10.6326/NDJ.202209_37(3).0003

國軍應對網路攻擊之法理框架
Investigating the Legality of the R.O.C. Armed Force's Response to Cyber Attacks

李彥璋 (Yen-Chang Lee)
國防大學管理學院上校教師

摘　　要

由於科技不斷的進步，網路攻擊(Cyber Attack)儼然逐漸成爲現代戰爭之新型態，其混合運用常規與非常規手段，超越傳統地緣戰略模式，並創新諸般組合攻擊手法，與傳統攻擊手段相較起來，更具靈活性及多樣性等特點，已漸次成爲新興作戰思維的環節。然網路空間相關國際法規的不確定性及模糊性，造成國家間衝突的潛在因素，且國際社會尚難將現有的國際法原則，或規則運用在網路空間的規範上，亟待持續就網路空間之議題進行研究。因此，如何在符合國際法及國內法之規範下，有效運用並發揮軍隊的多元化功能，深化全球化、資訊化的國土防衛，加以阻卻國家組織型的網路駭客入侵活動，避免國家關鍵基礎設施(Critical Infrastructure)遭受損壞，並建構安全、可靠的隱形國土安全防護網路，實屬刻不容緩之事。

關鍵詞：武力攻擊、網路攻擊、關鍵基礎設施、和平時期、間諜

Abstract

Due to the continuous advancement of technology, cyber attacks have gradually become a new type of modern warfare. It uses a mixture of conventional and unconventional methods, transcends traditional geostrategic models, and innovates various combination attack methods similar to traditional attack methods. In comparison, it is flexible and diverse, and this new way of fighting has gradually become a critical part of emerging combat thinking. However, due to the uncertainty and ambiguity of international laws and regulations in cyberspace, which is a potential factor for conflicts between countries nowadays, it is difficult for the international community to apply the existing international laws in cyberspace. It is imperative that scholars should continue researching issues of cyberspace. Therefore, how to use and exert the diversified functions of the military in compliance with the norms of international and domestic laws becomes very important. Besides, it is also an urgent matter to deepen the globalized, digitalized homeland defense, and prevent state-organized cyber hacking activities.

Hence, it is a challenging and needed task to avoid the damage of critical national infrastructure and construct a safe and reliable network to protect invisible homeland security.

Keywords: Armed Attack, Cyber Attack, Critical Infrastructure, Peacetime, Espionage

壹、前　　言

2013年美國國安局(National Security Agency)外雇人員史諾登(Edward Snowden)揭發美國對多個友邦、對手國（包括對中國大陸）的蒐集情報事件，美國媒體、企業也遭中國大陸網路駭客入侵。2015年美國政府指控中國大陸駭客入侵竊取聯邦人事管理局(Office of Personnel Management)資料，而使網路安全逐漸成為現今最棘手的問題。美國前總統川普(Donald J. Trump)政府的美中關係更進入網路科技的「圍堵戰」；而拜登(Joe Biden)政府更警告「網路攻擊可能觸發真槍實彈戰爭」。[1]

近年來國際實踐中不乏有網路攻擊的案例發生，從2007～2009年、2011年，美國國防工業公司洛克希德．馬丁公司(Lockheed Martin Corporation)先後遭中國大陸網路駭客入侵竊密，致美國F-35戰機引擎與雷達設計圖遭竊。[2] 再者，2021年7月2日，專門開發網路、系統與資訊科技基礎設施託管軟體的美國業者Kaseya，其所用於監測、管理企業伺服器、電腦等網路設備遭受到駭客攻擊，致約莫數千家小型企業受到衝擊，初估損失金額高達7,000萬美元。

由此可見，各國間的軍事攻擊已不僅僅侷限在傳統的武力攻擊，隨著資訊科技的進步，亦逐漸延伸至網路上的相互較勁；就軍事作戰而言，網路戰對於軍事嚇阻、戰力投射及戰略威脅，亦具有相當程度的影響力，[3] 進而更可左右他國之認知與決策，達到預期規劃作戰效益。攻擊行動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，進而達成破壞關鍵基礎設施(Critical Infrastructure，後簡稱CI)之目的，時值今日各國運用網路攻擊達成癱瘓，甚至攻擊敵國CI之作戰思維已然確立。

然而，關鍵爭議處在於，網路攻擊是否可視為《聯合國憲章》(Charter of the United Nations)第51條 [4] 所定的武力攻擊(Armed Attack)行為？其法律定性為何，國家間可否援引自衛權予以反擊，且現今國際社會如

1 Simon Sharwood, "Biden Warns 'Real Shooting War' will be Sparked by Severe Cyber Attack; Suggests Incident 'of Great Consequence' in the Real World Could be a Tipping Point," *The Register*, July 28, 2021, <https://www.theregister.com/2021/07/28/biden_cyber_attack_real_war_prediction/>, last visited December 23, 2021.

2 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (Victoria Australia: Scirbe Publication, 2018), p. 100.

3 The White House, *A National Strategy for A New Century* (Washington DC: The White House, 1998), pp. 7-9；蘇紫雲，〈國家安全與國防戰略思維的競合與定位〉，《國防情勢特刊—國安、國防戰略思維面面觀》，第11期，2021年8月，頁7-8。

4《聯合國憲章》第51條前段規定：「聯合國任何會員國受武力攻擊時，在安全理事會採取必要辦法，以維持國際和平與安全以前，本憲章不得認為禁止行使個別或集體自衛之固有權利」。

何論就網路攻擊，如何在國際法之規範下適用，皆是值得深究與釐清之議題。

雖「網路戰」一詞為常見用語，然在國際法層次討論上，卻甚少以網路戰作為主要用語，反而使用「網路攻擊」與「網路行動」居多；另觀察國際法文獻對於網路戰(Cyber Warfare, Cyberwar)及網路攻擊(Cyberattack, Computer Network Attacks)等用語不一而足，由於定義不易，且描述不一，為使本文討論議題聚焦，避免落入名詞解釋疑義；本文參據《網路行動國際法塔林手冊2.0版》(Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations)，以下簡稱《塔林手冊2.0版》第92點，關於網路攻擊之定義：「網路攻擊是一種網路行動，無論是攻擊性的或是防禦性的，可合理預期將會造成人員傷亡、物體損害或破壞」。[5]由於影響國際性或非國際性武裝衝突的因素頗多，為免名詞釋義不同致議題失焦，爰不再予細分網路戰或網路攻擊等用語，本文所指涉均泛指同一事項。

綜上所述，考量軍隊是確保國家利益的第一線力量，在戰爭時期，展開全面作戰，由國家總體動員，集中精力於軍事行動，誠無疑義；惟在和平時期，應在符合國際及國內規範前提下，始得展開軍事作為。而為使國軍網路防衛行動能在符合相關國際法與國內法之框架下推展，使網路部隊能在法治國原則下建立相對應之反制措施，並能與現行部隊指揮管制流程相結合，期藉本文探討業管部門究能否將網路攻擊反制程序納入平時部隊訓練，俾使戰時能迅速投入作戰序列，即時因應新型態戰爭，為保衛國民的財產與安全而時時整備及戒備，有效保護我們的數位國土。

貳、網路攻擊行動重要案例及意涵

隨著戰爭手段及型態的改變，近年來國際間網路攻擊(cyber attack)事件頻傳，而網際網路是一個超越傳統地緣戰略的虛擬空間，其攻擊方式除可藉由電腦病毒侵入各種網路應用領域，並得滲入各機關或組織內部對電腦進行打擊、癱瘓或破壞等，甚至造成實體上之損害，與傳統攻擊手段相較起來，更具靈活性及多樣性等諸多特點；且網路攻擊所花費的成本，遠低於傳統攻擊所耗費之費用，但所造成的人員傷亡及設施破壞，與傳統的軍事攻擊相比，幾乎具有同等甚至超過的嚴重程度。[6]因此，國際間多數國家均認為未來網路戰爭，將不再僅是屈居於不對稱戰力的附屬地位，也越趨重視網路攻擊之相關議題，因此各國紛紛成立獨立的資訊軍種部隊及相關的指揮結構體系，以鞏固國家安全。

20世紀90年代後期網路戰發生的可能性微乎其微，然而在「大規模干擾性武器」這個名詞出現了10年之後，網路上發生了多起

5 "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." Michael N. Schmitt & Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University, 2017), Rule 92.

6 網路攻擊的方式計有竊取機密資料、癱瘓資訊系統、侵入電腦控制系統藉以摧毀資訊或支持資訊的基礎設施，諸如發電廠、供水系統、水庫、電訊，交通、廣播電視、航空、航海等；達到實際使軍事設備、武器損壞或暫時失靈或產生錯誤功能，造成人員直接或間接傷亡。

對社會安全構成嚴重威脅的網路戰事件。

近年來國際間發生網路攻擊事件頻傳，除了難以就其下一確切定義外，且網路攻擊行為態樣多變，進而影響政府及社會運作，造成人民傷亡或財產損失，以及造成環境改變或其他足使國人生活、經濟活動、公眾安全，甚而會對國家安全構成威脅。[7] 茲就近年來國際間，較具代表性之網路攻擊行動重要案例及意涵加以說明，以瞭解其嚴重性：

一、愛沙尼亞分散式阻斷服務攻擊

2007年4月27日，愛沙尼亞政府決定將位於塔林市中心之二戰紀念碑重新安置在塔林（愛沙尼亞共和國首都），工程當天引發示威抗議，除出現群眾暴力行為並與警方發生對峙衝突，在愛沙尼亞網路上亦持續引發抗議，並有人在網路論壇上發帖，指導人們參與展開對愛沙尼亞政府系統進行分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)，[8] 成千上萬的俄羅斯用戶受到網路郵件的鼓動及指導，同時向愛沙尼亞政府計算機系統發送網路數據包，除使得議會的電子郵件服務器無法使用，系統持續12個小時處於離線狀態，並突破愛沙尼亞政黨的網路伺服器安全防護，對系統進行竄改，造成該國超過約1千萬歐元的經濟損失。

此網路攻擊事件所產生的效果，預示了DDoS在日後涉及計算機的紛爭中所扮演之角色，也是政治因素引發網路戰的開端，[9] 普遍認為是人類史上第一場網路戰爭。

二、俄羅斯政府軍入侵喬治亞事件

2008年8月，為了把喬治亞從南奧塞提共和國驅逐出境，俄羅斯軍隊入侵喬治亞，此次軍事行動展開的同時，也伴隨了大量經過協調的網路攻擊行動，雖然沒有證據顯示網路攻擊與常規部隊有所配合，且俄羅斯政府堅決否認；然而，一些安全專家認為，網路和地面部隊之間存在某種協助，例如：媒體和通信設施並不是動能手段(kinetic means)的目標，[10] 這可能是因為俄羅斯成功地實施了網路攻擊；另外俄羅斯駭客同樣地攻擊一個出租柴油發電機的網路，[11] 可能的原因是為利常規軍的行動，而打擊喬治亞電力基礎設施並提供支援。

這是第一次與大規模地面作戰行動配合的巨量網路攻擊，造成喬治亞境內之伺服器與網路流量開始遭到外部控制，並持續遭受

7 Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace* (Tallinn: NATO CCD COE, 2013), pp. 8-10.

8 分散式阻斷服務攻擊(Distributed Denial of Service)指利用異地電腦組成之傀儡僵屍網路，灌爆另一個電腦系統的連線或處理程式，使該系統無法提供服務；See Joshua Kastenberg, "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law," *Air Force Law Review*, No. 64, 2009, p. 43.

9 Franklin J., Paxson V., Perrig A., Savage S., *An Inquiry into the Nature and Cause the Wealth of Internet Miscreants* (New York: ACM, 2007), pp. 375-388.

10 動能手段(Kinetic Means)指的是使用子彈和炸彈的常規戰爭；See Rohini J. Haar, Vincent Iacopino, Nikhil Ranadive, "Death, injury and disability from kinetic impact projectiles in crowd- control settings: a systematic review," *Open Access*, No. 7, 2017, pp. 1-9.

11 Captain Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review*, November-December 2011, pp. 63-65.

DDoS，造成喬治亞網路數度癱瘓，使喬治亞政府與其人民及外界聯繫中斷，對政府、媒體以及民眾均產生了重大影響。此外，雖然此次網路攻擊不能直接與俄羅斯政府聯結起來，但網路攻擊的效益極佳，本事件成為混合戰（即資安攻擊結合常規部隊交互運用）的最佳示範。

三、美軍對伊朗政府發動網路攻擊

自2019年5月以來，美國聲稱伊朗發射導彈，擊落一架飛越霍爾木茲海峽附近海域的美軍無人偵察機，雖然該政府否認，但美國與伊朗兩國間陷入緊張情勢。美國網路司令部(U.S. Cyber Command)並於2019年6月20日對伊朗的情報組織和軍事電腦系統發動網路攻擊，導致其火箭和導彈發射系統癱瘓，惟未造成任何人員物理性傷亡；但五角大廈以相關政策涉及保護軍事行動安全為理由，拒絕對相關導報予以評論。

此外，2018年退役的前駐韓美軍司令部布魯克斯(Vincent Brooks)亦說明，各國政府通常都不會針對網路攻擊行動發表評論，包括美國政府也不例外。

但美國媒體在報導美軍對伊朗軍用網路系統發動攻擊時，曾敘述到：此次行動顯示美軍的網路攻擊能力正趨於成熟，並比以往更願意考慮使用這個選項對付包括中國大陸在內的潛在對手。[12]

四、殖民管線公司遭病毒癱瘓系統

2021年5月7日，美國境內最大的輸油管系統營運商殖民地管道公司(Colonial Pipeline，後簡稱CP)，在美國配置管線長達5,500哩（約8,851公里），佔美國東岸燃油供應的45%，也負責美國7個機場的燃油供應；在遭到DarkSide駭客使用勒索軟體攻擊時，癱瘓了所有管道作業系統，使得美國燃油供應不足，油價更因此上漲，並迫使美國政府宣布進入緊急狀態(State of Emergency)，以確保華盛頓特區及其他17個州的燃料供應無虞。

根據美國國土安全部旗下的網路安全暨基礎設施安全局(Cybersecurity & Infrastructure Security Agency，後簡稱CISA)調查，[13] DarkSide駭客不僅成功入侵CP內網，取得公司加密檔案，並下載將近100GB的檔案資料。

此事件驚動了美國政府，美國總統拜登也在記者會上特別說明此事，指出他們相信執行該攻擊的駭客居住在俄羅斯，但不認為俄羅斯政府與此有關，也已要求該政府應採取行動來打擊這些勒索軟體集團。最後，由CP支付了440萬美元的贖金，才使得網路恢復正常，這是在美國歷史上目標最大的石油基礎設施網路攻擊。

以上事件不過為近年網路攻擊事件之冰山一角，在事件爆發後，各大企業除自行解決外，同時積極與美國政府如FBI、CISA等部門合作，對事件進行詳細蒐證與調查。而參考美國國防部(U.S. Department of Defense, DoD)所發布「2018年網路戰略報告摘要」

12 Jeff Seldin, "Trump Reportedly Approved Military Retaliation after Iran Shootdown of US Drone," *VOA News*, June 20, 2019, <https://www.voanews.com/a/middle-east_trump-reportedly-approved-military-retaliation-after-iran-shootdown-us-drone/6170398.html>, last visited December 26, 2021.

13 Cybersecurity & Infrastructure Security Agency, Alert(AA21131A)-DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware, *National Cyber Awareness System*, July 8, 2021, <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>, last visited January 7, 2022.

(Summary: Cyber Strategy 2018)中所訂立的政策表明，[14] 於平常時期僅進行網路空間情報蒐集之軍事網路能力，並於危機時期，將平常時期所蒐羅之情報，運用在反制準備破壞，或阻止惡意之網路活動。

盤點上述多起以網路為執行任務要角之知名案例，可歸納出網路攻擊最主要的流程為「利用電腦程式控制或破壞對方資訊系統運作，進而達成主要任務之目的」，而此既定流程，迄今大致仍維持不變。而攻擊手法之主要趨勢，由過去常見的DDoS或網域名稱系統(Domain Name System, DNS)威脅，[15] 轉向勒索軟體為大宗。

近年的網路攻擊事件，越來越難認定攻擊發起者，且目標也逐漸轉向民生基礎設施，除造成生活之不便利，甚而影響一國整體經濟穩定，危害程度實不亞於傳統軍事攻擊。

且由於軍事和民用系統之間相互聯繫的普遍性，以及軍方對民用基礎設施的依賴，使得CI與國家安全具有高度連結性，從而各國為追求網路戰主動權，近年來紛紛組建網路戰部隊，企圖搶奪制網的空間及優勢，達到破壞對方網路系統、控制戰爭和削弱敵軍戰鬥力之目的。目的除出於公開宣揚國力之外，另擇定軍事設施為任務目標，攻擊者較難匿蹤，且容易遭受報復反擊，故攻擊軍事目標（如美國對伊朗政府發動網路攻擊）始屬特別例外之情形。

參、國際法上對於網路攻擊之規制

中國大陸於2015年軍改後，成立「戰略支援部隊」，專責網路攻防與電子對抗作戰任務，將主管情報、電戰、指管及心戰等過去分屬不同職能之組織單位納入管轄；[16] 持續強化推動「媒體融合」(Media Convergence)與「軍民融合」(Military-Civilian Integration)的發展策略，建構科技與網路強國戰略；[17] 並自2016年起，即計畫性的以我國作為其「無煙硝戰爭」之演練對象，藉由網路空間及社群媒體之操作，進行多元網路攻擊手段，包含對我國科技竊密、利用爭議訊息分化群體，與滲透破壞CI等項。

由於戰爭是指「國家間進行具有相當規模且持續一定期間的武力鬥爭」，就目的性而言，戰爭是國家遂行意志，迫使敵人服從的一種暴力行為。德國軍事理論家克勞塞維茲(Carl Philipp Gottfried von Clausewitz, 1780-1831)曾言：「戰爭是政治活動延續之另一種形式」。[18] 如國家面臨戰爭狀態，即國家安

14 Summary: Cyber Strategy 2018 Introduction: "We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict." U.S. Department of Defense, *Summary: Cyber Strategy 2018* (Washington: Department of Defense, 2019), pp. 1-2.

15 DNS通道穿越攻擊(DNS Tunneling)、DNS快取毒害攻擊(DNS Cache Poisoning)、DNS漏洞攻擊(DNS-based Exploits)，甚或藉由傳遞不正確DNS封包、釀成癱瘓式無窮迴圈，皆會讓企業不堪其擾。

16 林穎佑，〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第15卷第10期，2017年10月，頁104-112。

17 董慧明，〈大陸「軍民融合」發展戰略之現況與問題評析〉，《展望與探索》，第14卷第3期，2016年3月，頁31-34。

18 Carl von Clasuewitz, trans. Michael Eliot Howard and Peter Paret, *On War* (Princeton: Princeton University Press, 1989), pp. 1-3.

全受到嚴重威脅時，軍隊將處於最高級別的備戰準備，並向全國發布戰爭動員令的戰鬥緊張情勢。

但由於科技不斷的進步，網路攻擊儼然逐漸成為現代戰爭之新型態，其混合運用常規與非常規手段，並創新諸般組合攻擊手法，亦模糊武力攻擊的界限；而網路攻擊發展與盛行之主要因素如下：一、民主、自由、多元社會本身的弱點；二、低強度、低成本的軍事、外交手段與工具，成為有利與有力之工具，且現代戰爭所費不貲，在以經濟發展為主流的國際環境中，導致低成本的混合戰手段日趨盛行；三、國家權力對比的極化所產生刺激，混合戰能提供較為弱勢的一方，擁有平衡優勢對手的手段；四、軍民融合與軍民通（共）用戰術促動；五、地緣、種族親緣等環境因素，[19] 給予實施混合戰更佳之場域。

其次，網路攻擊呈現當前資訊、科技時代的戰爭模式，可靈活運用混合、創新，與不對稱的戰術、戰法，進而達成破壞目標國政經穩定及城市發展，更能轉化運用打擊新聞及言論自由之弱點，造成備戰目標的重大挑戰。

為此，全球有超過20個國家或地區，如美國、俄羅斯、英國、韓國、日本等國均積極進行網路安全戰略，針對網路攻擊實施各項演習，並設置專責網路戰機構，創設網路部隊，藉以持續強化本國實力。但當各國訴諸網路工具以延續其政治活動時，對於此新型態的「武力」手段如何適用於現行國際規範，亦產生衝擊與挑戰，故有再為予以探究之必要。

一、現行國際法制尚未具明確規範

誠然，國際法之形式法源(Formal Sources)乃指條約、國際習慣法與一般法律原則；[20] 縱然歐洲理事會(Council of Europe)有鑑於電腦及網路犯罪之嚴重性，且多屬於跨境犯罪，需要國際間的合作與互助，才得有效遏止及防範，期強化各國對抗網路犯罪之能量與跨國間之互助，[21] 遂於2004年7月正式生效「網路犯罪公約」(Convention on Cybercrime)，係首部針對網路犯罪行為所制定之國際公約，主要係針對網路犯罪類型、執法機關蒐證權限及國際合作關係進行探討。但該公約對於造成「相當嚴重性」程度的人員傷亡或重大財產損失之網路攻擊行動，由於各國無法達成一致決議，[22] 故此公

19 Andrew Radin, *Hybrid Warfare in the Baltics-Threats and Potential Response* (Santa Monica: Rand Corporation, 2017), pp. 7-9；黃柏欽，〈戰爭新型態—「混合戰」衝擊與因應作為〉，《國防雜誌》，第34卷第2期，2019年6月，頁64。

20 另外國際法判例、國際法學說、國際機構之決議、宣言或公允善良原則等，可作為國際法形式法源之補充資料，並能更明確之適用；David Kennedy, "The Sources of International Law," *American University International Law Review*, Vol. 2, No. 1, 1987, pp. 2-3.

21 Council of Europe (ETS-No. 185), Convention on Cybercrime, 2001, pp. 1-2. 有鑑於網路犯罪的跨國性，以及各國法規的不一致，歐洲理事會希望藉由訂定《網路犯罪公約》，建立一套國際一致的標準，共同對抗網路犯罪，主要是對於網路犯罪實施法律管制；至於網路攻擊的行動，需在有明確證據證明該行動是由某國發起、支持或負責的具體情況下，方可適用禁止使用武力原則予以制止。

22 Peter Csonka, "The Council of Europe's Convention on Cyber-Crime and other European Initiatives," *International Review of Penal Law*, Vol. 77, 2006, p. 495.

約並未具體規範，由各國自行決定。

另一為「網路行動國際法塔林手冊」(Tallinn Manual on the International Law Applicable to Cyber Operations，以下簡稱塔林手冊1.0版)，此源於愛沙尼亞在2007年遭受大規模網路攻擊後，位於該國首都塔林之北約網路防衛合作中心邀集涵蓋國際法、資通電技術及軍事等領域之數十名專家，共同於2009年編纂網路戰國際法手冊，嗣於2013年編修完成《塔林手冊2.0版》。儘管此手冊並非屬於官方正式文件，且國際社會迄今尚未針對網路攻擊制定專門條約，但完成手冊之主要目的在使當前國際法規制，得以適用於網路行動，並據以在符合《聯合國憲章》的規範下，對於未達該憲章第2條第4項所規定使用武力的程度，也不構成國際人道法下武裝衝突的網路行動，各國能參據並制定相對應的網路政策。

然由於網路空間相關國際法規的不確定性及模糊性，造成國家間衝突的潛在因素，且國際社會尚難將現有的國際法原則或規則運用在網路空間的規範上，亦難以達成一致的共識，亟待持續就網路空間之議題進行研究並展開推論。

二、網路攻擊應如何適用國際法規

進入20世紀，國際社會開始以制度和法律，將戰爭和武力使用予以限制或非法化，隨著國際聯盟(League of Nations)成立，國際社會開始討論如何建構一套制度，以減少國家間利用戰爭解決爭端的機會；[23] 其後在1928年《關於廢棄戰爭作為國家政策工具的普遍公約》(General Treaty for Renunciation of War as an Instrument of National Policy)中將戰爭非法化；[24] 1945年《聯合國憲章》則於第2條第4項中，明文對於武力使用(Use of Force)的一般性禁止，更規定武力威脅(Threat of Force)亦同樣是屬於禁止範圍內，[25] 並獲得國際習慣法(Customary International Law)的地位，對於所有國家均產生拘束力。

然而，禁止使用武力原則有兩項例外，即在符合憲章第七章所規定的集體強制行動，或憲章第51條所規定的單獨或集體自衛之權利情形下，方可考慮使用武力維持或恢復和平，且使用武力的對象往往限縮在對付「攻擊」或「侵略」者。誠有疑問者，「網路攻擊」能否歸屬於傳統武力行使之範疇，應否適用國際人道法所規定的義務或規則呢？

由於目前國際法對「網路攻擊」一詞雖尚未明確界定，惟國際法院(International

23 但是國際聯盟的爭端解決制度，並沒有將戰爭或武力使用予以非法化。

24《關於廢棄戰爭作為國家政策工具的普遍公約》又稱《巴黎非戰公約》(Pact of Paris)，或《凱洛格—白里安公約》(Kellogg-Briand Pact)。根據《巴黎非戰公約》，締約國宣布斥責「用戰爭來解決國際糾紛」，並放棄使用戰爭「作為實行國際政策的工具」；但卻沒有討論武力使用的限制。David A. Koplow, "A Nuclear Kellogg-Briand Pact: Proposing a Treaty for the Renunciation of Nuclear Wars as an Instrument of National Policy," *Syracuse J. Int'l L. & Com.*, Vol. 42, No. 1, 2014, pp. 132-133.

25《聯合國憲章》第2條第4項所規定：「各會員國在其國際關係上，不得以武力威脅或武力行使，或與聯合國宗旨不符之任何其他方法，侵害任何國家之領土完整或政治獨立」(All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations).

Court of Justice)在1996年核武器(Nuclear Weapons)案已明確認為，武裝衝突法對於任何武力的行使、迅速發展的軍事技術或一切新式武器（包括核武器）所引發的問題，均仍應有所適用，[26] 故可得知現行武裝衝突法之規範，可適用於國際性和非國際性武裝衝突的網路攻擊行為。

其次，國家欲防衛來自他國之網路攻擊行動，勢必採取許多防範措施。通常網路戰之發生係基於網路攻擊而產生，但網路攻擊並不必招致網路戰之結果。一般而言，在網路上所進行之駭客行為，亦被稱為網路攻擊，其主要是受國內法管轄之刑事犯罪行為範疇。

目前國際法對於「網路攻擊」一詞並未有明確界定；鑑此，網路攻擊能否構成國際法上所稱之武力行使或武力威脅？目前尚無定論，其主要關鍵取決於「武力」之解釋。依目前對此概念的定義及界定標準，迄今仍存有爭議，狹義說學者主張武力使用，單單指武裝力量而言；惟有廣義說學者認為不僅武裝力量，包含非武裝力量（如政治、經濟、外交等強制力）亦均屬之。然而就現今國家實踐及多數國家見解觀察得之，有關「武力」之解釋，仍大抵採狹義之武力概念。[27]

再從1970年聯合國大會通過第2625號《關於各國依聯合國憲章建立友好關係及合作之國際法原則之宣言》決議，第1項說明各國在其國際關係上應避免為侵害任何國家領土完整或政治獨立之目的，或以與聯合國宗旨不符之任何其他方式使用威脅或武力，第3項指出依照憲章不干涉任何國家國內管轄事件之義務，[28] 強調了武力使用及武力威脅的禁止。而1974年聯合國大會通過第3314號《關於侵略定義的決議》，第1條「侵略定義」係指一個國家使用武力侵犯另一個國家的主權、領土完整或政治獨立，或以與聯合國憲章不符的任何其他方式使用武力，[29] 明顯採狹義說，並再次確認憲章第2條第4項所認定「武力」的效力；故而侵略戰爭的武力使用是一項國際罪行，發動戰爭的國家或個人需負國際責任。

另從國際法院在尼加拉瓜訴美案(Nicaragua v. United States of America)之判決中，首次對「武力行使」與「武力攻擊」進行區別，[30] 必須具足夠嚴重性(Gravity)，才能提升至武力攻擊事件(Frontier Incidents)，

26 Provisions of the Charter relating to the threat or use of force "These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons." ICJ Reports (No. 96/23), Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of July 8, 1996.

27 Milorad Petreski, "The International Public Law and the Use of Force by the States," *Journal of Liberty and International Affairs*, Vol. 1, No. 2, 2015, pp. 3-5.

28 UN General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 24 October 1970, A/RES/2625 (XXV).

29 UN General Assembly, *Definition of Aggression*, 14 December 1974, A/RES/3314 (XXIX).

30 *Ibid.* "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State qualify as an act of aggression."

因此，是否構成攻擊行動，在某種程度上主要取決於行為的「規模大小及影響程度」。

換言之，認定一個行為是否構成武力攻擊，必然超過認定屬於武力行使之規模與效果。當網路攻擊造成大規模相當於傳統攻擊的物理損害或人身傷害，將可被視為武力攻擊的開始，於此同時所進行之網路攻擊行動將被認定屬武力攻擊之一環，故攻擊之方法及手段均應符合武裝衝突法之規定。因此，網路攻擊尚須受到習慣國際法與《聯合國憲章》的拘束與限制，各國政府與專家對此均持肯定的看法與立場；另一方面，由於網路攻擊未必造成如一般武裝攻擊所生之傷害與損害結果，或究竟是否構成武裝衝突，此部分在舉證以及國際法上仍存有諸多爭議及尚待論究之處。

而《塔林手冊2.0版》補充《塔林手冊1.0版》中關於武裝衝突法在網路行動之適用，並根據網路的特性，對「有效控制」之標準進行了補充與改良，更能正確認識並探索網路攻擊中有關國家責任的歸因；其中第68點規定「網路行動構成使用威脅或武力，或以與聯合國宗旨不符之任何其他方式，侵害任何會員國或國家之領土完整或政治獨立即為非法」，復於第69點規定，更就使用武力作進一步闡釋「若與該網路行動相當規模與效果之非網路行動已達到使用武力之門檻，則該網路行動也構成使用武力」，亦可做為考察和檢驗現存國際法規能否適用「新」戰爭形式的重要參考。

運用網路平臺執行攻擊的主體，不僅限於敵國的軍事機關，亦可能涵括不具有交戰資格的一般平民(Civilian Person)；而1949年《日內瓦四公約關於保護國際性武裝衝突受難者的附加議定書（第一議定書）》，以下簡稱為《第一附加議定書》中特別對民間防衛組織及要員給予保護。[31] 所謂民間防衛乃為保護一般平民於敵對行為之危險，意圖提供一般平民生存之必要條件，以遂行人道任務之一部或全部，[32] 故增加軍事行動於判定目標執行上的困難。

而據《塔林手冊2.0版》第92點規定：「無論該行動係攻擊或者防禦，網路攻擊是一種可合理預期將造成人員傷亡或物體毀損之網路行動」，[33] 故可得知具一定規模及影響程度的網路攻擊，可歸屬於武裝衝突之新型

31 1949年8月12日《日內瓦公約關於保護國際性武裝衝突受難者的附加議定書（第一議定書）》(Protocol Additional to the Geneva Conventions of 12 August 1949, and Relations to the Protection of Victims of International Armed Conflicts (Protocol Ⅰ))第48條規定：「為了保證對平民居民和民用物體的尊重和保護，衝突各方無論何時均應在平民居民和戰鬥員之間和在民用物體和軍事目標之間加以區別，因此，衝突一方的軍事行動僅應以軍事目標為對象」(In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives).

32 魏靜芬，《戰爭法學金》（臺北市：社團臺灣海洋事務策進會，2005年），頁142。

33 本規則闡釋的定義是基於《日內瓦四公約關於保護國際性武裝衝突受難者的附加議定書（第一議定書）》第49條第1款：「攻擊是指無論在進攻或防禦中針對敵方使用暴力行為」。在這一廣泛接受的定義中，將攻擊與其他軍事行動相區分的，是針對目標使用暴力。諸如心理網路行動或網路間諜行動等非暴力行動，不構成攻擊。

態攻擊模式。

三、平時國際法規範合法網路行為

《孫子兵法》「用間篇」記載：「先知者，不可取於鬼神，不可象於事，不可驗於度，必取於人，知敵之情者也」，作戰取勝的關鍵，很大程度上憑藉的是由「人」主動去獲取情報，情報取之於那些熟悉敵人內情的「人」，古往今來，東聖西賢亦皆承認此「人」的重要性，其同所指涉者即為「間諜」之意涵。

時值今日，傳統認知間諜的行為模式有所轉變，敵方作戰區不僅限於實體空間上之區域，虛擬空間的作戰模式，亦隨者科技演化而漸次展開；網路軍事行為即是一個現代化的作戰概念，與傳統上「間諜」之任務相似，平時仍以秘密或偽裝方式蒐集或刺探情報為其主要任務，殺害或毀滅敵人並非其主要目的，性質上應與主戰單位有所區隔。故而網路軍事行為在執行情報蒐集任務上，可視為「間諜」，於此並不違反武裝衝突法之規範，甚而應賦予一定程度上之地位及保護。以下即自國際法檢視「網路間諜」之合法性，或可在規範內強化此任務，亦可避免網路攻擊行動所產生的爭議。

依據1907年海牙第四公約《陸戰法規和慣例公約》與其附件《陸戰法規和慣例章程》第29條規定：「非處於交戰者的作戰地區（地帶）內，以通報對手（敵對）交戰者之意思，在隱密或虛偽的藉口（口實）下行動，而實行情報蒐集或欲蒐集者，不得視為間諜。故未實施變裝的軍人為蒐集情報而進入敵軍作戰地區內之人員，不得視其為間諜。又不問其為軍人與否，對本國軍隊或敵軍公然執行通信傳達之任務者，亦不得視其為間諜。為傳達通信及聯絡通往各個軍隊或各地之區域，而以輕氣球派遣之人員，亦同」。

而間諜行為的構成要件，必須滿足：(一)處於他方交戰者的作戰地區或作戰地帶(Zone of Operations of War)內，其中交戰者，即指對手（敵對）交戰國之軍隊；(二)須以通報對手交戰者之意思，亦即是通報敵對交戰國或另一方對手交戰國之政府或軍隊而言；(三)須以隱密的行動或虛偽藉口（口實）下之行動(Acting Clandestinely or on False Pretenses)；(四)須為蒐集情報或欲蒐集情報之人員等要件。[34]

換言之，具備上述要件者，不問其是否為軍人或非軍人（一般人民），又軍人亦不分其係為軍官或士兵，同時不論其國籍乃為敵國國籍或第三國國籍、中立國國籍，以及不問其是奉長官之命令或出於自己之意思者，同時亦不論其是出於愛國的行為或是私人利益，及其目的是否達成，[35] 皆屬於國際法上所規範的間諜行為。

此外，《塔林手冊2.0版》在第32點規定「雖各國在和平時期的網路間諜行為本身並不違反國際法，但實施該行為的手段可能會違反國際法」，[36] 由此可知，本規則可適用於非武裝衝突情形下的網路間諜行為。「網

34 Neil J. Beck, "Espionage and the Law of War," *American Intelligence Journal*, Vol. 29, No. 1, 2011, pp. 126-136.

35 歐廣南，〈間諜行為法制規範之現代意義探討（上）〉，《軍法專刊》，第64卷第3期，2018年6月，頁64-65。

36 Michael N. Schmitt & Liis Vihul, *op. cit*., Rule 32, Comment 1.

路間諜」一詞是指利用網路能力，以秘密、詐欺的方式蒐集或試圖蒐集訊息的行為；其包括但不僅限於利用網路能力監視、監控、採集或竊取通過電子傳輸或儲存的通訊、數據或其他訊息，[37] 由此檢視可得知，網路間諜行為應係屬不被禁止的「軍事行動」。

考量網路攻擊作為新型態的作戰模式，判斷是否足以構成武力攻擊，在認定及判斷上益發困難，且為避免對個人或非國家團體等非國家主體行使自衛權，違反國際法相關規範；然而，在和平時期的網路監控，在符合一定條件情況下，有可能構成國際法上的間諜行為。間諜活動自古以來被視為一種作戰的正當行使態樣，其並非以殺害或逮捕敵人為目的，而是作為探知敵情或地形的必要手段。[38] 而透過網路監視的行為，依其要件檢視，顯可屬於合法的軍事行動。

肆、國軍應對網路攻擊之法理框架

網路攻擊至今仍未有一致之國際條約就其特性加以規範，又因缺乏全球普遍性之共識，而無法直接將網路攻擊定義為戰爭行為；且網路攻擊是否構成武力攻擊，尚必須在「造成人員傷亡或重大財產損失」方面達到「相當嚴重性」的程度，才有可能構成「武力攻擊」，如此遭受攻擊之國家，也才得以援引「自衛權」實施反擊。

惟就網路攻擊的嚴重程度而言，其損失並非皆能明確達到人員傷亡或重大財產損失，再者，由於進行網路攻擊的攻擊方並非明確，甚至可能是由「非國家」為主體所發動；鑑此，即便網路攻擊其嚴重性已達武力攻擊之程度，然對於發動對象為非國家主體的私人主體，是否得援引自衛權展開反擊，[39] 此部分則仍有爭議。

2019年11月，臺灣與美國首度聯合舉行「大規模網路攻防演練」(Cyber Offensive and Defensive Exercises)，並仿效美國國土安全部每兩年舉辦一次的「Cyber Storm」網路安全演練，進行社交工程攻擊與網路攻擊實兵演練，保護智慧財產權不被他人從網路盜竊，基礎建設不被人蓄意破壞，民主體制也不受專制國家干預；[40] 另考量美國、臺灣與理念相近夥伴之間的資安政策能夠進一步深化，藉由雙方合作模式，先行探究U.S. Cyber Command所開展的一系列網路行動政策，再逐步啟動相關防衛機制，建立應對網路空間威脅戰略。

故本節先行檢視美國對於網路攻擊所相應的作為，再就我國現行法規及作法加以檢視相關行為是否符合適法性，期以茲作為日後我國應對網路攻擊的參考。

一、參考美國應對網路攻擊之作法

37 *Ibid*., Rule 32, Comment 2.

38 魏靜芬，〈網路攻擊、網路間諜及網路監控之國際法評價〉，《軍法專刊》，第65卷第1期，2019年2月，頁26。

39 同註38，頁23。

40 W. Brent Christensen, "Remarks by AIT Director W. Brent Christensen at The Opening Session of the Taiwan-led part of the 2019 Cyber Offensive and Defensive Exercises," *American Institute in Taiwan*, November 6, 2019, <https://www.ait.org.tw/remarks-by-ait-director-w-brent-christensen-at-the-opening-session-of-the-taiwan-led-part-of-the-2019-cyber-offensive-and-defensive-exercises/>, last visited January 5, 2022.

按網路攻擊之類型化結果，參酌美國洛克希德馬丁公司(Lockheed Martin)所提出之「網路狙殺鏈」與美國MITRE網路安全公司所提出之「ATT & CK矩陣模式」，為近代資安政策主流框架。MITRE公司擬定「偵查、武裝、派送、漏洞利用、安裝、命令控制、達成目的」七大階段，[41] 主要包含「簡訊誘導、魚叉式釣魚郵件、網頁漏洞攻擊、資料庫隱碼阻斷攻擊」等項反制措施；可由三大構面加以區分，從基本的網路防護能力(General Cyber Defense)、網路欺敵(Cyber Deception)，及與攻擊對手的交戰行動(Adversary Engagement)，開展出8個戰略，[42] 與36個不同技法，[43] 試圖提前阻止與偵測攔截攻擊，可爰引作為國軍反制網路攻擊之參據。

應對新時代的網路戰略，美國國防部發布「2018年網路戰略報告摘要」，藉以擬訂網路軍事行動的政策及規劃；[44] 首先美國國防部設定三個主要目標：(一)採取網路行動以蒐集情報並加強部隊的網路作戰能力；(二)網路防禦措施的「前置化」，在源頭干擾或阻止惡意的網路攻擊行為；(三)強化對現在和未來全國軍事優勢有貢獻的網路及系統的安全性與抵抗力。

美國國防部更提出一系列關於網路空間之競爭與威懾的措施，包括：(一)以保護國防部敏感資訊，及威嚇網路上對全國及其盟友構成使用武力的惡意攻擊為優先手段，若威嚇手段無效，聯合部隊會準備好使用所有的軍事能力應對外來威脅；(二)網路部隊會透過強化國防部網路安全與採取「前置性」的攔截與制止手段，持續性(Persistently)的對抗惡意網路活動；(三)美國國防部會與其他政府機關及民間單位合作，加強美國關鍵基礎設施對抗惡意網路攻擊的能力。

觀察國際上資安政策之發展，各國透過擬定國家資安戰略，揭示其所關注的資安發展重點，面對國際情勢動盪與網路攻擊加劇，資安防護亦應同步提升，過去被動的資安防護，恐不敷使用。而現今已有部分國家，如英國、美國於資安政策文件中，融入「主動式網路防禦」(Active Cyber Defense，後簡稱ACD)之概念，[45] 更向前一步的抵禦資安攻擊，ACD即「摧毀、消滅敵人的直接防禦措施，或降低友軍與其資產之網路威脅的

41 在偵查、派送、安裝及命令控制階段，較可能利用「釣魚郵件」、「密碼破解」等手法執行目標偵蒐，並將攻擊工具派送、安裝於目標系統，待命觸發以取得目標系統之控制權或阻斷其服務；MITRE ATT & CK, *Resource Development*, <https://attack.mitre.org/>, last visited January 5, 2022.

42 包括引導管道(Channel)、收集(Collect)、牽制(Contain)、偵測(Detect)、破壞(Disrupt)、促成(Facilitate)、合法化(Legitimize)、測試(Test)。

43 多數與欺敵誘餌有關，包括誘餌帳號、誘餌內容、誘餌帳密、誘餌多樣性、誘餌網路，以及誘餌角色、誘餌過程與誘餌系統等；Christina Fowler, Mike Goffin, Bill Hill, *An Introduction to MITRE Shield* (Virginia: MITRE, 2020), p. 10.

44 U.S. Department of Defense, *op. cit*., pp. 6-7；林勤富、吳建輝、陳怡靜、楊蕙亘，《國防部109年度委託研究計畫報告（案號：HC09109P099）—國軍對於網路戰反制作為之法律建置暨運用》（臺北市：國防部，2020年），頁84-85。

45 孫鈺婷，〈國際資安防護政策趨勢探討—關於「主動式網路防禦」〉，《科技法律透析》，第32卷第1期，2020年1月，頁37-46。

有效性」，係針對特定威脅所產生的直接行動。

另參考北大西洋公約組織(North Atlantic Treaty Organization, NATO)，就ACD定義為「一種主動措施，用來偵測或取得有關網路入侵、網路攻擊或即將發生的網路行動資訊，或用來判定一項行動的來源，以對抗入侵來源」。惟最大爭議點在於是否可以進行「反擊」，若可以「反擊」，則應判斷發動是否具有正當性，實際的運作及發展仍持續辯論中，且有政治與法律層面的風險；尤須注意者，ACD並非取代傳統的資安防禦措施，而是作為補充手段，正本清源之道，各國仍應從基礎建構穩健的資安環境做起。

二、國軍平時應對網路攻擊之檢視

我國於2017年7月1日依國家安全戰略指導，整合國軍現有資通電部隊，編成資通電軍，[46] 統合網路、電子及資通平臺等三大領域，籌建可恃之國軍資通電戰力，並在從事國家情報事項範圍內，視同情報機關。

按國家情報工作法第3條第2款規定：「二、情報工作：指情報機關基於職權，對足以影響國家安全或利益之資訊，所進行之蒐集、研析、處理及運用」。國防部參謀本部通信電子資訊參謀次長室（以下簡稱通次室）及資通電軍指揮部（以下簡稱資通電軍）於平時主責為網路情蒐、網路防護及網路滲透等任務之執行與管制，性質上初步符合國際法所規範間諜之構成要件，而透過網路監視的行為，自然是屬於合法的軍事行動。

且國防法第14條規定：「軍隊指揮事項如下：一、軍隊人事管理與勤務。二、軍事情報之蒐集及研判。三、作戰序列、作戰計畫之策定及執行。四、軍隊之部署運用及訓練。五、軍隊動員整備及執行。六、軍事準則之制頒及作戰研究發展。七、獲得人員、裝備與補給品之分配及運用。八、通信、資訊與電子戰之策劃及執行。九、政治作戰之執行。十、戰術及技術督察。十一、災害防救之執行。十二、其他有關軍隊指揮事項」。其中「通信、資訊與電子戰之策劃及執行」解釋上即涵蓋國軍網路部隊之任務，職司防禦性、偵蒐性及阻斷性措施之策劃與執行；亦即可在符合指揮鏈層級及狀況任務分配下，由通次室督導資通電軍針對國家網路遭受侵入、破壞時，擬定類似相對應軍事行動之反制措施，依不同情況，授權合宜層級且具決定權之指揮官下達執行命令，由此可知，國防法第14條之規定似已能達到原則性之授權規範。

而國防部資通電相關部門平時之任務係以情資蒐集為主要目的，並加以蒐整研析；而戰時或武裝衝突發生時，則運用平時情蒐所得之CI相關資料，發揮阻斷性之功能，對目標發動網路攻擊使其失去運作能力。

由於軍隊是捍衛國家權利及展現權力的武裝力量，也是維護國家利益的防衛工具，主要功能是代表國家行使武力的主體，更應在符合規範之前提下妥慎運用。且網路攻擊往往橫跨數個管轄權，攻擊對象亦不限於軍方，亦涵蓋政府部門、民間企業，或是各種

46 國家情報工作法第3條第2項規定：「海洋委員會海巡署、國防部政治作戰局、國防部憲兵指揮部、國防部參謀本部資通電軍指揮部、內政部警政署、內政部移民署及法務部調查局等機關（構），於其主管之有關國家情報事項範圍內，視同情報機關」。

CI，純以軍事機關為攻擊目標的公開案例，尚難以見諸於相關公開報導。

我國目前對於網路攻擊的反制措施，主要係由資安公司進行第一波的善後處理，先行回復正常狀態；嗣後由法務部調查局進行刑事調查，對於網路攻擊涉及之刑事犯罪進行犯罪偵查，[47] 並與相關國家交換情資，進行共同偵辦。

國防部資通電相關部門亦在防衛國家網路安全的前提下，扮演一定的角色，除了協助犯罪偵查以外，國軍於平時可參考仿效美國之作法，以「執法行動」作為主要遏阻網路攻擊手段，透過政府跨部會合作，或公、私合作的方式協力進行，強化國防部與法務部之橫向協調，在符合國際法相關規範及國家安全之前提下，運用非戰爭軍事行動之手段，實施相對應之反制措施。

依照我國現行指揮鏈規範，軍隊指揮權屬於總統，由總統責成國防部長命令參謀總長指揮軍隊遂行各項軍事任務，而「通信、資訊與電子戰之策劃及執行」亦屬軍隊指揮事項。[48] 基此，資通電軍之網路行動均應受參謀總長指揮；[49] 惟如各項網路行動倘均應由總統、部長，參謀總長之逐級命令制度指揮，就網路行動立即性之特徵，能否達成迅速反應之目的，非無疑義。或可參照美軍的指管系統模式，部分網路行動之任務執行，授權由適當層級人員實施，或建立事後呈報審查機制，加速對抗惡意網路攻擊的反制措施。

就國內法而言，目前我國對於軍事行動並未制定專法，然因戰場狀況瞬息萬變，軍事行動必要依據客觀環境、狀態及他方作為，而實施適當且迅速之反應，如欲制定專法加以規範，誠有其必要性；惟恐亦僅能就原則性之規範加以訂定，實無法就多元且複雜的軍事行動作出詳細之規範，故授權國防部訂定相關規則，使第一線部隊人員據以因應，實有其必要性及急切性。

伍、結論與建議

在戰爭違法化的趨勢下，「禁止使用武力與威脅原則」已具有習慣法與絕對法的地位，全球議題日趨複雜且多元，傳統與非傳統安全議題交互影響國際局勢的發展；目前雖無真正戰爭意義的網路戰爭發生，但網路空間的軍事行動，對於國際安全與國家戰略仍有龐大的影響力，而在「網路攻擊」定義、規範不明確之際，倘貿然動用軍隊行使防護或攻擊，恐違反國際法及產生嚴重的爭議，因此各國政府在對於網路攻擊的判斷上，均採取較為保守的態度及作法。

因此，如何在符合國際法及國內法之規範下，有效運用並發揮軍隊的多元化功能，因應全球化、資訊化的國土防衛，阻卻境外勢力，或國家組織型網路駭客入侵等活動，

47 林勤富、吳建輝、陳怡靜、楊蕙亘，同註44，頁121-122。

48 我國憲法第36條規定：「總統統率全國陸海空軍」。而國防法第8條規定：「總統統率全國陸海空軍，為三軍統帥，行使統帥權指揮軍隊，直接責成國防部部長，由部長命令參謀總長指揮執行之」；同法第九條復規定：「總統為決定國家安全有關之國防大政方針，或為因應國防重大緊急情勢，得召開國家安全會議」，明確規範了總統在國防軍事事務的指揮權及指揮的程序。

49 國防法第13條規定：「國防部設參謀本部，為部長之軍令幕僚及三軍聯合作戰指揮機構，置參謀總長一人，承部長之命令負責軍令事項指揮軍隊」，明確規範了參謀總長與部長間的隸屬關係。

避免國家CI遭受損壞，誠屬刻不容緩之事；爰此，結合本文論述脈絡，茲綜整檢視分析如下：

一、從國際法層面檢視現有之作為

《聯合國憲章》第2條第4項規定「各會員國在其國際關係上不得使用威脅或武力，或以與聯合國宗旨不符之任何其他方法，侵害任何會員國或國家之領土完整或政治獨立」，此條款又稱為武力不行使原則，雖然當今國際社會對於「武力」(Force)之定義多半採狹義說，即視為武裝武力(Armed Force)之意；然鑑於網路行動可能造成多種態樣，及以國家為後盾支持，進而攻擊他國重要經濟CI的操作行為不斷增加，因此可將網路攻擊行動在符合一定要件之情況下視為武力行使。

而所稱之一定要件，可以從《塔林手冊2.0版》以規範及效果之角度總結八項要素（即嚴重性、即時性、直接性、侵入性、合法性、軍事性、效果的可衡量性及國家的介入程度以為判斷），以輔助判斷網路行動是否屬於「武力行使」；雖手冊中同時強調前揭要素並未完全詳盡所有情況，且非屬絕對的，但一個行為究竟是否屬於武力行使(Use of Force)，可由各國參酌具體實際情況後，再加以適用。

若具體武裝衝突事件發生，已構成上述國際法上之武力行使或武力攻擊，當遭受網路攻擊之際，應可視為武力行使，則依《聯合國憲章》第51條之規定「聯合國任何會員國受武力攻擊時，在安全理事會採取必要辦法，以維持國際和平及安全以前，本憲章不得認為禁止行使單獨或集體自衛之自然權利」。應允許一國受到攻擊時，得以動能或網路之使用武力方式回應，以符合自我防衛之權利。

惟鑑於武力攻擊的構成要件，長久以來都未能確立，而網路攻擊作為一種新型態的作戰型態，判斷是否構成武力攻擊，在認定及判斷上就益加困難。儘管《塔林手冊2.0版》在第92點的評論中指出，當符合「導致人員傷亡或物體毀損」之要件時，可視為網路攻擊，惟此規範並非全然明確且具體；此外，在可能會滿足武力攻擊的「規模大小及影響程度」之要件，在客觀公平性上的判定，也是備受爭議。[50] 再者，即便網路攻擊符合武力攻擊要件時，遭受攻擊國家是否有權展開反擊（諸如：個人或非國家團體等非國家主體行使自衛權等行為），這也是國際法學界長久以來備受爭議的問題。雖然個人在符合一定條件下，得為國際法上之主體，但是與國家的國際法地位相比較，個人的權利及義務仍然是較受限制的情況。

因此，在符合武裝衝突法之相關各公約、《第一附加議定書》或國際習慣法，於不使用特定非法手段的前提下，或可強化資通電軍於「網路間諜」之訓練及反制，使能於和平時期實施防衛任務，保衛國家安全。

二、從國內法層面檢視現有之作為

國內現行法並無針對軍隊之軍事行動訂有專法，盤點國內法可資適用於網路行動者為國家安全法、國家情報工作法與國防法，而該三法主要均為原則性之規定，現行實務上有關軍隊之行動、範圍，仍以行政規則及命令為依歸。

目前我國對於遭受武裝攻擊時，已訂有

50 Michael N. Schmitt & Liis Vihul, *op. cit*., Rule 71, Comment 6.

相關計畫及想定，作為實施反制之準據，因此當遭受網路攻擊時，或可再由通次室或資通電軍就各項具體任務，訂定迅即反應的軍事行動教範或準則，俾在面對外來的各項網路威脅時，能對於不同層級、輕重、程序的狀況展開相對應的反制措施，亦能提升整體國家安全防護。

儘管國際法意義上之網路戰並未真實發生，然而網路戰時代早已悄然到來；國軍在面對全球化網路新興議題，在現行體制架構下，除重視網路安全與網路戰之國際法與武裝衝突法之問題以外，應更新考量網路攻擊多樣性、匿名性、隱密性、防止困難性等多項特徵，配合修訂新型態網路戰爭之防護與反制措施，以及決策層級，並制定明確、直接、有效的常設性軍事行動規範，達成快速反制機制，建構安全、可靠的隱形國土安全防護網路。

（收件：111年1月10日，接受：111年2月25日）

參考文獻

中文部分

專書

魏靜芬，2005。《戰爭法學》。臺北市：社團臺灣海洋事務策進會。

專書論文

林勤富、吳建輝、陳怡靜、楊蕙亘，2020。《國防部109年度委託研究計畫報告（案號：HC09109P099）—國軍對於網路戰反制作為之法律建置暨運用》。臺北市：國防部。

期刊論文

林穎佑，2017/10。〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第15卷第10期，頁102-128。

孫鈺婷，2020/1。〈國際資安防護政策趨勢探討—關於「主動式網路防禦」〉，《科技法律透析》，第32卷第1期，頁37-46。

黃柏欽，2019/6。〈戰爭新型態—「混合戰」衝擊與因應作為〉，《國防雜誌》，第34卷第2期，頁45-68。

董慧明，2016/3。〈大陸「軍民融合」發展戰略之現況與問題評析〉，《展望與探索》，第14卷第3期，頁31-38。

歐廣南，2018/6。〈間諜行為法制規範之現代意義探討（上）〉，《軍法專刊》，第64卷第3期，頁61-88。

魏靜芬，2019/2。〈網路攻擊、網路間諜及網路監控之國際法評價〉，《軍法專刊》，第65卷第1期，頁18-31。

蘇紫雲，2021/8。〈國家安全與國防戰略思維的競合與定位〉，《國防情勢特刊—國安、國防戰略思維面面觀》，第11期，頁1-10。

外文部分

專書

Clasuewitz, Carl von, trans. Howard, Michael Eliot and Paret, Peter, *On War*, 1989. Princeton: Princeton University Press.

Fowler, Christina, Goffin, Mike, Bill, Hill, 2020. *An Introduction to MITRE Shield*. Virginia: MITRE.

Hardt, Michael and Negri, Antonio, 2004. *Multitude: War and Democracy in the Age of Empire*. New York: The Penguin Press.

J., Franklin, V., Paxson, A., Perrig, S., Savage 2007. *An Inquiry into the Nature and Cause the Wealth of Internet Miscreants*. New York: ACM.

Radin, Andrew, 2017. *Hybrid Warfare in the Baltics-Threats and Potential Response*. Santa Monica: Rand Corporation.

Sanger, David E., 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Victoria Australia: Scirbe Publication.

Schmitt, Michael N., & Vihul, Liis, 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University.

Walzer, Michael, 2004. *Arguing about War*. New Haven: Yale University Press.

Ziolkowski, Katharina, 2013. *Peacetime Regime*

for State Activities in Cyberspace. Tallinn: NATO CCD COE.

期刊論文

Beck, Neil J., 2011. "Espionage and the Law of War," *American Intelligence Journal*, Vol. 29, No. 1, pp. 126-136.

Captain Shakarian, Paulo, 2011/11-12. "The 2008 Russian Cyber Campaign Against Georgia," *Military Review*, pp. 63-68.

Csonka, Peter, 2006., "The Council of Europe's Convention on Cyber-Crime and other European Initiatives," *International Review of Penal Law*, Vol. 77, pp. 473-501.

Haar, Rohini J., Iacopino, Vincent, Ranadive, Nikhil, 2017. "Death, injury and disability from kinetic impact projectiles in crowd-control settings: a systematic review," *Open Access*, No. 7, pp. 1-9.

Kastenberg, Joshua, 2009. "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law," *Air Force Law Review*, No. 64, pp. 43-64.

Kennedy, David, 1987. "The Sources of International Law," *American University International Law Review*, Vol. 2, No. 1, 1987, pp. 1-96.

Koplow, David A., 2014. "A Nuclear Kellogg-Briand Pact: Proposing a Treaty for the Renunciation of Nuclear Wars as an Instrument of National Policy," *Syracuse J. Int'l L. & Com*., Vol. 42, No. 1, pp. 124-191.

Petreski, Milorad, 2015. "The International Public Law and the Use of Force by the States," *Journal of Liberty and International Affairs*, Vol. 1, No. 2, pp. 1-9.

官方文件

Council of Europe (ETS-No. 185), 2001. *Convention on Cybercrime*.

ICJ Reports(No. 96/23), 1996. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of July 8*.

International Court of Justice, 1986/6/27. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).

The White House, 1998. *A National Strategy for A New Century*. Washington DC: The White House.

U.S. Department of Defense, 2018. *Summary: Cyber Strategy 2018*. Washington: Department of Defense.

UN General Assembly, 1974/12/14. *Definition of Aggression*, A/RES/3314 (XXIX).

UN General Assembly, 1970/10/24. *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, A/RES/2625 (XXV).

網際網路

Christensen, W. Brent, 2019/11/6. "Remarks by AIT Director W. Brent Christensen at The Opening Session of the Taiwan-led part of the 2019 Cyber Offensive and Defensive Exercises," *American Institute in Taiwan*, <https://www.ait.

org.tw/remarks-by-ait-director-w-brent-christensen-at-the-opening-session-of-the-taiwan-led-part-of-the-2019-cyber-offensive-and-defensive-exercises/>.

Cybersecurity & Infrastructure Security Agency, 2021/7/8. "Alert (AA21131A)-DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware," *National Cyber Awareness System*, <https://us-cert.cisa.gov/ncas/alerts /aa21-131a>.

MITRE ATT & CK, *Resource Development*, <https://attack.mitre.org/>.

Seldin, Jeff, 2019/6/20. "Trump Reportedly Approved Military Retaliation after Iran Shootdown of US Drone," *VOA News*, <https://www.voanews.com/a/middle-east_trump-reportedly-approved-military-retaliation-after-iran-shootdown-us-drone/6170398.html>.

Sharwood, Simon, 2021/7/28. "Biden warns 'real shooting war' will be sparked by severe cyber attack; Suggests incident 'of great consequence' in the real world could be a tipping point," *The Register*, <https://www.theregister.com/2021/07/28/biden_cyber_attack_real_war_prediction/>.