編號：574

議題研析

一、 題目：建構「資通電軍」新軍種之配套措施與修法方向研析

二、 所涉法律

資通安全管理法

三、 探討研析

（一）據 2018 年 10 月 11 日聯合晚報報導：國軍成立資通電軍指揮部，未來希望達到第四軍種「資通電軍」的規模。新軍種目前剛起步，業務與過去大同小異，主要執行「網戰」與「電戰」任務。資通電軍指揮部今（2018）年 1 月 1 日起，開始實施「網路戰士志願短期在營服役」，希望充實網路戰大隊的人力，負責全軍通信電子與資訊管理，舉凡資通電路設施、戰術數據鏈路、戰情指管與視訊系統維護，都由資通電軍指揮部負責。除衡山指揮所的通訊外，國家政軍指揮中心即時傳遞戰情、敵情資訊，維持各戰情中心戰情系統運作所需軟、硬體設備作業，也都是資通電軍指揮部的業務範圍。此外，也支援國家慶典、重要節日、三軍聯合演訓、重點戒備、災害防救及防汛期間需求之語音、視訊、衛星、網路及電偵等各類型資通電戰備整備工作。自實施「網路戰士」志願短期在營服役措施，鼓勵國軍屆退官兵及提供後備軍人多重服役選擇，以充實「資通電軍」部隊戰力。網路戰士享有待遇、加給、口糧代金及一天有 500 元的網戰勤務加給。

但今年軍方為這類戰士薪餉僅編列 65 萬元，顯示其招募規模太小且建構之目標亟待加強。

（二）基於全球化、資訊化時代來臨，政府、企業及民眾大量使用網際網路進行線上管理、提供服務與網路互動，世界各國正面臨著快速增長的網路安全威脅，包括全球駭客持續入侵、竊取智慧財產、商業機密及國防軍事資料與散布假消息等問題。透過運用電腦、通信與影像系統、電子郵件及網際網路連結等新科技，促使作戰、外交、商業和其他領域的運作模式及傳統力量發生重大變革，當今資訊及網路的力量，對確保個人、社會及國家安全至為關鍵。新興網路犯罪與網路攻擊之路徑是藉由網際網路發動，犯罪地點大都集中在已發展國家或發展中國家，網路攻擊目標已由針對個人資料、新聞媒體及工商機密，擴大到財政金融機構、通訊網路設施、軍事情報及國家安全機關。大部分電腦犯罪是來自於個別駭客不法行為，但最嚴重者則是有官方組織的「網軍」成立，係由國家的政府或軍隊相關人員，從事或參與網路竊取機密或攻擊破壞活動。過去美國情報機關進行網路監控多年，愈來愈多的數據顯示，近年對各國公司、機構和政府單位的網路攻擊行動，絕大多數源自中國大陸地區。

（三）據報導今年底選戰進入最後激烈時刻，中國大陸很可能頻密發動網軍，攻擊特定政黨或候選人的言論或製造假消息、假新聞打擊特定候選人[1]。檢調人員分析，中共干擾台灣大選所採取之資訊戰，係透過垃圾郵

[1] 「黨政人士：選戰最後關頭防中國網軍狂轟」2018-10-23 自由時報，第 A04 版，政治新聞 。

件、網路釣魚、社交工程、網路詐騙及資訊散播等行為，導致資訊系統中斷、資訊洩密、網頁置換、非法入侵及散布假新聞、假訊息等手法。有組織及計畫性的網路攻擊手法，很可能造成災難性後果，不可掉以輕心，而其引發國家層級的資安問題，則需要建構完整之公務資安專業及軍方與國家安全部門協力發展、研究、推動資安技術方能解決。

（四）美國網戰司令部（United States Cyber Command ，USCYBERCOM)於 2009 年成立，並於 2015 年完成建置，新增 40 支網路安全部隊，其中有 13 支部隊是以反制攻擊為目的之攻擊型網路部隊，其他 27 支部隊則為防禦及支援網路反制攻擊的幕僚部隊。世界多個國家正式設置網路攻擊部隊，未來網際網路將成為軍事交戰的正式戰場。國內外、學者研究觀察指出：中國大陸在網路空間不畏懼與美國或其他國家硬碰硬作戰，中、美在網路攻防上競爭激烈，中國大陸在網路上已是崛起的霸權之一，其對境外網站的攻擊及入侵，逐漸引起國際的重視，促使美國、日本等國家採取積極反制的作為，「網路軍事化」已成國際趨勢。

（五）基於確保資訊及網路安全所需，先進國家無不加強相關防護作為，要求政府機關與相關的企業加強資訊安全防護，共同建立資訊及網路安全防護的執行架構，美國及日本等國家相繼成立「網軍」以鞏固軍隊資安防線。我國資訊科技發展快速，面臨網路犯罪與駭客入侵、癱瘓政府機關網站案件日增，受到網路攻擊的危機迫切，網路安全問題已是國家安全的重要議題。為積極推動國家資通安全政策，加速建構國家資通安

全環境，以保障國家安全，維護社會公共利益，特於2018年6月6日公布「資通安全管理法」(以下簡稱本法)。依本法第3條第1項第5款「公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。」，軍事機關及情報機關基於保密需求，另於公務機關之外設置資通安全管理之專業部門及人力，確屬非常必要且亟待充實之一環。

（六）行政院資通安全處於2016年8月1日正式成立，兼具資通安全政策制定、執行和產業推動的角色，負責行政院所有相關的資安事宜。另國家安全局為強化我國在網路世界必備的防衛力量，該局原設有一至六處的業務單位，分管掌理臺灣地區安全、大陸地區及國際情報工作、國家戰略情報研析、科技情報工作、統籌政府機關密碼政策及其裝備研製、鑑測、密碼保密等、國家安全情報工作督察業務、其他有關國家安全情報及特種勤務事項。因應網軍攻擊威脅與防護上的需要，除原有科技安全情報、密碼管制業務之外，已新設網路安全及反制網軍的專責單位，調整內部機制並成立「網域安全處」，專責處理網路安全業務。行政院所屬公務機關及國家安全情報部門之資通安全業皆已設置專業部門及人力，國防軍事之資通安全業務亦應配合儘速設置，以建構國家整體資通安全網。

四、建議事項

目前行政院資通安全處係負責公務機關之資通安全管理，國家安全局成立「網域安全處」(第七處）負責情報安

全網域之維護。資安不僅是與國家安全息息相關，更是國防政策的一環。而國防部資通電軍指揮部則負責國軍資通安全及網路作戰，其實施志願在營服役招募「網路戰士」措施確有必要性，以因應駭客及網軍實施網路之攻擊作為。本議題分析基於當前政策需求，建議如下：

（一） 因應國軍成立「資通電軍」新軍種並充實其人力需要，確有檢討本法相關條文之必要，應將「資通電軍」新軍種與充實網路戰大隊人力之規定納入本法，建議增訂第 5 條之 1 條文「國防部應規劃並推動國軍資通安全政策、資通安全科技發展、合作及資通安全整體防護等相關事宜。（第 1 項）前項國軍資通安全整體防護概況報告及資通安全發展方案，應定期送立法院備查（第 2 項）」。

（二） 將資通安全管理納入國軍之戰略性規劃實有必要，且符合國際趨勢。我國將面臨複雜且難以獨自處理的資通安全防護問題，目前國內缺乏訓練有素且擁有執照的專業資安人才，亦是政府應重視的問題。故而，對資通及網路安全之維護機制，宜參考美國及日本成立「網軍」的作法，指定軍方專責單位並指派專責人員為之。爰建議國防部為辦理網路安全防護措施及監測工作，應成立資通電軍指揮部並招募專業資安人才為之。

（三） 辦理網路安全防護措施及監測工作之特定專業領域人才，包括涉及國家安全及國防機密資訊與技術之「資訊類」、「技術類」人才，應於法律明定獎勵規定及保密機制。基於提高招募高科技產業及特定專業領域之人才之誘因，建議於本法增訂第 9 條之 1 條文「基

於國軍資通安全整體防護之需要，得對該關鍵技術之專業人才，設定特別獎勵項目及專業加給。（第 1 項）前項關鍵技術之特定專業項目、加給及保密機制與獎勵項目，由國防部會商中央主管機關擬訂，報請行政院核定公告。（第 2 項）」規定，以利招募國軍資通安全專業人才。

撰稿人：蘇顯星