作戰研究

DOI:10.6237/NPJ.202208_56(4).0007

運用「主動式網路防禦」強化國軍資安防護能力之研究

The Research on the Application of the Active Cyber Defense to Strengthen the Military Information Security Protection Ability

海軍中校 李建鵬、空軍少校 邱采柔

提　　要：

一、我國在新版《國家資通安全情勢報告》中指出，網路攻擊手法多元且日益複雜，近年新興科技如「物聯網」、「工業控制系統」、「無人飛行載具」及「5G」行動通訊等應用普及，使得人們更加容易受到網路駭客攻擊威脅。此類攻擊伴隨來的全球資安問題層出不窮，印證國軍面對中共持續的網路攻擊威脅及挑戰，尤應有所警惕，萬不可掉以輕心。

二、「善戰者，致人而不致於人」。欲掌握網路攻防行動之主動權，必須善用「主動式網路防禦」機制及手法，先期察覺、牽制，甚至反擊來自攻擊方的駭侵行動，並讓防禦手段方能超前部署、即時應變，以因應「日新月異」的網路攻擊。

三、國軍在面臨中共日益嚴峻的網路威脅下，建議應朝「主動式網路防禦」機制發展，化「被動」防護為「主動」防禦，持續強化資安縱深防禦、建構「人工智慧」(AI)分析平台，及完善網路威脅情資共享，方能提升國軍資安防護能力、防堵及遏止中共網路駭侵，強化國家數位疆土安全。

關鍵詞：主動式防禦、網路攻擊、主動式防禦知識庫、資安防護

Abstract

1.The latest edition of “2020 National Information and Communication Security Situation Report, Taiwan” points out that cyber-attacks are diverse and increasingly complex. In recent years, the popularity of emerging technologies such as the IOT, ICS, UAV, and 5G communications have made everything easier to be threatened by hacker attacks. Along with the trend, plus cyber threats from China, MND should take actions cautiously.

2.To take the initiative in the network's offensive and defensive actions, the "Active Cyber Defense (ACD)" mechanism, from detection to the counter measurement, should be deployed ahead, respond immediately, and effectively deter in response to ever-changing cyber threats.
3.Under the threat of cyber-attacks from CCP, it is recommended that the military should develop ACD mechanism, turn defense from passive to active, and so forth empower the defense-in-depth mechanism, build an AI analysis platform, and improve the cyber threat COP network. By means of the above-mentioned, we are able to strengthen the military's information security, prevent and deter the CCP's invasion in a timely manner.

Keywords: Active Cyber Defense, Cyber Attack, MITRE Engage, Cyber Protection

壹、前言

隨著數位時代來臨，資訊科技已融入人們生活中，雲端運算、行動通信、社群媒體及「物聯網」(Internet of Things，以下簡稱IoT)[1]等網路科技應用的蓬勃發展，使數位生活蔚為潮流；其快速擴張的同時，往往伴隨著各類型難以預測的資安威脅，並對國家安全、交通運輸、金融經濟及軍事等關鍵基礎設施，產生重大影響。一旦網路遭到癱瘓、攻擊，不僅影響一國之政、經、軍、心各層面，更將導致社會動盪不安；因此，運用「網路戰」正可「兵不血刃」地癱瘓、破壞敵指管通資系統、阻斷指揮鏈，致使部隊調度、武器裝備無法正常使用。故面對「日新月異」的網路威脅，各國政府皆積極尋求相對應的策略，並將其列為國家層級之資安戰略。

1991年美軍在「沙漠風暴」(Operation Desert Storm)行動中，將伊拉克軍隊的指揮、通信、防空、情報等軍事指管系統列為打擊核心，使對手從作戰初始就處於混亂無序的狀態，並迅速獲致戰果；[2]同時在「心理戰」方面，透過媒體散播，製造有利於己方的資訊，使作戰全程得以充分打擊伊軍的士氣，並提高己方之士氣。[3]綜觀此次戰役是將資訊科技成功運用於戰場的典範，可視為「網路戰」的一個里程碑。一般「網路戰」可分為「網路攻擊」與「網路防禦」兩項，而美軍在此次戰爭中係運用純粹攻擊式的網路戰，網攻目標是敵方指管、武器系統與敵軍心理、士氣，透過癱瘓伊軍戰場經營機制，達到「不戰而屈人之兵」之目的，並大獲全勝。[4]

註1：張菀庭，〈什麼是物聯網 IoT ?〉，服務創新電子報，2016年4月19日，https://innoservice.org/9802/主題週專題報導-什麼是物聯網-iot/，檢索日期：2022年5月2日。
註2：Daniel E. Magsig著，〈資訊時代的資訊戰(Information Warfare In The Information)〉，《資訊作戰譯文彙集》(臺北市：國防部史政編譯局，1997年)，頁250-252。
註3：同註2，頁252。
註4：蔡輝榮、吳宗禮，〈面對資訊作戰之準備、發展與落實〉，《資通安全專論》(臺北市)，2007年，頁3。

我國行政院新版的《國家資通安全情勢報告》中，歸納近年來發生在國內的資安重大事件，可看出資安威脅趨勢包含「個資洩漏」、「勒索軟體攻擊風險遽增」、「物聯網設備資安弱點威脅升高」、「進階持續性威脅攻擊竊取機敏資料」及「政府機關委外供應鏈遭駭侵」等項，[5]且公私機關部門均難以倖免。駭客從「隨機」攻擊方式，轉為鎖定民生基礎設施或大型企業等特定目標進行攻擊，進而癱瘓、破壞政府或民間業者的各類設施運作，將可造成國家重大影響；因此，更容易成為國家級駭客覬覦之重要目標。[6]綜觀近年來全球重大網路攻擊事件，亦與我國歸納之資安威脅趨勢相符合，且從各國政府機關、軍事單位及民生設施均曾遭受不明網路攻擊，凸顯資訊安全防護之重要性。[7]

我國戰略地位特殊，又屬高科技供應鏈國家之一，時刻面臨來自各方之網路駭侵威脅，其中尤以中共為甚。因此撰寫本文主要目的，即希望透過蒐集「主動式網路防禦」(Active Cyber Defense，以下稱ACD或「主動式防禦」)機制相關文獻資料，瞭解其特點、部署及運用方式，分析其對強化國軍資安防護能力之優勢，並結合國家資通安全發展方向，探討「ACD」機制對國軍之適用性，進一步提出國軍發展「主動式網路防禦」機制之策略建議，期做為國軍提升整體資安防護規劃與決策參據，達到強化國軍資安防護能量目標，以應對日益嚴峻之資安威脅。

貳、主動式網路防禦機制探討

以往資安運作思維的重點強調「防護」，其相對於「攻擊」而言，屬於靜態且被動的作為，防護方要在事件觸發時才進行應變處理；不同於「防護」概念，「防禦」則是將敵之攻擊方式列入考量，具有動態而主動的思維，適用於早期預警或設下各類型陷阱，讓攻擊方如同掉入泥沼而動彈不得，其作為亦可提升至戰略層次。將資安作為從「防護」升級至「防禦」，並非代表無須精進防護之流程、方法，而是應著重於以攻擊方的思維，以制定應變措施。以下探討「主動式網路防禦」(ACD)概念、運用及「主動式網路防禦知識庫」框架，並綜整其效益。臚列說明如後：

一、主動式網路防禦概念

網路駭侵手法日趨多元、且源頭追溯困難，被攻擊方大多只能「見招拆招」，針對受駭系統進行隔離、封鎖埠口，並加強監控等被動回應之防護手段；[8]然而，近年資安防護策略已隨著駭侵手法的演進，由原本的「防護」進化延伸到「偵測」與「回應」，並興起新式「主動防禦」概念，而有「主動

註5：國家行政院資通安全會報，《109年國家資通安全情勢報告》(臺北市)，2021年6月29日，頁6。

註6：〈2020資安重大事件回顧〉，iThome，2021年1月14日，https://www.iThome.com.tw/voice/142236，檢索日期：2022年5月26日。

註7：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71-72。

註8：〈請君入甕行不行？ 借喬治亞「請君入甕」案情境，談私人執行主動式網路防禦的刑事法律風險〉，資安人，2021年9月27日，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9479，檢索日期：2022年5月2日。

式網路防禦」(ACD)一詞出現。[9]當世界各國逐漸認知，面對網路攻擊不能僅採取被動防護模式，須有更積極主動的防禦思維與策略，進而促成「ACD」機制形成；其可以運用較無害的措施和作法(如設置誘餌目標)，以減輕遭受網路攻擊時之損害。進一步作法則是對攻擊方報復，造成破壞性反應。以下就ACD定義、優點及其風險，做概要陳述：

(一)ACD定義

1.「ACD」一詞可指軍事或網路安全領域的防禦戰略。在網路安全領域，其可能意味著「非對稱防禦」，即為降低網路防禦者的成本來增加網路攻擊者成本的防禦。[10]「北大西洋公約組織」(North Atlantic Treaty Organisation，簡稱「NATO」或「北約」)將其定義為「用來偵測或取得網路駭侵、網路攻擊或即將發生的網路行為所採取主動式措施；或判斷、對抗網路駭侵行動的來源，包含先發制人、預防措施或網路反制行動等，而採取的主動應對措施。」[11]

2.美國國防部將ACD定義為「必須是對敵方進行攻擊或者是反擊，以爭取陣地的控制權，方可稱為主動式網路防禦。」[12]其目的就是要在攻擊方進行駭侵行動時，就須以各種手段迫其現形，阻擋其接觸到機敏的資料，並儘早把攻擊方阻絕在外，或者使其無法駭入；其關鍵在於防禦方必須持續觀察攻擊方的惡意網路行為，分析發動攻擊之目的，並在攻方發動駭侵前，即對該行為進行破壞。[13]簡言之，「主動式網路防禦」是為摧毀、消除或降低對我軍和友軍產生之網路威脅，而採取的直接防禦行動；而「被動網路防護」則是除主動網路防禦之外的所有措施，以減少對我軍和友軍資產的網路威脅。換言之，ACD是針對特定威脅而採取的直接行動，而被動防禦則更側重於保護網路資產，免受各種可能的威脅。[14]

(二)ACD優點及風險分析

1.根據美國「網路空間日晷委員會」(Cyberspace Solarium Commission，CSC)研究分析主任羅伯特・莫格斯(Robert Morgus)指出，ACD策略若要發揮作用，須先掌握完整情報；然情報的蒐集必定有限，須透過整合網路安全策略，釐清情報蒐集的優先順序，以縮小不同部門間的情報落差。[15]此外，整合不同部門組成聯合防禦系統，可將

註9：〈新世代主動式防禦興起，牽制駭客也成攻防手段之一〉，iThome，2021年3月30日，https://www.iThome.com.tw/tech/143477，檢索日期：2022年5月2日。

註10：Burshteyn, Mike, “What does 'Active Defense' mean?”, https://blog.cryptomove.com/what-does-active-defense-mean-4ecff-93c4bc4, accessed 6 May 2022。

註11：〈首波大行動：主動防禦+「駭回去」〉，哈佛商業評論繁體中文版，2021年7月19日，https://www.hbrtaiwan.com/article_content_AR0008127.html，檢索日期：2022年5月26日。

註12：U.S. DoD, “Active defense”, https://www.militaryfactory.com/dictionary/military-terms-defined.php?term_id=37, accessed 6 May 2022。

註13：〈淺談網路攻擊與主動防禦〉，TWNIC財團法人臺灣網路資訊中心，2021年4月15日，https://blog.twnic.tw/2021/04/15/17745/，檢索日期：2022年5月26日。

註14：Dorothy E. Denning, Bradley J. Strawser, “Active Cyber Defense: Applying Air Defense to the Cyber Domain”,https://carnegieendowment.org/2017/10/16/active-cyber-defense-applying-air-defense-to-cyber-domain-pub-73416, accessed 7 May 2022。

註15：Robert Morgus, “The SolarWinds Breach Is a Failure of U.S. Cyber Strategy”, Lawfare, https://www.lawfareblog.com/solarwinds-breach-failure-us-cyber-strategy, accessed 8 May 2022。

責任分擔給可能遭受網路攻擊的利害關係人，相關措施包含透過法規規範強化內部網路安全工作、設置處理網路攻擊與事件之獨立單位等。

2.各項措施均有其相對的風險，ACD雖然可以增加對潛在威脅之瞭解、增強破壞(或終止)攻擊方計畫中(或進行中)的攻擊行動能力，以及提升攻擊嚇阻作用等優點；但亦可能因為「人為」誤判或錯誤的攻擊策略，破壞無辜的「第三方」電腦或網路，造成非必要的損害擴大；甚至可能演變為互相攻擊，導致衝突加劇及升級，最終可能遭受他國的政治與法律制裁。[16]故於規劃ACD策略時，同時必須審慎評估其風險，以權衡最佳方案。

二、主動式網路防禦運用探討

ACD主軸在於政府各部門及企業共享情報，並深化網路防禦措施與意識，其目標是確保國家網路安全，而非擴張網路權力。網路安全指的是確保國家關鍵基礎設施安全及數位服務功能的完整，涉及消費者個資、企業以及國家機密等所有網際網路空間的保護措施；但在保護國家安全不受任何威脅影響之前提下，國家可將自身網路能力投射至任何有關政策目標上，包含攻擊敵國網路之行為。[17]然以「ACD」做為網路安全戰略，必須在主動防禦措施正在或可能進行的背景下權衡其優、缺點，以重塑內部網路環境和相對應的結構，並以改變攻擊方的駭侵為基礎，設定最佳防禦戰略。針對網路「ACD」案例分析，概述如後：

(一)俄羅斯於2008年8月對喬治亞(Georgia)發起軍事行動，喬國重要機關與組織不斷遭受來自俄國的網路攻擊，俄國駭客在喬治亞政府多台電腦上放置惡意程式，這些程式使用如「美國」、「北約」等關鍵字來搜尋文件檔案，然後把目標文件回傳到駭客所使用的伺服器。為此，喬國政府「將計就計」，也為駭客打造了一個名為「喬治亞-北約協議」(Georgian-NATO Agreement)的誘餌文件，並植入間諜軟體存放在已遭病毒感染的電腦內，誘餌文件被駭客取走後，成功植入該間諜軟體，除了取得被駭電腦中相關的文件外，也開啟該電腦上的攝影機鏡頭，並把他的臉部照片一併回傳。這個例子可以發現喬治亞採取的主動式網路防禦手段相當「積極」，不但深入敵營，也可監看敵方、搜查其電腦資料、取走重要情資，達到阻敵於戰前之效果。[18]

(二)英國政府於2016年發布《國家網路安全戰略》(National Cyber Security Strategy 2016 to 2021)，推行「主動網路防禦計畫」(Active Cyber Defence Programmes)，[19]主要標的為檢查公共機構網站

註16：Wyatt Hoffman & Ariel Levite, “Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?”, https://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236, accessed 8 May 2022。

註17：同註10。

註18：同註8。

註19：“National Cyber Security Centre - GOV.UK”, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, accessed 8 May 2022。

的安全性、阻止虛擬電子郵件、網路釣魚攻擊，及阻斷公部門機構連結惡意網站等工作，以減少駭客針對企業和公民的網路駭侵行為。自2016年實施前述措施起，該國政府已成功阻擋超過百萬次的網路攻擊，平均一個月攔截400餘萬封垃圾郵件，最高紀錄曾於一個月內阻擋超過3,000萬封垃圾郵件，成功防護網路攻擊，計畫成效卓著。[20]因此，英國於2021年12月再公告新版《國家網路戰略》(National Cyber Strategy 2022)，將持續推行「ACD計畫」，以建構大規模的網路防禦能量，該計畫凸顯其確實具有一定防護成效。[21]

三、主動式網路防禦知識庫

(一)研發組織

「MITRE組織」(Mitre Corporation)是由美國聯邦政府所資助的非營利機構，專為政府執行資安研發計畫，收錄多樣化的入侵攻擊手法，並負責維運「通用漏洞披露」(Common Vulnerabilities and Exposures，以下簡稱CVE)資料庫。[22]其所提出的「對抗戰術、技術和通用知識庫」(Adversarial Tactics, Techniques & Common Knowledge，以下簡稱「ATT&CK框架」)，近年深受世界各國政府單位、軍方與大型企業所重視。「ATT&CK框架」為一個標準化、架構化的知識庫，主要描述駭客攻擊戰術流程，著重在攻擊情境與攻擊手法描述，並提供具體且通用的架構，能有一致的標準可參考；更可清楚檢視駭侵前後過程與關連性，以用來強化自我的防禦體系及評估的標準，目前已成為各國重要資安攻防策略的參考指標。[23]

(二)知識庫簡介

1.為扭轉「資安攻防戰」不對稱的局面，「MITRE組織」於2020年8月以「ATT&CK框架」為基礎，公布新的「防禦知識庫」(MITRE Shield)，並於2021年重新定名為「主動式網路防禦知識庫」(以下簡稱MITRE Engage知識庫)，解析如何透過觀察與運用威脅情資等方式，強化其主動式防禦技術與策略。防禦方若能同時應用兩者，更可有效強化網路防禦能力，進而成為資安領域的新焦點。[24]由於以往的資安重點，大多聚焦於保護、偵測與回應等方式，而欺敵、觀察與互動則是未來資安攻防的重點，並將「對抗戰術、技術和通用知識庫」(ATT&CK框架)的攻擊技術手法，對應到ACD上，透過兩者互相輔助，可提供防禦方更多反制的機會。

2.該知識庫除有基本的網路防禦外，更主動透過駭侵偵測、駭侵分析及威脅獵捕等方式，查找駭侵行為或是網路攻擊態樣，進而搭配威脅情資找出攻擊方，並採取預防反

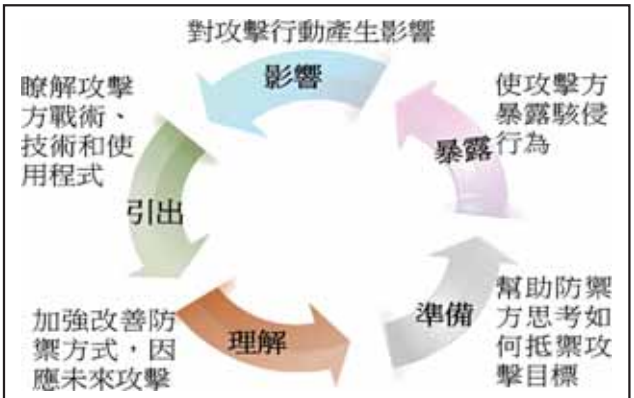
註20：“National Cyber Security Centre - GOV.UK”, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress-so-far, accessed 8 May 2022。

註21：“National Cyber Security Centre - GOV.UK”, https://www.gov.uk/government/publications/national-cyber-strategy-2022, accessed 8 May 2022。

註22：蘇柏鳴，〈MITRE ATT&CK框架概述〉，《金融聯合徵信》(臺北市：金融聯合徵信中心)，第37期，2020年12月，頁27-29。

註23：〈用MITRE ATT&CK框架識別攻擊鏈，讓入侵手法描述有一致標準〉，iThome，2020年3月3日，https://www.iThome.com.tw/news/129054，檢索日期：2022年5月9日。

註24：〈MITRE Engage將取代MITRE Shield，聚焦交戰、拒絕與欺敵領域〉，iThome，2021年9月7日，https://www.iThome.com.tw/news/146581，檢索日期：2022年5月9日。



圖一：「MITRE Engage知識庫」網路防禦五大目標示意圖

資料來源：參考Mitre Corp.,“MITRE Engage”,https://engage.mitre.org/matrix/,accessed 9 May 2022，由作者彙整製圖。

制行動。隨著攻擊方突破網路防禦能力更為精進，除了重視事件發生期間的偵測與處置，也包含如何有效反制敵人攻擊行為，此也將成為未來網路防禦的重要戰略。

(三)知識庫應用目標與方法

過去的網路駭侵係由攻擊方選擇地點、時間及駭侵模式，同時也在駭侵網路時，探索組織內部的網路防禦環境；但隨著「MITRE Engage知識庫」的建立，防禦方可誘使攻擊方朝所選定的特定路徑，進而達到主動防禦效果。該資料庫置重點於與敵人交戰的技術與策略，主要為「交戰」、「阻斷」及「欺敵」三大領域，並將相關戰略與戰術手法，彙整成一套有系統的知識庫與戰略性的具體活動，讓防禦方更好觀察與反擊；藉以提升政府機關、企業及組織等網路防禦機制，進而做到更主動的資安防護。[25]「MITRE組織」更將主動式網路防禦的各種技術與方法，歸納統整為「五大目標」、「九項方法」與對應之具體活動方式，相關內容摘述如下：

1. 五大目標：

目標層級網路防禦區分為「戰略規劃」與「交戰行動」兩種，依序包含「準備」、「暴露」、「影響」、「引出」與「理解」等五大目標(如圖一)。「準備」及「理解」屬於「戰略規劃」層級的目標，主要在幫助防禦方思考如何抵禦攻擊，並瞭解利用攻擊方所使用的駭侵方式，以加強、改善防禦方式；而「暴露」、「影響」、「引出」屬「交戰行動」層級，主要在於使攻擊方暴露其駭侵行為，並對其行動產生影響，進而瞭解其戰術、技術和使用程式等攻擊方式。[26]

2. 九項方法：

為確定要對攻擊方採取何種行動，以實現其對應目標，防禦方可依序採用「計畫、蒐集、偵測，防護、引導、中斷、確保、動機、分析」等九項方法。[27]知識庫中列出各目標可使用的方法與對應之具體行動手法，目的是將攻擊方引導至特定方向或特定路徑，蒐集其使用的網路駭侵手法、觀察駭侵行為與分析相關情報，再進行一連串的反制動作(五大目標對應九項方法，如表一)。例如「引導」方法中一項行動方案就是透過建立誘餌帳號，以創造攻擊方無法區分真假之環境，並監視誘餌帳號是否被攻擊方利用，包含置入攻擊方想獲取的誘餌文件，以鼓勵攻擊方執行其他駭侵活動，透過這種防禦方式

註25：同註24。
註26：Mitre Corp.,“MITRE Engage”, https://engage.mitre.org/matrix/, accessed 1 May 2022。
註27：同註26。

表一：五大目標對應九項方法彙整表

目標	準備	暴露		影響			引出		理解
方法	計畫	收集	偵測	防護	引導	中斷	確保	動機	分析
具體行動	•定義標準 •發展模型 •人員創建 •戰略目標 •模擬環境	•API監控 •網路監控 •軟體操作 •系統活動監控	•誘餌檔案和系統 •觸發惡意軟體 •網路分析	•基準 •硬體操作 •隔離 •網路操作 •安全控制	•誘餌檔案 •觸發軟體 •移轉攻擊 •周邊管理 •安全控制	•誘餌檔案 •隔離 •網路操作 •軟體操作	•多樣性 •系統紀錄 •資訊操作 •周邊管理 •欺騙資料	•多樣性 •觸發軟體 •資訊操作 •角色	•產生情報 •回顧 •更新態樣 •完善操作

資料來源：參考Mitre Corp.,“MITRE Engage”,https://engage.mitre.org/matrix/, accessed 11 May 2022，由作者彙整製表。

，更是要與攻擊方鬥智，當對手滲透至內部網路環境時，可及早發現其駭侵行為，當受駭時，在應處作為上更具主導權。[28]

3. 效益分析：

(1)打造「主動網路防禦機制」(ACD)之重要因素包含持續維運、早期預警、阻斷與緊急應變機制及歸因與減災等項，其目的在於瞭解攻擊方的能力與意圖，提升既有的防禦架構，綿密協調各部門，並運用有關的網路威脅情報，達到共享情資目的。另外，增加攻擊方的攻擊難度或迫其終止駭侵行動，進而減輕或消弭網路遭駭侵或攻擊後所帶來的影響。

(2)運用「MITRE Engage知識庫」對抗駭客攻擊，採先發制人、預防與反制行動，以掌握防禦主控權、降低威脅風險，有系統的歸納主動式防禦的各項具體行動概念，策應及規劃有效的戰略與手法；再透過「ATT&CK框架」，將攻、防兩方面的思維與技術手法加以對應整合，能更有效強化防禦能力，並可反覘檢視組織內防禦縱深是否足夠，建構更完善之資安壁壘。

參、現行資安防護政策暨應用分析

面對日趨嚴峻的資安威脅，世界先進國家均發展對應的資安策略與規範，而我國亦提出「資安即國安」的國家層級資安思維及戰略，在未來將朝向「主動式網路防禦」發展，建構強大防禦機制，打造韌性安全的數位環境。[29]以下針對美、日、韓及我國資安重要政策、規範與應用做簡要分析，俾做為國軍發展主動式網路防禦策略之參據。

一、美國

(一)政策發展

1. 美國政府為應對來自各方不斷的網路攻擊行為，建立整體網路安全戰略，並擴大部門合作，[30]其「國家標準技術研究所」(National Institute of Standard and Technology，NIST)於2014年發布第一版《資通安全架構》(Cybersecurity Framework)，旨在幫助各組織機構加強自身網路安全防禦，以利聯邦政府各機關或相關單位

註28：同註8。

註29：行政院國家資通安全會報，《國家資通安全發展方案110至113年核定版》(臺北市)，2021年2月23日，頁3。

註30：〈美國網路安全政策倡議之轉向〉，臺灣網路資訊中心，2021年6月1日，https://blog.twnic.tw/2021/06/01/18665/#_ftn9，檢索日期：2022年5月12日。

表二：主動式網路防禦(ACD)六大功能領域表

ACD六大功能領域						
功能項目	感知 (Sensing)	意義建構 (Sense-making)	決策 (Decision-making)	行動 (Acting)	消息傳遞與控制 (Messaging and Control)	任務管理 (ACD Mission Management)
領域內容	●監控網路環境 ●掌握現況	●分析理解 ●確認情資	●縮小因應措施選擇範圍 ●選擇最佳方案	●執行因應措施	●保持情資傳遞共享 ●自動因應控制	●建立和維護ACD操作 ●促進ACD工作流程

資料來源：參考孫鈺婷，〈國際資安防護政策趨勢探討〉，《科技法律透析》(臺北市：財團法人資訊工業策進會科技法律研究所)，第32卷，第1期，2020年1月15日，頁43，由作者彙整製表。

依循，並於2018年4月發布修正版。同年9月，再公布《國家網路戰略》(National Cyber Strategy)報告，內容以網路安全問題為主軸，涵蓋安全、外交與經濟等三大面向，以奠定美國在網路安全領域的總體戰略指導，同時確認網路科技在國家安全戰略中的核心地位。[31]

2.2021年1月成立「網路安全與新興技術局」(Cyberspace Security and Emerging Technologies，CSET)，[32]透過外交與情資共享方式，保護網路空間和關鍵技術，降低網路衝突的可能性，及在網路戰略競爭中取得優勢，以因應中共、俄羅斯、伊朗、北韓等國所帶來的網路安全威脅。[33]2021年5月，由拜登(Joe Biden)總統簽署一項行政命令，主要為「消弭政府和私營企業間共用威脅資訊的障礙」，確保資訊服務提供者能夠與政府共享有關安全漏洞的資訊，並要求企業增加網路安全架構投資，以減少未來網路駭侵事件，也為避免過時的網路安全模型和未加密的數據導致企業受到侵害。[34]

(二)應用探討

美國「國防部」(Department of Defense)運用「主動式網路防禦」做為防禦性網路行動最主要的整體戰略，並建立即時資安防護能量，達到迅速發覺、檢測、分析威脅與處置，並透過情資整合，以對抗國家級網路攻擊，不僅為國防和情報界增強防禦性網路安全能力，亦強化聯邦、州和地方政府機構和組織、國防承包商及關鍵基礎設施的

註31：同註29，頁8。

註32：〈國務院成立新的網路安全和新興技術局〉，THEHILL，2021年2月7日，https://thehill.com/policy/cybersecurity/533237-state-department-sets-up-new-bureau-for-cybersecurity-and-emerging，檢索日期：2022年5月12日。

註33：〈蓬佩奧國務卿批准新的網路空間安全和新興技術局〉，U.S. Department of State，https://2017-2021.state.gov/secretary-pompeo-approves-new-cyberspace-security-and-emerging-technologies-bureau/index.html，檢索日期：2022年5月12日。

註34：The WHITE HOUSE,“FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks”, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/, accessed 12 May 2022。

網路應處能力。ACD包含「感知」、「意義建構」、「決策」、「行動」、「消息傳遞與控制」及「任務管理」等六大功能領域(如表二)。由各功能領域內容可看出，ACD雖在其保護的網路環境中處於主動狀態，但本質並未具有攻擊性。[35]

二、日本

(一)政策發展

1.日本資安主管機關為「網路安全戰略本部」(Cybersecurity Strategic Headquarters)與「國家資通安全事件應變處理與戰略中心」(National center of Incident readiness and Strategy for Cybersecurity，以下簡稱NISC)，在其2013年版《網路安全戰略》中著重推動和訂定網路空間國際規則、與各國建立信心措施、建構網路安全防護能力，並制定網路安全的國際規則；[36]2014年另通過《網路資訊安全基本法》，針對政府機構與民間單位進行資訊安全規範。[37]2018年版《網路安全戰略》則調整戰略目標，從「事後應處轉為事前防禦」、「被動轉變為主動態勢」，並發展與世界各國網路威脅資訊共享機制，從被動安全防護轉變為主動預測。[38]

2.2019年4月，日本成立「網路安全協會」，此為官、民共用資訊的組織，當成員受到網路攻擊時，將通報「NISC」進行分析，再將結果通知所有會員，以防止受害範圍繼續擴大。2021年9月最新版《網路安全戰略》中，再從「推動數位轉型與網路安全」、「促進連結及公共空間化的網路空間，確保其安全性」及「以國家安全保障為觀點強化施政」等三大方向推動網路安全措施。「NISC」則統籌政府機關資源，並負責蒐集、分析、評估和警示相關網路威脅情報，據以訂定防止網路攻擊再次發生之政策。[39]

(二)應用探討

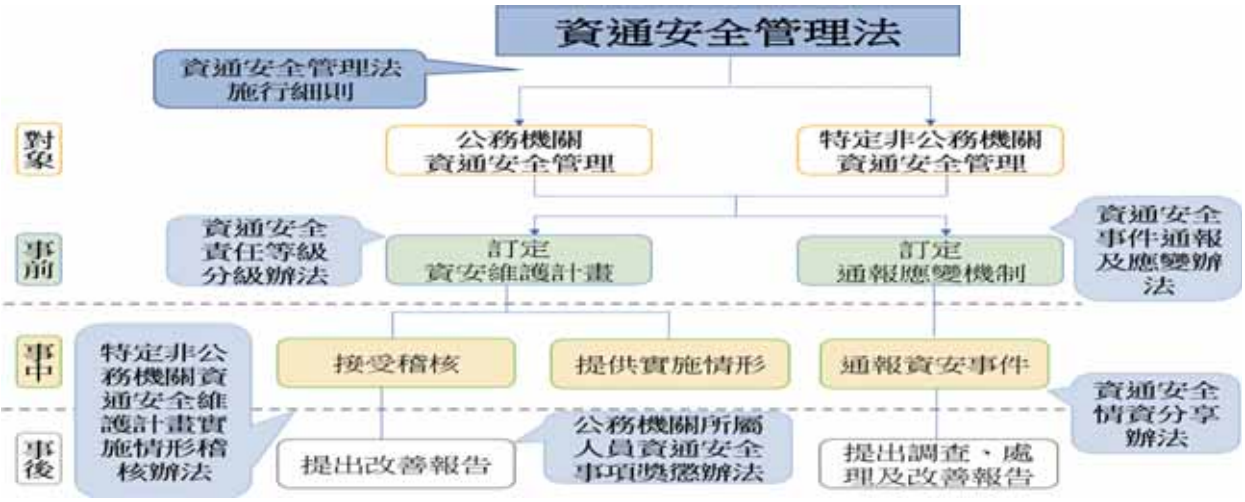
為瞭解攻擊方所使用的手法與方式，日本政府與網路企業合作，利用技術誘導網路攻擊方式加強攻擊資訊蒐集，強化威脅資訊共享機制。[40]最新一版《網路安全戰略》更明確指出，網路安全政策應由被動的網路安全防護，轉變為積極預測與有效防禦網路攻擊。例如運用自動化技術，持續審查和追踪風險，並將網路安全議題提升至國家安全層級，推進政府內部與他國間之網路威脅情報共享與交換機制，[41]更加強與各國調查機關的情報交流，以溝通、增進國際合作等概念，強化網路安全議題處理能力。

三、南韓

(一)政策發展

南韓由「國家安全辦公室」(Office of

註35：孫鈺婷，〈國際資安防護政策趨勢探討〉，《科技法律透析》(臺北市：財團法人資訊工業策進會科技法律研究所)，第32卷，第1期，2020年1月15日，頁43。
註36：古涵詩，〈日本網路安全戰略調整與組織變革〉，《全球政治評論》(臺中市：國立中興大學國際政治研究所)，第70期，2020年4月，頁141。
註37：〈各國家對資通安全立法與管理概述〉，國家實驗研究院科技政策研究與資訊中心，https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=18377，檢索日期：2022年5月13日。
註38：同註36，頁137-138。
註39：〈日本發布令和3年版網路安全戰略〉，電信技術中心，2021年12月15日，https://www.ttc.org.tw/News/more?id=407e5ad9233d47efb97dc6084d189810/，檢索日期：2022年5月11日。
註40：同註36，頁146。
註41：同註39。



圖二：我國資通安全管理法應用架構示意圖

資料來源：參考〈資通安全管理法：各單位因應之道〉，緯育，https://www.tibame.com/course/622，檢索日期：2022年5月11日，由作者彙整製圖。

National Security)負責推動資安政策，並分別由「國家情報院」(National Intelligence Service)負責國家與公共機關之資訊安全，「科學技術情報通信部」(Ministry of Science and ICT)負責民間資通基礎設施以及主要資通基礎設施之業務。[42]2019年4月，公布的《國家網路安全戰略》及《國家網路安全基本計畫》，目標是確保國家的穩定運作，應對網路攻擊，俾在韓國本土建立強大的網路安全基礎。主要目標包含「強化國家關鍵基礎設施安全」、「提高網路應變能力」及「領導國際資通安全合作」等項，透過整合國家各部會能量，大量蒐研、分析網路駭侵威脅資訊，據以因應影響國家安全之網路攻擊。[43]

(二)應用探討

南韓在《國家網路安全基本計畫》中概述未來要完成的100項任務，包括國際合作、國際規範制定、國家關鍵資訊基礎設施防護(Critical Information Infrastructure Protection，CIIP)、危機管理和訊息共用等，[44]而首要工作便是改善並提升網路威脅應變能力，包括加強民間、官方和軍方聯合應變系統，以主動阻止網路攻擊；其次，在個人、企業和政府之間的相互信任與合作的基礎上，啟動國家級的資訊共享機制，並與地方政府、中小企業、資訊支援中心等單位合作，建立全面的網路安全治理架構。南韓並透過持續人力培養、研發計畫等，打造創新的安全產業生態系統，確保網路安全核心競爭力；並讓全體國民體認到網路安全的重要性，同時建立人民參與和信任的網路安全

註42：同註29，頁15-16。

註43：同註37。

註44：SO JEONG KIM, SUNHA BAE,“Korean Policies of Cybersecurity and Data Resilience”, https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164, accessed 14 May 2022。

圖三：我國第六期資安發展方案架構示意圖

資料來源：參考行政院國家資通安全會報，《國家資通安全發展方案110至113年核定版》(臺北市)，2021年2月23日，頁35，由作者彙整製圖。

文化。[45]

四、我國

(一)政策發展

2018年5月，我國通過《資通安全管理法》(即《資安法》)，並於2019年施行，成為我國首部資通安全管理之法制框架，藉由資安法制化，消弭資安風險、建構完善的數位安全環境；另授權主管機關訂定相關施行細則與子法，明確規範資安事件前、中、後適用對象及可應用法規(如圖二)。[46]鑑於過往資安規範僅針對公務機關，在考量網路普及與隨之附加的資訊安全，將可能影響國安與民生、經濟活動；因此，已將對象擴大至特定非公務機關，包含關鍵基礎設施、公營事業等，影響範圍更擴增到多層面。[47]

(二)應用探討

我國資通安全基礎建設工作自2001年開始推行，迄今已邁入第六期，[48]當前《資通安全發展方案》(指2021-2024年)，主要願景即為「打造堅韌安全之智慧國家」，並預劃達成「成為亞太資安研訓樞紐」、「建構主動防禦基礎網路」、「公私協力共創網安環境」等三項目標。[49]其中建構主動網路防禦部分，就是透過調整防護機制、精進應變措施，「化被動為主動」將預警、偵查、溯源及反制等作法導入防護策略，以完善「政府網際服務網」(Government Service Network，GSN)防護，並透過分析情資、提升科

註45：同註44。

註46：〈資通安全管理法：各單位因應之道〉，緯育，https://www.tibame.com/course/622，檢索日期：2022年5月11日。

註47：〈資通安全管理法之衝擊與影響〉，SGS，2019年3月11日，https://www.sgs.com.tw/news-media-resources-content/page?id=2，檢索日期：2022年5月11日。

註48：黃彥棻，〈透過數據驅動的資安情資，做資安防駭超前部署〉，iThome，2020年8月24日，https://www.iThome.com.tw/news/139538，檢索日期：2022年5月13日。

註49：同註29，頁38-46。

技偵查能量，以防制新型網路犯罪(策略及具體措施，如圖三)。

肆、國軍資訊安全防護精進作為

國軍資安防護以貫徹「軍民網實體隔離、專網專用」政策，配合資安管控軟體等機制，設置「國軍資安防護管理中心」(Military Security Operation Center，以下稱「M-SOC」)實施網路狀態全時監控，並與「國軍電腦緊急應變中心」(Military Computer Emergency Response Team，以下稱「M-CERT」)進行相互聯防通報作業。另為提升國軍資通安全及發展「不對稱戰力」，亦於2017年7月成立「資通電軍指揮部」(以下簡稱「資通電軍」)，期發揮「攻守一體」特性、破解駭侵作為並做出有效反制，以強化國軍聯合作戰的資通電戰力，持續朝向「網路攻防為核心、電磁發展為前瞻」目標，發展網路作戰能力。[50]

面對中共近年內部網軍組織改革及調整，同時提升網路作戰能力，並以網路攻擊做為潛在性的武裝攻擊；鑑於中共網軍對國軍威脅日益嚴峻，現行資安防護機制確有檢討精進之必要。[51]以下針對加強國軍網路安全防護精進作為，研提建議如后：

一、建構主動式網路防禦戰略、主動偵測反制駭侵行動

(一)未來「網路戰」戰法，勢必將「先聲奪人」，而守勢戰略構想將無法適應未來網路作戰進程。國軍須知網路空間「戰略高地」乃交戰雙方必爭之地；奪占網路制高點，將是攸關臺海勝負關鍵。[52]從2022年2月爆發的「俄烏戰爭」中發現，在正式開火前，雙方「網路戰」早已「不宣而戰」；尤其當俄軍坦克部隊開進烏克蘭前，美國「微軟公司」(Microsoft)的「威脅情報中心」(Threat Intelligence Center cert)便已響起警報，發現一個從未見過的惡意刪除軟體「Wiper」鎖定烏國政府單位和金融機構。該部門立即行動反制措施、分析病毒態樣，將防禦軟體及相關病毒碼資訊提供烏國政府，並在美國政府要求下，將資訊分享給波羅的海國家(其中愛沙尼亞、拉脫維亞和立陶宛一般稱「波羅的海三國」)、波蘭及其他歐洲國家，以預防惡意程式擴散到烏克蘭以外地區。隨著實體戰爭開火，網路世界戰況更激烈，情勢也比部隊戰鬥更加混亂。[53]

(二)有「俄烏戰爭」教訓當前，國軍面對中共持續的駭侵攻擊，實應建構「主動式網路防禦」之戰略，運用威脅情資資料如「MITRE Engage知識庫」以及「ATT&CK框架」等工具，以各式誘餌、欺敵的方式及技術，監控、混淆對手、引導或誘使攻擊方掉入陷阱，才能發現攻擊方的意圖，進而箝制攻擊方之行動。另運用主動偵測技術，掌握攻擊方的思維，有助瞭解如何交戰，並發展應對

註50：國防報告書編纂委員會，《中華民國110年國防報告書》(臺北市)，2021年10月，頁61。
註51：四年期國防總檢討編纂委員會，《中華民國110年四年期國防總檢討》(臺北市)，2021年3月，頁40。
註52：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》(臺北市)，第54卷，第3期，2020年6月1日，頁81-82。
註53：〈俄烏掀史上最大網軍戰微軟也捲入，專家警告外國企業恐服務中斷〉，科技新報，2022年3月9日，https://technews.tw/2022/03/09/microsoft-is-also-involved-in-russia-ukraine-cyber-war/，檢索日期：2022年5月16日。

策略及反制措施；唯有透過積極與駭侵行為抗衡，才能建立更完善的網路防禦壁壘。

二、強化資安縱深防禦機制、全面資安健檢與分析

(一)依新版《資通安全發展方案》政策目標，「縱深防禦」包含「零信任網路資安防護」、「政府領域聯防監控」、「資安弱點通報機制」及「端點偵測資安防護」等4項工作。[54]國軍除藉「M-SOC」機制全時監控全軍網路狀態外，亦可於內部的資訊環境或指管系統中，部署欺敵、誘敵與交戰環境機制，同時比照推動「零信任」資安防護，於內、外網建立網路身分鑑別機制，對任何人要求存取工作資產皆必須先驗證身分，合格者再授予其相對存取權限，達到任何資料存取都「永不信任」且「必須檢驗」之目標，藉此進行精準反制，才能有效扭轉網路攻防「不對稱」之態勢。

(二)因應資安威脅日趨多元，我國於2019年即與美國「國土安全部」(United States Department of Homeland Security，DHS)聯手規劃舉辦「大規模網路攻防演練」(Cyber Offensive and Defensive Exercises，CODE)，包括美國、日本、澳洲、馬來西亞、印尼和捷克等超過10個印太國家均有參加，藉此擴大與外界接軌、交流。[55]因此，國軍「網路戰」專業部隊(如資通電軍網路戰聯隊)可比照此方式，配合年度演訓時機，邀集國內、外各專業單位實施大規模網路攻防演練，強化網路戰人員滲透測試專業能力，再據以對全軍網路(含指管系統)全面實施健檢分析，驗證國軍網路防護強度、找出潛存資安弱點，並提出改善建議，以減低資安威脅。

三、運用人工智慧分析平台、主動防禦未知潛在威脅

(一)現今網路攻擊方多採用「長週期」潛伏模式，伺機找出內部防禦弱點後再行入侵，亦代表透過人力作業，將難以迅速察覺網路異常態樣。為適應日益嚴峻之網路威脅，防護系統應具全自動化技術及採用「人工智慧」(AI)分析平台模式，透過AI等自動演算技術，對巨量的資安日誌進行大數據分析，將可大幅縮短偵測及回應時間，找出隱藏在龐大數據背後之資安風險及危機，並從中辨識出駭客作業軌跡，擺脫資安監控的被動防禦劣勢。

(二)當前政策要求各單位成立資安專責部門，惟面臨人力與專業人才短缺等問題，確實不易解決；如能透過科技判讀技術，將能加速辨識各類型駭客的行為與手法。並依據不同的情境，判斷這些行為是否正常，再對異常行為及早示警與阻擋，以提早發現駭客及惡意程式的攻擊行為。再者運用人工智慧分析平台自動偵測可能的網路威脅，除避免企業遭駭侵造成損失外，亦可減少資安人員的負荷。[56]因此，透過自動化技術手段處理各類駭侵攻擊，從既往的「人工防護」進

註54：同註46。

註55：〈臺美首度聯手舉辦大規模網路攻防演練，臺銀行組藍隊聯隊對抗紅隊攻擊〉，iThome，2019年11月4日，https://www.ithome.com.tw/news/134003，檢索日期：2022年5月18日。

註56：〈奧義智慧創辦人吳明蔚:AI技術讓資安防護邁向自動化〉，資安人，2019年12月11日，https://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=8774&pages=2，檢索日期：2022年5月18日。

化到「科技防禦」，並以主動出擊策略，建構資安防禦新高度。

四、跨域資安威脅情資交流、完善網路威脅情資共享

(一)我國已針對8大關鍵基礎設施(含能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區)成立「資安資訊分享與分析中心」(Information Sharing and Analysis Centers，以下簡稱「ISAC」)，[57]提高國家資安整體防護能力，並讓跨領域之部門彼此資安能聯防、交換情資，掌握最新的攻擊手法。另透過資安情資共享、綜整歸納內、外部各種遭受攻擊方式與系統潛在弱點，進而將其納為「網路戰」戰略運用，將對防範未知威脅提供重大效益。

(二)「ACD」的機制中，威脅情資的更新速度將是與駭客攻防的決勝關鍵。國軍雖經常與部外單位進行情資交流，面對跨領域之資安威脅時，迅速反制應變將攸關攻防成效；若能建構國防領域之「ISAC」，透過共享平台即時交流威脅情資，將更能落實以威脅情資驅動網路安全的防禦概念，達到跨域即時分享、迅速整合及有效應用之目的，亦能有效提升整體資訊安全應變與防禦能力。[58]如若能與各國軍事單位相互交流、綿密合作溝通渠道，建立跨國網路威脅情資共享管道，將更升級國軍在網路攻防之實力，同樣值得政府高層重視。

五、培育資安菁英人才、強化優質人力留用機制

(一)隨著資訊安全威脅高漲，國內外資安產業人才需求大增，各企業皆以高薪招募資安菁英，而國軍現行俸給制度與民間科技公司薪資待遇存在明顯落差，將使國軍資安優質人力及網路戰人才難以「長留久用」。在中東地區，強敵環伺的以色列在「全民皆兵」政策下，除強制兵役外，該國軍方更優先挑選在數理、資工方面有卓越表現的高中畢業生，進入菁英情報單位「8200部隊」(Unit 8200)服役，[59]役期內並由政府提供資源到一流大學就讀，同時擔任該國的「網軍」，參與國家網路攻防實戰，此一作法確實值得仿效，並讓國內優秀青年學子成為國家資安創新的「生力軍」。[60]

(二)國軍在發展ACD機制時，亦應著重資安人力資源管理策略，不僅要盤點人力及關鍵技術需求；另需透過跨領域聯合演習、網路安全合作、專家互訪交流或產學策略聯盟等機制，網羅資安精英與培育人才；另藉強化滲透與攻擊解析、鑑識及防禦管理、情資蒐集與數據分析、威脅分析及資安漏洞探

註57：「ISAC」為透過情資格式標準化與系統自動化之分享機制，提升情資分享之即時性、正確性及完整性，建立縱向與橫向跨領域之資安威脅與訊息交流，達到情資迅速整合、即時分享及有效應用之目的，提升國家資訊安全整體應變與防護能力。

註58：李建鵬、陳保佑，〈淺談國軍網路安全防護作為之研究〉《海軍學術雙月刊》(臺北市)，第55卷，第1期，2021年2月1日，頁129-130。

註59：〈以色列的創新之源，竟然來自這個頂尖間諜機構：Unit 8200〉，每日頭條，2016年11月25日，https://kknews.cc/finance/48l6mrg.html，檢索日期：2022年5月11日。

註60：〈以色列成為全球第二大資安強國　關鍵竟是這支神祕部隊〉，《天下雜誌》(臺北市)，2019年2月14日，https://www.cw.com.tw/article/5093988?template=transformers，檢索日期：2022年5月13日。

析等專業能力養成，一方面提高現有人員水準；另一方面可厚植資安實力於民間。畢竟資安攻防專才養成絕非「一朝一夕」之功，平時即定期檢討人力留用策略、提高專業人力薪資加給，方能吸引民間資安人才加入國軍行列。當遭到戰爭威脅時，方可結合「科技動員」政策，整合軍、民「網路戰」領域之人才，共同為國家所用，以獲取網路作戰勝利契機。

伍、結語

2014年時，俄羅斯即曾運用假訊息，干預烏克蘭領土南部的克里米亞地區公投，藉影響民眾的輿論與認知，最終該地區壓倒性的決定脫離烏國，並主動要求併入俄國轄下。[61]2022年2月下旬爆發的「俄烏戰爭」，雙方除軍事行動外，更以「認知作戰」攻勢短兵相接，亦透過社群影音媒體進行輿論攻防，如謠傳烏克蘭總統棄逃、政府瓦解、基輔棄守；或烏軍節節勝利、反攻俄羅斯等假消息。[62]細究雙方在開戰前就已經開始啟動網路攻擊與認知作戰，且為求勝利不擇手段；而戰場實情卻如「羅生門」一般「撲朔迷離」。此正凸顯「網路戰」像是一顆威力強大「無聲的核彈」，正在顛覆世人對戰爭場景的既定認知，更被當作一款攻擊武器，用來癱瘓對手、瓦解敵營或麻痺鄰國，[63]另一方面，亦切實反映「資安攻防」係時刻存在且需重視的議題，有必要寄予高度的關注與正視。

面對中共霸權野心及持續戰略性的網路攻擊，國軍仍須時刻檢視網路防護能力與威脅趨勢，以及早預警應變、掌握駭侵前兆；如欲防範於未然，勢必得持續跟進攻擊手法演進的腳步，方有能力即時發現與攔阻。《孫子兵法》有言：「無恃其不攻，恃吾有所不可攻也」、「兵無常勢、水無常形」。網路防禦工事「永遠不會做太多，也永遠會做不夠」，透過建構「主動式網路防禦」機制，將能加強對網路攻擊的抵禦能力。唯有瞭解攻擊方的思維脈絡、建立早期預警，掌握危安徵候，以強化國軍資安防禦縱深；另結合人工智慧、新式科技防禦手段之運用，即時交流跨領域之資安威脅情資，同步培育資安菁英人才，並化被動防護為主動防禦，方能增強國軍資安攻防能力，防堵及遏止中共網路駭侵，鞏固國家數位疆土安全。 ⚓

註61：呂兆祥，〈網路空間的新形態作戰模式-虛假訊息攻擊〉，《海軍學術雙月刊》(臺北市)，第54卷，第5期，2020年10月1日，頁138-139。

註62：吳宗翰，〈烏俄戰事爆發前烏克蘭面臨的「認知戰」攻勢〉，《國防安全雙週報》(臺北市：財團法人國防安全研究院)，第48期，2022年2月25日，頁53。

註63：劉彥伯，〈不費一兵一卒癱瘓一個國家，假訊息顛覆俄烏戰等現代戰爭〉，遠見，2022年3月8日，https://www.gvm.com.tw/article/87755，檢索日期：2022年5月18日。

作者簡介：

李建鵬中校，中正理工學院正87年班、國防大學管理學院指參101年班、國防大學理工學院資工所碩士108年班。曾任建陽軍艦修護組長、臺北通信隊區隊長、通信系統指揮部科長、海軍司令部戰系處資參官、電戰官，現服務於國防大學管理學院。

邱采柔少校，空軍航空技術學院99年班，陸軍通校通資安全正規102年班。曾任資電部通資二大隊分隊長、資電部網路戰大隊資網官、人事官、資參官、資通電軍指揮部資工官，現為國防大學陸軍指揮參謀學院學員。