍網路戰人才向民間專業機構學習，取得相關證照甚或師法國外相關頂尖之網路戰機構學習更具威脅性之攻防技巧，對於網路戰能力的提升皆具有正面長遠之意義。且建議相關人才必須提高相關待遇，構建一順暢之培訓及升遷制度，以利人才之長留久用。

(三)強化網路戰攻防演練

國軍致力推動聯合作戰及構建 C4ISR 系統，不斷實施聯合演訓，磨練各軍、 兵種聯合作戰能力，惟網路戰的攻防訓練與演訓，尚在持續培訓中，致我網路戰整體攻防能力未能確切驗證。1997 年，美國政府招募數十名電腦高手組成「紅色小組(Red Team)」，實施 「合格接收者(Eligible Reciever)66」網路攻防演習，允許「紅色小組」實際攻擊國防部所屬系統，並針對國家資訊基礎建設發動模擬攻擊，「紅色小組」僅利用自網際網路獲得的開放程式碼與駭客工具，即證明美國國防網路的脆弱及國家資訊基礎建設的弱點，是極易受到攻擊的。此外，美國也從此次演習得到經驗教訓，迅速建立了「弱點有效評估、網路預警機制、指定網路防禦指揮部、 跨部會規劃、訂定相關程序流程」等，其中最重要的是「成立由國防部負責的中央指揮單位」及「網路戰專責業管單位」。日前國軍派員代表國家至美國參加「國際虛擬網路安全競賽」，其目的、宗旨係為了強化網路攻防及提升網路作戰能力，希望藉參加競賽的經驗，汲取國外網安人才培訓模式、網路攻防訓場發展，及各國網路戰發展能量等，參考外界新知並與世界資訊接軌，同時也遂行資通電作戰，以提升國軍網路安全。

(四)整合電戰環境實施演練

未來戰爭型態皆離不開電子作戰之範圍，國軍需針對臺灣各電磁戰場環境、敵情威脅及作戰需求，與我通信及網路作戰相結合，尤其針對電子戰防護部分，如何防敵電磁脈衝攻擊，建立備援 C4ISR 系統及各項通資電鏈路，完成陸、海、空的電戰防護網，爭取局部優勢。若無法結合電子戰概念實施網路作戰，那麼在敵電磁壓制，進而癱瘓我各項指管設施情況下，再多的網路戰攻防演練也是枉然。

由於我國處於面對中共網軍駭客威脅的第一線，應以強化全民對其認知資訊戰目的、手段、影響的警覺意識，將為當前確保國家安全及維護社會穩定的當務之急，可行工作包括，可透過學校教育為主，社會及機關教育為輔的途徑，傳授基本、易學、有效的資安防護概念與技能，以期養成民眾具備良好個人資安防護習慣，進而鞏固全面性的社會資安防禦環境，亦或者許多國家已將識別假訊息視為公民基本素養，除公眾組織、媒體平臺設置資訊檢核機制外，亦應廣泛教導民眾對所接觸資訊，採取懷疑標題、留意連結、調查來源、參考其他報導等態度，杜絕假訊息危害，既以全民國防教育所涵蓋學校、機關、社會教育等全面性特質，應將防範中共網軍認知資訊戰的相關觀念、做法等，融入教育內涵中，以做為保障社會不受訊息戰侵犯的重要屏障，更重要的是，在中共網軍及其宣傳活動更趨猖獗的情況下，此類全民國防教育或可帶動精進反制策略的啟發，期以全民群策群力，共同因應認知資訊戰的挑戰。(如表四)

表四：國軍強化作為與具體作法

國軍強化作為	具體作法	現今防護手段	防護之面向
資安防護作為標準程序化	1.建立資安事件應變程序化。 2.落實實體隔離、專網專用政策。	1.安裝防毒軟體並定期更新。 2.封包過濾防火牆。 3.阻斷服務防禦系統。	◎設備及服務
持續培訓人才並增加誘因	1.提高待遇。 2.構建培訓及升遷體制。 3.建立專人專職機制。	1.安裝防毒軟體並定期更新。 2.落實網路的安全監管。	◎設備及服務 ◎環境
強化網路戰攻防演練	1.增加攻防演練頻率。 2.成立國防部負責的中央指揮單位」及「網路戰專責業管單位」，提升網路作戰能力。	1.建立橫向與縱向通報機制並提升跨領域間資訊分享效率。 2.建立告警機制，於危機或緊急狀況發生時，即時向民眾發出告警。	◎關鍵基礎設施
整合電戰環境實施演練	1.建立備援 C4ISR 系統及各項通資電鏈路，完成陸、海、空的電戰防護網。 2.針對臺灣各電磁戰場環境、敵情威脅及作戰需求實施演練。	1.阻斷服務防禦系統。 2.建立橫向與縱向通報機制並提升跨領域間資訊分享效率。 3.落實網路的安全監管。	◎設備及服務 ◎關鍵基礎設施 ◎環境

資料來源：作者彙整

結論

由於網路空間在作戰影響的層面亦趨擴大，無論是網路戰或是資訊戰，雖然只是一個助攻的角色，主要仍依靠陸、海、空軍遂行作戰，但是資電作戰所能發揮出的效果絕對超乎想像地巨大，甚至能達到「不戰而屈人之兵」之效果。

近年中共已將所謂的信息化戰爭列為優先發展目標，中共也已成立所謂「戰略支援部隊」之網路部隊專責資訊戰攻防作為，亦已籌設信息戰模擬中心，利用高科技模擬技術與設備，營造資訊戰與模擬戰環境，用以進行對抗演練，而國軍對於網路戰的作為絕不能僅止於被動防禦，或是在電腦上安裝資安管控軟體諸如此類的作為就可以，因為在這個未知而廣袤的戰場中，各國都積極於發展無限的可能，並且於平時中持續佈放所需要的病毒程式，潛伏於各政府、民間甚至是軍事電腦系統中，一旦需要用到之時便發揮極具影響的作用，動輒造成難以計算的傷害與損失，我惟有全面檢討，徹底修正，結合產官學研究資源，留住高素質高科技人才，組建專精網路戰部隊，期使能在網路作戰中以小博大，達成所謂不對稱作戰的思維，進而確保我防衛作戰任務之達成。

2017年間雖成立資通電軍並設立網路戰聯隊及電子戰聯隊培養網路戰及電子戰之相關人才，也結合政府及民間企業的相關資源，提升網路系統及技術，但是網路的安全性及危險性與日俱增的，因網路相關攻防及侵入是沒有國際界線的，畢竟網路甚或是程式的漏洞都存在於我們看不見的地方，就算每次更新如何地修補系統及程式漏洞，還是有其缺陷存在，現今網路攻防的手段、方式只會持續性不斷的進步對我產生新的威脅，而我們的網路安全性挑戰會隨著科技的進步，不斷的面臨新的考驗。

參考文獻

一、Graham Allison, “How America and China Could Stumble to War,” NationalInterest,http://nationalinterest.org/feature/how-america-china-could-stumble-war-20150,URL Year，(2017/April/12)。

二、劉德勳，〈國家安全局因應中共網路戰威脅之策略與執行成效〉，《監察院109年上半年度通案性案件調查研究報告》，https://cybsbox.cy.gov.tw/CYBSBoxSSL/edoc/download/41921，(檢索日期：2021年1月20日)。

三、林穎佑，〈中共戰略支援部隊的任務與規模〉《陸軍學術月刊》，第15卷10期，民國106年10月，頁107-108。

四、江蔚，〈中央網路安全和信息化領導小組成立:從網路大國邁向網路強國〉，《新華網》，https://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html，(檢索日期：2020年11月27日)。

五、郁智隆，〈中共網軍兵力結構與戰力評估〉，《陸軍學院畢業論文集》，https://edts.lib.tku.ed

u.tw/etdservice/view_metadata?etdun=U0002-0102201803140000&start=61&end=80&from=CATEcateid=B006，(檢索日期：2020年11月28日)。

六、江國顯、于成森〈中共網路發展暨威脅之研究〉(陸軍學術雙月刊，第544期，2015年12月)，第1頁。

七、鄧炘傑〈中共軍事現代化及網路作為〉《陸軍學術月刊》，第五十二卷第544期，第138頁

八、湯瑪士,詹森篇。(網路安全-捍衛網路時代中的關鍵基礎設施)，(國防部編印，2017年8月)，頁63。

九、吳祥億，資訊時代對國家安全的挑戰，《行政院農業委員會》，https://www.coa.gov.tw/ws.php?id=13849，(檢索日期：2021年8月27日)。

十、〈什麼是DDoS攻擊?〉，《aws網站》，https://aws.amazon.com/tw/shield/ddos-attack-protestion/，(檢索日期：2020年11月27日)。

十一、Gordon Fang，〈資安滲透攻防筆記〉，《Gordon Fang網站》，https://gordonfang-850054.medium.com/資安滲透攻防筆記-1-c9a6b8ada5fa，(檢索日期：2020年11月28日)。

十二、小茶，〈進階持續性滲透攻擊APT〉，《IT邦幫忙網站》，https://ithelp.ithome.com.tw/m/aeticles/10188821，(檢索日期：2020年11月29日)。

十三、〈前瞻基礎建設計畫〉，《國家發展委員會》，https://www.ndc.gov.tw/cp.aspx?n=608FE9340FE6990D，(檢索日期：2020年11月29日)。

十四、Techtion科技行動派，〈趨勢科技2016年資安全總評報告出爐，勒索病毒家族數量飆升7倍!臺灣受勒索遍讀攻擊排名全球前20%〉，《T客邦》，https://www.techbang.com/posts/49804-trend-micro-2016-information-security-rating-report-blackmail-families-number-soared-7-times-taiwan-ransomware-virus-attack-times-ranked-the-worlds-top-20，(檢索日期：2020年11月29日)。

十五、呂俊儀，〈企業成為網路犯罪來源〉，《Media信傳媒》，https://www.cmmedia.com.tw/home/articles/3037，(檢索日期：2020年12月1日)。

十六、〈國家資通安全戰略報告-資安即國安〉，《總統府網站》，https://www.president.gov.tw/Page/317/969/，(檢索日期：2020年12月5日)。

十七、陳毓璋、李俊毅、高志孝、楊陳俊，〈入侵式防禦系統設計之研究〉，《TANET2007臺灣網際網路研討會論文集(一)》，http://itech.ntcu.edu.tw/tanet%202007/5%5C137.pdf，(檢索日期:2021年7月8日)。

作者簡介

張思瑩:專業軍官班104年班、通資電正規班109-1期。經歷：區隊長、人事官及教官；現職為陸軍通信電子資訊訓練中心上尉中隊長。