10.6326/NDJ.202303_38(1).0004

網路作戰的認知與迷思：從網路地理、科技能力與法律規範反思網路的攻擊與防禦

Conceptions and Misconceptions of Cyber Operation: Reflections on Cyber-attacks and Cyber-defense based on the Investigations of Cyberspace Geography, ICT Capabilities, and Legal Norms

姚宏旻 (Hon-Min Yau)

國防大學國際與國防事務學院國際安全研究所所長

摘　　要

後疫情時代對於資訊科技的大量運用與依賴，幸尚未產生傳統安全研究文獻所擔憂的網路浩劫；亦即當人類社會過度仰賴資訊科技將使人類社會暴露於不可控制的數位末日。特別是2022年2月起的俄烏戰爭顯示，即便各國所畏懼的俄羅斯網路作戰能力在戰前或許活躍，但在開戰後卻鮮有戰果。然當前國內網路安全論述普遍推斷，由於「攻擊是最好的防禦」，故我國須透過網路攻勢能量的強化來占據未來網路戰場主導地位。而過去這樣的主流論述，常忽略任何的戰略設想須同時檢視「地理」及「科技」等因素，瞭解這些因素如何影響所關切作戰領域在攻擊與防禦間之發展計量。本研究希望能縮小當前國內學界主流論述與軍事作戰實務在本項安全議題上的文獻缺口，並結合近年多次國際事件之實證性與經驗性證據論述，以精進當前我國戰略與安全研究社群對網路安全之認知。

關鍵詞：動能性網路攻擊、網路安全、國防安全、網路空間

Abstract

In the post-COVID-19 era, the prevalent utilization of ICTs offers an excellent contrast against the pessimistic prophecy of past literature, which is that over-dependence on ICTs makes human society extremely vulnerable to digital catastrophe. While the Russia-Ukraine War starting in 2022 also indicated that the Russian cyber force may be very active prior to the conflict, it has accomplished no significant achievement since the conflict has escalated. Given that Taiwan faces a unique geopolitical threat from China, it has often been argued by scholars that Taiwan shall enhance its offensive cyber capability to defend itself and improve its cybersecurity. However, this kind of mainstream view is based on the same assumption of the

military operation in the physical domains that "offense is the best defense." Such an argument ignores that the advance in "technology" and the change in "operational environment" are two essential factors to include when considering the preference between offense and defense. This research plans to reduce the knowledge gap between cybersecurity and the above factors, to improve the understanding of cybersecurity among the epistemic community of security and strategic scholars in order to offer policy-relevant recommendations for the future improvement of Taiwan's cybersecurity policy.

Keywords: Kinetic Cyberattack, Cybersecurity, National Defense Policy, Cyberspace

壹、前　　言

21世紀初期見證網路衝突興起的時代。首先，2007年愛沙尼亞(Estonia)因計畫搬遷冷戰遺緒的紅軍雕像而遭到據信為俄羅斯資助的網路攻擊。[1] 其次，當2008年俄羅斯以軍事行動介入位於高加索地區喬治亞(Georgia)共和國境內親俄分離運動時，喬治亞境內各公私網站也突遭巨量式分散阻塞攻擊(Distributed Denial of Service attack, DDoS)並經癱瘓其功能。[2] 而2010年，伊朗更於其納坦茲(Natanz)機密核武設施內，發現遭他國植入被稱為史上第一種等同飛彈「射後不理」(fire and forget)主動追蹤能力的網路武器—震網(Stuxnet)蠕蟲。[3] 2017年國際媒體更大幅報導，美國利用先進電腦病毒執行一項稱為「主動抑制發射」(Left-of-launch)的作戰行動，破壞北韓導彈發展工作。[4] 顯然的，就軍事作戰角度而言，網路安全問題已不單單是早期文獻所關切的政治操弄亦或輿論宣傳等軟殺(soft-kill)作戰形式，而在當前傳統的國家行為體(state actor)透過非傳統的網路手段引發「動能性攻擊」(kinetic attacks)的可能遽增時，網路攻擊的硬殺(hard-kill)威脅已被國家安全需求賦予新的意涵，並成為未來國家生存與軍事安全所必須考量的因素之一。

因應這樣的全球安全趨勢，以及與日俱增產生「實體破壞效果」的新興數位威脅，我國也企希藉由軍事力量的強化來防衛數位國土，並於2017年成立資通電軍指揮部。[5] 根據資通電軍指揮官馬英漢中將於2018年10月回顧成立一周年後的報告指出，我國當前遭受的網路攻擊有80%以上源自中國大陸，若單以2017年為例，則國防部每一個月便遭受到61,208次以上網路攻擊，而自2018年1至10月間，每個月遭到對岸攻擊頻率則升高至

1 Otto Kreisher, "Risk to One Is Risk to All," *Sea Power* 50, no. 12, 2007, pp. 28-30.

2 Steven Bucci, P, "A most dangerous link," *US Naval Institute Proceedings*, 135, no. 10, 2009, pp. 38-42.

3 Lukas Milevski, "Stuxnet and Strategy: A Space Operation in Cyberspace," *Joint Forces Quarterly*, 63, no. 4, 2011, pp. 64-69.

4 William J. Broad and David E Sanger, "U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight," *New York Times*, 14 March 2017.

5 MOFA, "*Ministry of National Defense launches new cybersecurity command*," Taiwan Today, <https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=117794>（檢索日期：2022年9月15日）

75,368次，顯然中國大陸對我網路威脅問題嚴重。[6] 換言之，就國防角度而言，我國必須持續強化網路軍事能量，方能捍衛數位國土。有鑒於此，本文的重要性在於回應這樣的威脅發展，對於網路安全的政策發展提出具體建言。其主要目的是希望引用後疫情時代各項經驗性發展，對網路軍事作戰執行與時俱進的分析與比較；主要意義在透過對過去文獻在網路作戰軍事價值上的各項迷思進行檢驗，進而對各項網路攻擊普遍認知的討論作出貢獻。本研究之學理價值，在於透過系統性的分析與討論，擴大吾人對網路攻擊與防禦的給定(given)知識執行反思。據此，以下行文論述邏輯說明如次：首先對網路攻擊的一般設想與當前經驗性觀察之反差執行說明，以凸顯本文的核心問題意識；其次，就地理與科技兩因素如何在戰略理論管理分析，對軍事作戰產生影響執行重要之因果關聯陳述；其三，依前述學理立基，進一步就網路地理與資訊科技如何影響網路作戰行動作出細部檢視；其四，在掌握地理與科技對網路行動之影響後，本研究進一步對文獻上普遍歸結之三大網路攻擊認知執行檢驗；其五，在釐清網路攻擊具體限制後，本文進一步回顧我國現行法律規範與網路攻擊在理論與政策實踐間之反差；其六，全文最後對我國網路安全政策未來精進空間提出建言，最終進而歸結主要分析結論。

貳、攻擊勝於防禦？

承前言所述，資通電軍指揮部過去的各項量化數據描述雖容易吸引媒體標題的青睞，並凸顯網路威脅對我國與日俱增的嚴峻挑戰，但對於我國應如何反制以及可採用何種策略強化，並對這類高強度攻擊運作方式與可能的具體應對作為等面向的實質性討論卻非常少。尤其是此處資通電軍指稱的「網路攻擊」統計數據包羅萬象，小從簡單的網路傳輸Ping指令試探，大到複雜的網路滲透，並與國際法理慣常認定的「使用軍事武力」(use of the force)內涵具有相當出入。故當國防部門籠統的將任何與網路入侵相關的行為納入統計公式，這樣的估算便容易模糊在所稱數據中的入侵攻擊技術細節，並含糊的將不精準的簡易漏洞窺探，逕自等同為複雜的惡意軟體攻擊。[7] 也因此若我國執行這種過度化約的統計計量，並囫圇吞棗的理解網路攻擊可能效果，便將潛移默化的認同美國學者約翰．阿奎拉(John Arquilla)及大衛．朗費爾特(David Ronfeldt)等學者論點，[8] 亦或自然而然接納如中國大陸學者王湘穗與喬良所稱，[9] 網路攻擊可以小博大、易攻難守，而我國未來網路安全政策規劃方向，亦將循此不加思索的脈絡反映「攻擊仍是最好的防禦」的戰略判斷。[10] 故本研究的問題意識在於，即便當前主流論述不斷強調網路世界是

6 Ying-han Ma, "Military Cyber Threats and Responses," *Defense Security Brief* 7, no. 2, 2018, p. 6.

7 Peter Warren Singer and Allen Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know?* (Oxford, UK: Oxford University Press, 2014), p. 68.

8 John Arquilla and D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997).

9 王湘穗、喬良，《超限戰》（北京：解放軍文藝出版社，1999）。

攻擊優於防禦的天然數位環境，然若循此論述脈絡，那當代社會自20世紀末高度仰賴資訊科技的水電金融等關鍵基礎服務，似乎早難以招架這種廉價、易於發起、且具全球性效力的攻擊形式，並依前述學理推斷而多次深陷不可挽回之巨大數位劫難，進而使人類社會活動返璞歸真。然而，當前人類社會所幸仍未遭遇如此的數位浩劫，並持續仰賴這些看似脆弱且難以防護之資訊設施提供關鍵服務，顯然網路攻擊的理論預測與政策實踐間，似乎在攻擊與防禦間仍存在未經深究的探討空間，並亟待學者進一步思辨與解釋當前的矛盾與反差。

尤當新冠肺炎(COVID-19)期間，公、私部門愈加仰賴資訊科技從事資訊交換以降低社交接觸所產生疾病傳播的可能，故這樣網路科技增加運用的趨勢，似乎更應提供駭客相較於以往充足的攻擊機會與條件，並促成其摧毀過去人類活動高度仰賴之資訊關鍵基礎設施(Critical Information Infrastructure)；在後疫情時代，儘管諸如SolarWinds及殖民管線公司(Colonial Pipeline)等資安事件仍層出不窮，[11] 但目前人類社會仍能持續仰賴過去文獻所認為，這些看似脆弱的資訊系統從事關鍵服務，並未因網路攻擊的數位浩劫而回歸原始時代。同時，即便2022年俄烏戰爭軍事交火發生前，科技巨擘微軟早於2022年1月便發現俄羅斯大量預置WhisperGate等資料刪除惡意軟體對烏國發動網路攻擊，意圖摧毀其資訊服務；[12] 然自2022年2月24日戰事開打後卻仍鮮見俄羅斯透過網路攻擊達成任何的巨大戰果；[13] 這使得西方軍事觀察家質疑俄羅斯網路攻擊能量是否被誇大，而英國「政府通訊總部」(GCHQ)總監佛萊明(Jeremy Fleming)更指陳俄羅斯在網路戰場上是徹底失敗。[14] 最後，在2022年8月初美國眾議院議長裴洛西(Nancy Pelosi)訪臺後，中共除於臺海周邊海域執行軍演，更透過網路對我持續攻擊，然所幸大多數攻擊形式仍屬於網頁置換與虛假封包流量製造，國

10 戴政龍，〈中共「網軍」發展與網路攻防：兼論我國資通安全之政策規劃〉，《戰略與評估》，第4卷第4期，頁97-120。

11 Brad Heath, "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president," *Reuters*, 15 February 2021, <https://www.reuters.com/business/media-telecom/solarwinds-hack-was-largest-most-sophisticated-attack-ever-microsoft-president-2021-02-16/>（檢索日期：2022年9月15日）; David Uberti and Catherine Stupp, "Colonial Pipeline Hack Sparks Questions About Oversight," *Wall Street Journal*, 10 May 2021, <https://www.wsj.com/articles/colonial-pipeline-hack-sparks-questions-about-lax-cyber-oversight-11620689340>（檢索日期：2022年9月15日）

12 Microsoft, "Destructive malware targeting Ukrainian organizations," *Microsoft*, <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>（檢索日期：2022年9月15日）

13 Economist, "*Cyber-attacks on Ukraine are conspicuous by their absence*," Economist, 1 March 2022, <https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence>（檢索日期：2022年9月15日）

14 Mehul Srivastava, "*Prospect of Russian cyber war may have been 'overhyped', says UK spy chief*," Financial Times, 10 May 2022, <https://www.ft.com/content/d5657df5-a962-4acf-b0bd-b892c6b15361>（檢索日期：2022年9月15日）

際媒體指陳這種中共網攻抗議程度較多、威脅程度較少(Theater, Rather Than Threat)，並仍未有證據支持過去攻擊勝於防禦的論述。[15] 從前述案例觀察顯示，究竟是由於當代科技的進步使得網路防禦愈趨周延，故大規模毀滅之網路浩劫遭到有效抑制？亦或過去文獻論述過度誇大網路威脅，以致世人低估這種高複雜度網路攻擊的難度？無論如何，當前的經驗性觀察(Empirical observation)似乎提供直接的反駁證據，並為過去的主流觀點提供一強而有力的否證(Falsify)；[16] 或許網路空間並非可簡單的歸結為「攻擊勝於防禦」[17]、亦或是一個攻勢主宰(offense-dominated)的數位空間。[18]

參、網路地理、科技、法律與政策

有鑒於此，吾人對於網路攻擊的戰略認知與能力掌握，顯然仍有精進空間，網路攻擊似乎並非如傳統安全研究文獻論述與設想般的容易達成。也因此本研究目的在於藉由詳加比較網路攻擊與傳統軍事作戰的異同，企希精進我國網路安全的戰略研究並進而破除不必要的刻板迷思；最終希望透過對網路作戰行為的深入思辨，降低以下兩種層次的負面影響。

首先，就政策性思辨而言，過去這樣不清晰的統計數據易招致「威脅膨脹」的疑慮，[19] 致使我國政府施政資源錯置並過度集中於攻勢能量的建立。到目前為止透過網路攻擊行動，在世界各國所造成的官方傷亡人數仍然為「零」，因此部分歐美學者便直言稱道：「這世界沒有網路戰爭」。[20] 少部分論述甚至主張網路攻擊是政府官員、媒體及學者的「言語行動」(Speech Act)，並透過話語建構(discursive construction)製造出「恐懼」的概念影響國家決策。[21]

其次，就學理性思辨而言，若過去文獻上對網路攻擊的運用發想是延續傳統作戰領域的經驗假借，並未對網路作戰空間本體(ontological)層次作細部考究，這種想當然耳的設想是否可能誤導我國整體網路防禦的發展思維？特別是在國際關係學門上，「地理」及「科技」兩因素，一直是歷史上影響不同戰略理論發展的主要動因。也因此過去依附不同「地理」環境前提下，便產生「陸戰」、「海戰」及「空戰」等不同戰略理論體系；而依附在「科技」這獨立變數下，便產生科技決定論或「軍事事務革新」

15 Sarah Wu and Eduardo Baptista, "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit," *Reuters*, 5 August 2022, <https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/>（檢索日期：2022年9月15日）

16 黃光國，《社會科學的理路（第三版）》（臺北：心理出版社，2013年），頁137。

17 同註10，頁118。

18 John Arquilla, *The advent of netwar* (Santa Monica, CA: RAND Corporation, 1996), p. 94.

19 Hon-min Yau, "*Framing Cyber Security in Taiwan: A Perspective of Discursive Knowledge Production," Korean journal of defense analysis* 32, no. 3, 2020, p. 464.

20 Thomas Rid, *Cyber War Will Not Take Place* (Oxford, UK: Oxford University Press, 2013). p. 1

21 如學者鄧恩(Myriam Dunn Cavelty)依據英國分析語言學家奧斯丁(John Austin)的語言行動理論，論證美國網路威脅的根源來自語言。請見M. D. Cavelty, "Cyber-terror-looming threat or phantom menace? The framing of the US cyber-threat debate," *Journal of Information Technology & Politics* 4, no. 1, 2008, pp. 19-36.

(Revolution of Military Affair)等思維脈絡。假如網路作戰不同於陸戰而沒有地障限制，不若海戰而言無交通線考量，更異於空戰而言沒有航程限制，因此值得深思的是，這些迥異於過去戰略理論所依賴的陸、海、空戰之「地理」設想與「科技」因素，是否造成網路空間環境需發展新的戰略脈絡？同時更應進一步檢視這些因素對於各國網路戰略設想的影響，是否因而與過去傳統作戰場域所能發揮的效果不同？並進一步檢視這些限制如何衝擊「法律」進而影響各國政策。

基此，現行學界對於網路安全的討論，多強調在技術性之細節描述亦或軍事性之可能推測，但並未回頭檢視這些網路作戰立論所依據的地理與科技變因前提，並檢驗這些假設基礎是否穩固並須適度修正？進而自然的認定網路世界的攻擊與防禦應與實體空間攻防模式類同。故吾人若能體認網路空間的「地理」因素可能與實體領域作戰不同，則我國便可跳脫過去主流視野，而據以思索可行之精進策略。同時，若資訊「科技」對網路攻守所產生的影響性不同，則我國便須據以精進過去網路安全戰略姿態設想。這樣的理解呼應戰略研究學者科林．格雷(Colin Gray)就網路安全研究的殷切提醒，他認為現行著重網路世界之技術類文獻雖非常豐富，但運用或發展戰略理論來檢視該領域作戰運用之研究卻非常匱乏。[22]

肆、網路攻擊的「地理」與「科技」限制

21世紀網路世界充斥著低於戰爭門檻的假消息、阻斷攻擊與資料竊取等網路攻擊之手法，但本文所設定探討的網路攻擊範疇則僅聚焦在能造成實體破壞的動能性攻擊，而當前學界上則普遍將這類網路攻擊逕自比擬為等同實際空間軍事作戰行動的研究形式，文獻上亦泛稱為網路戰爭(Cyber War)。[23] 主張可以針對敵國特定資訊系統執行精確打擊與破壞，也因此即便許多已知網路作為多發生於軍事作戰前，但前述這些文獻卻仍未能重新正視以傳統軍事作戰思維全面評量網路戰成果是否恰當。而另一方面，由於網路空間具有不分前、後方與平、戰時的作戰「地理」特性，故過去這樣的論述也鼓勵各國大量運用低於常規衝突強度的作戰形式，在無論是結合灰色地帶(gray zone)亦或混合戰(hybrid warfare)手法運用上，似乎都直接或間接的造成推波助瀾效應並促成各國肆無忌憚的運用。正如同過去伊朗核武設施的震網

22 原文為："... the technical and even tactical literature on cyber is as abundant as the strategic theoretical treatment is both thin and poor." Colin S Gray, *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling* (Pennsylvania, U.S.: Strategic Studies Institute, US Army War College, 2013) iii.

23 同註10；呂兆祥，〈共軍網路作戰對我資電作戰之影響〉，《國防雜誌》，第30卷第6期，2015年11月，頁1-27；許秀影、劉豐豪、張瑞勇，《前瞻國軍對次世代網路之應用》（桃園：國防大學，2010）；Richard A Clarke and Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2011); Paul Cornish et al., *On Cyber Warfare* (London: Chatham House, 2010); Franklin D Kramer, Stuart H Starr, and Larry K Wentz, *Cyberpower and national security* (Washington, DC, US: Potomac Books, Inc., 2009); Fred Schreier, *On cyberwarfare*, DCAF Horizon 2015 Working Paper Series (Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2012).

病毒案例中所呈現的，[24] 網路病毒具有能創造動能性(kinetic)能量並可採精準打擊般實體破壞的能力，故如果部署得宜將可達成作戰目的而不必承擔政治責任。[25] 也因此，如同過去精準打擊武器為軍事研究所帶來的軍事事務革新研究般，國內軍事專家普遍認為，網路武器勢必成為軍事作戰的新元素，並就未來作戰形式帶來強烈變革。

然而，這樣過於簡化的設想，並將網路攻擊的動能性潛能與傳統軍事作戰運用產生等同聯結，若未能細部檢驗可能的執行障礙，便可能產生誇大網路攻擊作戰效果，亦或產生美化其軍事效用的疏失。為謹慎應對這種未經熟慮的戰略風險，以下僅從網路作戰的執行角度，分別從軍事作戰所需的兩種「科技」支援能力，包含情監偵(Intelligence/Surveillance/Reconnaissance, ISR)及戰果評估(Battle Damage Assessment, BDA)等方面，瞭解「地理」如何影響這些能力的執行進行檢驗。

一、網路作戰地理的情監偵限制

傳統軍事作戰須要良好的情監偵能力支援，俾確保作戰前的戰場經營與戰場情報蒐集(Intelligence Preparation of the Battlefield)，並支援作戰期間的即時目標捕獲與識別，故情監偵需求能力為執行資訊化作戰不可或缺的關鍵能力。然而1991年波灣戰爭經驗顯示，即便美軍透過動員眾多先進的情監偵資產，卻仍難以完整掌握伊拉克機動部署飛毛腿飛彈車動向與可能來襲位置；[26] 即便科索沃戰爭期間北約部署先進的情監偵載台於戰鬥地境，美國蘭德公司於軍事行動後的詳盡評估報告中，卻仍給予盟軍情監偵能力「三流以上」(C-plus)等級評比。[27] 前述這兩個案例顯示，各國軍事行動的執行立足於良好的目標捕獲能力為前提，而維持有效的情監偵能力，一直是各國在確保軍事作戰行動成功的必要條件。

但對網路作戰而言，網路世界除撲朔迷離外，亦沒有高山海洋、沒有叢林平原，由於網路地理迥異於陸、海、空的環境特性，便使得網路情監偵能力不足的缺點特別顯著。如同在實體作戰領域的衝突般，成功的攻擊在於對敵裝備性能及部署的掌握；故網路攻擊也須基於對敵資訊系統的瞭解，方能判斷可滲透的系統漏洞，這包含須掌握敵所使用之軟硬體設備型號、網路拓撲(network topology)與參數設定等構型資訊能力，甚至是這些電腦裝備所直接連接控制的系統。能否獲得這些情資，為網路攻擊（成功滲透）與否的有效關鍵前提，但由於網路世界低戰場能見度的數位地理特性，使得這樣的需求如同緣木求魚不易達成，主要限制如下：首先，網路攻擊的成功須立基於掌握敵方資

24 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, US: Crow Publishing Group, 2014).

25 Peter Dombrowski and Chris C Demchak, "Cyber war, cybered conflict, and the maritime domain," *Naval War College Review* 67, no. 2, 2014, pp. 70-96.

26 Thomas A Keaney, *Gulf War air power survey*, vol. 4 (Washington DC: Office of the Secretary of the Air Force, 1993), p. 340.

27 Benjamin S Lambeth, *NATO's air war for Kosovo: A strategic and operational assessment* (California: Rand Corporation, 2001), p. 161.

訊系統前述軟、硬體構型(configuration)資訊，包含作業系統版本、安裝軟體及所控制的相關裝置，方能採取對症下藥的方式發起網路攻擊，並利用相對應的軟、硬體設計缺陷或漏洞達成入侵。其次，就網路攻擊成功與否的前提，則須仰賴能否植入與其軟硬體平臺相容的惡意程式，並確保軟體可以發揮預期效果；故在惡意程式開發期間，攻擊方亦須依所蒐集的敵系統情資，建置類似的軟、硬體構型環境，以協助電腦病毒的開發(software development)及測評(Operational Test & Evaluation)。即便諸如網路通訊標準協定(TCP/IP)形式的通訊協定強調透通設計且層層相連，但有鑑於機密資訊系統通常實體隔離與外界隔絕，故這將使得前述軟、硬體的構型資料完全與外界阻絕，故將造成網路內使用前述通訊協定的軟、硬體構型資料完全與外界阻絕，並無法透過公共網路獲得。同時，也由於現今資訊系統無論是漏洞修補與軟體版本更新多採即時線上即時派發，故當代的軟硬體構型資料也愈加具有時限性的特徵(time sensitive)，即便暫時獲得情資也可能因攻擊對象後續採取軟硬體更新而成為無效情資。[28] 最後，最大的限制或許在於眾多軍民設施採用互通的網路骨幹傳輸，然而由於資訊設備在網路上並無地形、地物或地貌可比對，皆僅僅以網際網路位址(IP address)顯示（本文中「網際網路位址」以「電腦位址」簡稱），故多大程度上網路的情監偵作業能避免將民間設施誤判為軍事設施。前述網路地理對網路作戰的特殊限制，使得透過網路執行情監偵作業的可行性雖不致無法達成，但相較於傳統實體空間的情監偵活動而言，卻極富挑戰。因此，對網路空間的作戰行動而言，不可靠的網路情監偵戰場資訊，不僅代表著一次無效的網路攻擊，同時由於無法獲得較清晰的網路戰場能見度，這亦意味指揮官在下達攻擊決心前，可能要思考後續若因無法掌握遭入侵的網路系統所牽連之控制設備數量，以及當這些裝備失效後之具體影響性，而須承擔不可預估與控制之連帶政治責任。

二、網路作戰與戰果評估需求

有效且即時的戰果評估(Battle Damage Assessment)，是支持指揮官下達後續作戰決心，並達成火力集中或節約選擇的先決條件，也是能否有效癱瘓目標的關鍵因素之一。以空中轟炸行動為例，任務指揮官在第一波轟炸執行完畢，便須仰賴後續戰果評估報告的實施，來辨識前次攻擊的效果與範圍，並作為規劃次波攻擊任務需求的依據。而過去美軍在波灣戰爭的行動後分析(after action review)顯示，即便能獲得傳統偵照行動提供之影像情資，但在後續判斷對敵掩體或強化工事的摧毀效果上仍有其相當限制；[29] 而2001年阿富汗及2003年伊拉克戰爭後，美國審計總署(General Accounting Office)於事後的審計報告也指出，戰事期間無法立即且有效的執行戰果評估，故造成美軍火力效果無法發揮，也嚴重延遲整體戰事的推展。[30] 顯然的，任何的軍事行動中，戰果評估與當代軍事行動之有效與否，具有強烈之

28 Dudu Mimran Blog, "The Emergence of Polymorphic Cyber Defense," <https://www.dudumimran.com/2015/02/the-emergence-of-polymorphic-cyber-defense.html>（檢索日期：2022年9月15日）

29 同註26，p. 30-37.

因果關聯。

而對網路空間作戰環境而言，戰果評估自然也是每一場網路作戰至為重要的關鍵因素，但由於網路科技特性造成戰場能見度低，故實難以單靠網路空間來達成。例如以色列在2007年轟炸敘利亞核子反應的「果園行動」(Operation Orchard)中，[31]「據傳」就是由以色列先以電腦病毒破壞防護庫巴爾(Al-Kubar)核武設施的周邊防空飛彈系統，後方能成功執行空襲行動。[32] 在該案例，若是以傳統武器形式壓制敵方防空任務(Suppression of Enemy Air Defenses)，指揮官則較易掌握，主要因為包含所採用彈藥射程、威力以及預計彈著時間具有明確性，可供任務部隊指揮官執行規劃及協調。但前述這種資訊，對網路武器而言卻被網路空間濃重的戰場迷霧(fog of war)所包圍。由於當代資訊系統往往具有嚴密的複式配置及緊急復原設計，任何對於資訊系統的網路作戰成果可能是暫態的，如果缺乏立即的戰果評估能力，作戰指揮官可能會因此喪失最佳戰鬥時機，也因此假如以色列指揮官若真的如同媒體所轉述的預先執行網路病毒攻擊，則必須能在就網路攻擊發揮當時作精確戰果評估，諸如回答何時電腦病毒攻擊敘利亞防空系統？以及何時能成功癱瘓敵系統等戰術層面操作問題，方能協調各部隊行動、執行聯合空襲。由於迄今尚未有官方釋出資料說明「果園行動」運用所謂網路攻擊的具體細節，故吾人仍無法確認以色列當時是否真的單單透過網路攻擊癱瘓敘軍防空系統；不過由於慣常的軍事作業程序，當一國遭到攻擊時必定亦立即切斷或管制對外之民間通訊網路，故外軍難以透過網路空間獲得前述情資，也因此在本案例中以色列勢必透過網路以外的偵搜方式，方能掌握前述軍機資訊並執行所需之戰果評估。

伍、網路攻擊的優勢檢驗

從上述分析顯示，網路作戰在許多方面並無法等同實體空間的傳統作戰行為，而不論是戰場「地理」與「科技」能力而言，都與實體空間的運作形式有所落差。然現行許多網路攻擊的優勢論述，卻都是立基於過去未經仔細檢驗的假設基礎，並在未瞭解網路地理與科技之限制條件下而逕自歸結「網路攻擊優於網路防禦」的主流定見，[33] 並進而形成以下三種既定形象的標籤化論述，亦即包含「網路攻擊者享有匿名優勢」、「網路攻擊是廉價且有效的行為」以及「網路世界易攻難守，故網路攻擊優於網路防禦」。[34] 換言之，當網路空間之「地理」與「科技」因素相較於陸、海、空等戰略理論假定與發揮效果確實有所差異時，這便迫使本研究必

30 NP Curtin, "*Military operations: recent campaigns benefited from improved communications and technology, but barriers to continued progress remain*," in GAO Reports, 04-547 (2004).

31 同註20，p. 42.

32 Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012), p. 7.

33 John Arquilla; US DoD, *Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011* (Washington, DC, US: Department of Defense, 2011); 同註10。

34 同註23。

須對過去前述三項戰略層次的假定執行進一步的檢視。

一、網路攻擊者是否享有匿名優勢

首先，網路攻擊者是否真的享有匿名優勢？過去文獻將網路活動難以追本溯源(attribution)的特性歸咎於網路通訊標準協定(TCP/IP)開放與透通的設計，[35] 由於早期網路架構的創始人員藉由路由通訊設計以達成無節點的高存活度，故在此思維主導下強調通訊透通(connectivity)而忽略網路活動的溯源紀錄。也因此紐約時報漫畫專欄作家彼得．施泰納(Peter Steiner），在1993年便創造出「在網際網路上，沒人知道你是一隻狗」(On the Internet, nobody knows you're a dog）的貼切諷刺漫畫，[36] 並凸顯出網際網路能夠提供一種無須透露個人背景的通訊方式來發送或接受資訊。不過這樣的論述卻忽略隨著21世紀資訊科技的不斷演進，過去誕生於20世紀的網際網路匿名性特徵已遭到各項數位鑑識科技的逐漸侵蝕。[37] 以中國大陸政府對於其境內網路掌控強度為例，透過對於國土內骨幹網路電信商的掌握，便能有效追蹤境內用戶使用者活動歷程；[38] 明顯的例子便是過去我國人權活動人士李明哲，在被中共湖南地方法院作為起訴的詳盡數位證據，便包含大量透過境內資訊商所蒐集李明哲的數據足跡。[39] 而近年隨著人工智慧、大數據技術的演進，資訊界也發展出越來越多的軟體技術，並已能提供類似過去在警界鑑識理論中所採用的「工具痕」(Tool Marks)理論的技術。換言之當現行許多文獻擔憂中國大陸以「數位極權」技術輸出世界，除鞏固許多非民主政體並協助其人權迫害活動，但這些論點的主張同時也證明過去認為網路活動具有絕對匿名優勢論述的基礎，實際上是非常薄弱的。[40]

同時，正如在前段「網路攻擊的軍事作戰限制」分析指出，由於在網路空間上難於執行精確的戰場情監偵，故電腦網路上任何的控制系統對於攻擊方而言僅是一臺數據設備，換言之判斷該受入侵資產是否具有攻擊價值的專業基礎，則須仰賴攻擊者對目標系統本身所提供之各項內部特徵長時間的蒐集與分析，這反而提供科技鑑識有效分析立基。首先，由於全球網際網路路由分配的技術需求，故電腦位址是透過具地理性的分配管理，因此常能透過其電腦位址反推標定攻擊來源地，並能縮小範圍過濾來自國外的系

35 Kenneth Geers, "A brief introduction to cyber warfare," *Common Defense Quarterly*, no. Spring 2010, pp. 16-17.

36 Glenn Fleishman, "Cartoon Captures Spirit of the Internet," *New York Times*, 14 December 2000, <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html>（檢索日期：2022年9月15日）

37 C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools* (New York: Elsevier Science, 2011).

38 B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York, US: W. W. Norton, 2015).

39 岳陽市中級人民法院，〈彭宇華、李明哲顛覆國家政權案〉，《微博》，2011年9月17日，<https://www.weibo.com/3960688335/FlijUcKOA?from=page_1001063960688335_profile&wvr=6&mod=weibotime&type=comment#_rnd1508944658512>（檢索日期：2022年9月15日）

40 Sebastian Heilmann, "Leninism upgraded: Xi Jinping's authoritarian innovations," *China Economic Quarterly*, 20, no. 4, 2016, pp. 15-22; Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism: The Russian and Chinese models," in *Policy Brief, Democracy and Disorder Series* (Washington, DC: Brookings, 2019), pp. 1-22.

統拜訪者。其次，由於當代的科技技術亦已經具備許多主動式的數位分析工具，例如網路蜜罐(honeypot)誘捕系統便是過去常見用來蒐集攻擊者資訊及手法普遍工具。[41] 故透過網路蜜罐的嚴密部署，便能成功對敵偽冒諸如掌控電信、伺服器或重要關鍵基礎設施的資料採集與監視系統 (Supervisory Control and Data Acquisition, SCADA)，並進而在敵人入侵時捕獲其攻擊數據證據，一定程度瓦解攻擊者匿名優勢。事實上由於數位鑑識技術不斷進步，目前已經有許多案例顯示網路攻擊者的追本溯源是可能的。[42] 最有名案例發生在2018年底，當時俄羅斯人員對於位於荷蘭的國際禁止化學武器組織(Organization for the Prohibition of Chemical Weapons, OPCW)執行網路攻擊，荷蘭政府在向北約(NATO)通報的安全事件紀錄中，公布詳盡的影像、監視畫面、人員行蹤電子紀錄使得俄羅斯官方介入的行為無從否認。[43] 不過主動式誘捕裝置雖可能誤導網路攻擊者攻擊錯誤的目標，確保網路重要資訊裝置的安全性，並進而掌握攻擊者的網路攻擊方式與攻擊來源，但能否全面有效瓦解攻擊者匿名優勢仍有不同程度操作限制。且先進的網路駭客進行網路攻擊時，亦慣常利用各種網路連結形式，進入多國網路節點執行跳板以抹除其網路足跡，並製造網路斷點，製造溯源難度。也因此本文要特別強調的是，網路攻擊源課責的證據強度，通常無法立即與法院所需之客觀證據強度一致；由於網路攻擊事件的本質，通常是實體空間角力的延伸，故佐證強度自然會跟各國國內法律標準有所落差。[44] 換言之，沒有簡單的靈丹妙藥能確保我們準確的知道誰是來自網路空間的攻擊者，然而務實地透過由現代數位鑑識線索和當代先進網路監視技術所能支持的徵候，結合這些問題背後的國際局勢、攻擊動機與成本，我們便能作出有利陳述歸責與指控特定國家。

二、網路攻擊是否為廉價且有效的行為

其次，網路攻擊是否真的廉價且有效？在當今惡意軟體氾濫且資安攻擊報導層出不窮，似乎顯示出網路攻擊工具的普遍與廉價，然而若細部觀察這些攻擊行為可發現，低端的入侵行為充斥，但高端的攻擊仍是有限。也因此氾濫的網路低端資安事件凸顯出普羅大眾對於基本資訊安全警覺與訓練不足，但並不代表網路攻擊對於專業機構是一樣容易。事實上專業級資訊系統通常採實體隔離設計，[45] 無論在伺服器、資料及網路傳輸骨幹上都會有嚴密的系統設計，包含資料

41 Gordon W Romney et al., "IT security education is enhanced by analyzing Honeynet data" (paper presented at *the Information Technology Based Higher Education and Training*, 2005. ITHET 2005. 6th International Conference, 2005), pp. FJOIlO-F3D/l4.

42 US DoD, *The DoD Cyber Strategy* (Washington DC, US: Department of Defense, 2015), pp. 11-12.

43 Pippa Crerar, "Russia accused of cyber-attack on chemical weapons watchdog," *The Guardian*, 4 October 2018, <https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body>（檢索日期：2022年9月15日）

44 同註7。

45 Thomas Rid, "Cyber war-Think again," *Foreign Policy*, no. 192 (2012), <https://foreignpolicy.com/2012/02/27/think-again-cyberwar/>（檢索日期：2022年9月15日）

加密及複式配置，在系統運作上有人隨時監控，同時在受攻擊後又有緊急轉換及復原程序，確保工作持續運行。[46] 也因此當後疫情時代的我們仍能仰賴資訊系統所提供的銀行交易與商業活動持續不輟，並未遭致無法挽回災難而使人類活動回復紙本作業，便儼然為「網路攻擊是廉價且有效的行為」提出一具體反證。

為人所知的震網病毒事件中，網路攻擊之所以能成功入侵伊朗的核武設施，絕對不是如電影情節般單單透過駭客的鍵盤與滑鼠便能成功滲透。[47] 若能詳加檢視則該事件則發現，該惡意程式的發展者是預先獲得該設施資訊系統的型號與網路配置，方能發展與目標系統相匹配的惡意程式執行有效攻擊。然而，這些情資絕對不是單單透過網路執行的情監偵作業便能獲得，畢竟當伊朗政府採用實體隔離的網路設計，便能完全阻絕來自外部的網路情監偵活動。換言之，震網病毒在正式入侵到伊朗之資訊系統前，該意圖攻擊者在軟體發展階段便已透過長時間與大量金錢投注的人員情報蒐集作業、軟體發展、效能測試以確保能達到預期的作戰效能，而後續在部署階段時又必須結合社交工程或是魚叉式網路釣魚(Spear Phishing)將惡意程式部署到關鍵的維護工程師作業電腦。[48] 然而即便前述這些作業得以成功，攻擊者在惡意軟體成功部署後，仍必須考量到如何執行戰果評估以判斷是否已確實命中攻擊目標，並達成所望戰果。

然而，前文已說明在網路上的戰果評估實際上是不易執行的。依此特性，部分的觀察家早已指出由於網路空間特性，受害的一方卻通常無法即時就資安事件的影響幅度做出戰損評估；[49] 但本文亦希望額外強調的是，網路空間這種特性對希望發動攻擊的那一方也會產生同樣行動限制。過去傳統軍事行動的戰果評估，係仰賴監偵載臺的派遣運用來蒐集戰場近況，然而由於伊朗核武設施系採用實體隔離，故除非透過安排的內部情報人員，否則外部網路攻擊者無法透過網路執行戰果評估。也因此除非伊朗政府自行揭露該事件對其之影響幅度，否則真正的損害程度，恐怕只有伊朗人知道詳情。故這樣的網路戰場迷霧限制，對於網路作戰便產生至為重要的限制因素。簡言之，發展惡意程式雖然可能比不上發射衛星、建造航空母艦、投資新式戰機昂貴，不過本文要強調的是，高端惡意軟體的發展絕對不是一種「廉價」的投資；同時最大的網路限制因素乃是，假如網路作戰指揮官無法有效執行戰果評估，那又能如何判斷下一步行動，以及多大程度下能確保攻擊計畫「有效」？

三、網路世界是否易攻難守

最後，在網路世界裡是否真的「攻擊是最好的防禦」？許多希望就本項議題產出經

46 Sandra I. Erwin, "Defense CIO: Cybersecurity Improving but Innovation Lags," *National Defense*, 8 August 2016, pp. 1-20.

47 同註24。

48 Hon-min Yau, "A critical strategy for Taiwan's cybersecurity: a perspective from critical security studies," *Journal of Cyber Policy*, 2019, pp. 1-21.

49 Michal Thim, "Taiwan's Invisible Frontier: Cyberspace," *Thinking Taiwan Foundation*, <https://taiwan-in-perspective.com/2015/09/05/taiwans-invisible-frontier-cyberspace/>（檢索日期：2022年9月15日）

濟計量數據的嘗試，可能都是徒勞無功的努力，但震網病毒案例或許能對這一爭辯提供可能之標竿分析(Benchmarking)。軍事等級惡意軟體的開發就跟任何商業軟體開發般，所發展之軟體產品不可避免的會有程式缺陷甚至相容問題，故其系統發展就跟任何軍事系統一樣，必須經過最終作戰測評驗證，以確保實際作戰部署時能滿足所設計殺傷效果。因此即便震網病毒的開發者在獲得有關伊朗政府所採用執行控制的資訊設備與濃縮鈾萃取設備型號等情資後，若為確認屆時震網病毒可以真正有效，在開發期間也必然建置同樣的軟硬體環境執行驗證。[50] 這便需要組織包含情報人員、軟硬體工程師，甚至是核能專家的參與。同時，由於受害方之商用作業系統及軟體亦不時執行漏洞修補或軟體改版，故從震網病毒開發到完成交貨的前置時間(lead time)全程，開發者必須隨時掌握伊朗核武設施內軟硬體系統的各次升級時間與作業內容；主要是希望確保自身開發軟體其設定部署環境反映實際網路戰場現況，俾確保惡意軟體匹配敵作業環境，防止因有稍稍的一絲情資落差，造成過去耗費時間、金錢與精力開發的軟體武器在實際部署時的意外失效；其後，就算是完成惡意軟體部署，在該惡意軟體接收指令從潛伏模式觸發為甦醒模式但尚未完成攻擊指定設備前，伊朗工程人員可能在這段時間內就其設備執行新的更新並使軟硬體環境丕變，如此則剛開發完成的軍事等級惡意軟體，便可能因絲毫目標系統軟體的構型變動而逾貯存時限（shelf life，又譯為「保質期」或「有用期」）失效。這樣的限制反映在2021年以色列手機間諜軟體案例中，當時據報為以色列數位軍火商所發展出的Pegasus惡意軟體，具可輕易侵入過去蘋果手機引以為傲且宣稱防護力甚佳IOS作業系統能力，其後美國蘋果公司在正式新聞稿中指出，這種惡意軟體的網路攻擊形式非常複雜，其開發成本需要數百萬美元，而且通常「保質期」很短。[51] 故即便這種高端網路武器獲得成功部署後，但只要經過一次實際攻擊行動後，受害國必然會針對其病毒碼執行更新並嚴加防守，也因此耗費巨資研發的任何網路武器，在經過一次使用後便無法再次運用。

俄烏戰爭為前述三項認知迷思作出另一案例檢驗。首先，依據歐盟就俄烏衝突所作之網路攻擊統計資料顯示，俄羅斯自2014年入侵克里米亞後便對烏克蘭執行各項複雜之網路攻擊，然多數攻擊仍僅止於假消息、資料竊取、騷擾與服務阻斷。[52] 由於烏克蘭自2014年以來便處於俄羅斯惡意網路攻擊的複雜環境中，故經國際各資安機構長時間的數位足跡蒐整與分析，就算是自2017年所發現的先進勒索病毒NotPetya，資安單位仍能研判為俄羅斯發起之勒索病毒攻擊。[53] 其次，

50 Hon-min Yau, "Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation?," *Issues & Studies*, 56, no. 03, 2020, pp. 1-20.

51 Nicole Perlroth, "Apple Security Update Closes Spyware Flaw," *New York Times*, 14 September 2021, <https://www.nytimes.com/2021/09/13/technology/apple-software-update-spyware-nso-group.html>（檢索日期：2022年9月15日）

52 Jakub Przetacznik and Simona Tarpova, "*Russia's war on Ukraine: Timeline of cyber-attacks*," (Brussel, Belgium: European Parliamentary Research Service, 2022).

正如同過去在震網的案例中，若資訊系統管理人員可以履行更加良好的資安紀律與安全措施，諸如落實實體隔離與系統構型管理，相信相較開發這些惡意軟體所需資金來的低廉，並能以極小投資有效反制網路攻擊所可能帶來的效應；[54] 而在俄烏衝突經驗中，由於戰事已然開打，故俄羅斯使用精密且昂貴的電腦病毒攻擊烏國資訊設備，可能比不上使用傳統火砲對這些系統攻擊來的廉價、迅速及有效。最後，及至2022年2月24日全面入侵烏克蘭後，最明顯的進展僅有透過資料刪除軟體造成歐洲衛星通訊服務業者ViaSat暫時無法持續提供烏克蘭所需之衛星通訊，仍未有網路戰爭案例。[55] 顯見即便是不斷擴充網路攻擊能力的俄羅斯，在面臨較弱小之烏克蘭時，網路入侵仍必須先行找到侵入資安破口，由於烏國的資訊安全習慣養成，便能降低俄羅斯成功入侵破口數量。透過商用市場上輕易獲得且為數眾多並經多次驗證的資安產品，這些經市場多次驗證的成熟設備相較於政府專案經費開發的網路武器而言更為低廉，並確保烏國政府在戰時的永續運作。及至2022年9月15日，歐盟正式推出「數位韌性法案」(Cyber Resilience Act)，希望透過全面性提升數位產品的安全性標準，達成「彎而不折」(To Bend, not to break)的數位策略。[56] 顯然歐盟逐漸體認到藉由提升加密、存取管制、流量監控、網路管理、甚至是人員查核等韌性策略，資安風險絕對可以在合理的預算下達成一定的風險控管；正如同資安業界耳熟能詳的一句比喻：「沒有百分之百的資訊安全」，網路世界即使難守，但也絕非易攻。[57]

陸、網路作戰與法律規範之探討

綜上所述發現，網路作戰並不能單純設想為傳統作戰環境，在各項技術的運用上也有諸多限制。然而，即便未來網路作戰部隊能克服前述在網路空間的各項戰術與技術鴻溝，並進而獲得戰略優勢，但從法制層面而言，卻仍有下列問題：

一、國際法層面

目前規範網路行為戰爭與和平的國際規範雖持續發展中，但就聯合國憲章及傳統武裝衝突法如何適用在網路世界上之討論仍未有明確共識。

53 National Cyber Security Centre, "Russian military 'almost certainly' responsible for destructive 2017 cyber attack," *National Cyber Security Centre*, <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack>（檢索日期：2022年9月15日）

54 Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3, 2017, p. 105.

55 Viasat, "KA-SAT Network cyber attack overview," *Viasat*, <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>（檢索日期：2022年9月15日）

56 European Union, "Cyber Resilience Act," *European Union*, <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>（檢索日期：2022年11月19日）

57 Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan, "Information security management system standards: A comparative study of the big five," *International Journal of Electrical Computer Sciences IJECSIJENS* 11, no. 5, 2011, pp. 23-29; Charles Smythe, "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance," *Yale Journal of International Affairs*, 15, 2020, p. 98.

首先，最為人所熟知的便是愛沙尼亞於2007年遭受來自俄羅斯的網路攻擊，進而希望啟動華盛頓公約第5條款「集體防衛」(collective defense)機制，並要求各北約盟國介入與防禦當時針對愛沙尼亞的巨量網路攻擊威脅。雖然當時各國網路攻擊歸責須長時間蒐集與分析相關紀錄，並不容易在短時間內釐清俄羅斯官方是否為其行動背後主使者而未予支持，且網路攻擊並未造成人員死亡與裝備實際損失，故北約各國對於這種新興攻擊形式是否應納入「集體防衛」內涵更未建立共識。其後，北約於愛沙尼亞首都塔林成立北約合作網路防禦中心(Cooperative Cyber Defence Centre of Excellence, NATO CCDCOE)，其主要工作之一便是探索與發展未來網路與戰爭之規範行為。在北約資助下產出《塔林手冊1.0》(Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare)，當時遭到中國大陸及俄羅斯質疑僅是西方國家看待網路活動的片面共識，其當時參與討論的學者雖進一步就未解爭議邀請中俄專家一起參與研討，其修正版後稱為《塔林手冊2.0》，但國際上就其內容目前仍定調為學術著作，並未受世界各國正式認可。[58]

除此之外，過去聯合國負責探討網路空間戰爭與和平的「資訊和電信領域發展政府專家組」(The United Nations Group of Governmental Experts, UNGGE），在歷經2010年、2013年及2015年討論並發布三次小組共識報告(consensus report)後，自2019年討論也面臨來自中國大陸及俄羅斯發起的新挑戰。最主要爭議在於過去2015年會議中，雖然達成「各國不應從事或故意支持蓄意破壞或以其他方式損害關鍵基礎設施的利用和運行的信通技術活動」，[59] 但中國大陸偕同俄羅斯、巴基斯坦、白俄羅斯與馬來西亞等國指出西方國家認為網路攻擊構成「使用武力」(use of force)，可能形成西方濫權干預行動藉口，反對各國可以據此主張遭到「武力攻擊」(armed conflict)，進而援用聯合國憲章第51條視同他國之「準」戰爭行為並行使自衛權(right of self-defense)反擊。[60] 這除了國際法對於當「使用武力」的程度超越何種門檻時，便可視同「武力攻擊」並沒有客觀的共識外，當時更因美國自2014年起便不斷指控中國大陸從事網路間諜活動並起訴5名解放軍駭客，[61] 故中共擔心恣意將網路攻擊等同為「使用武力」，將促使西方國家有正當國際法律基礎制裁中國大陸。[62]

58 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017).

59 聯合國大會，《關於從國際安全的角度看信息和電信領域的發展政府專家組(A/70/174)》（紐約：聯合國，2015），頁2。

60 Adam Segal, "Chinese cyber diplomacy in a new era of uncertainty," *Hoover Institution*, Aegis Paper Series 1703, 2017, p. 7.

61 Ellen Nakashima, "*Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyberspying*," Washington Post, 22 May 2014, <https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html>（檢索日期：2022年9月15日）

國際社會對於國際法如何適用網路空間的討論愈趨分歧，中國大陸於2019年底聯合俄羅斯於聯合國成立新的不限成員名額工作組(Open-Ended Working Group, OEWG)，並另闢場域討論未來有關國際安全之資訊及電信問題。[63] 而2020年後聯合國網路規範的討論因新冠疫情(COVID-19)影響而推遲，中國大陸方面主張新的OEWG工作小組的優勢在於與過去西方主導的討論更為「開放」、「包容」以及「透明」。[64] 同時，正如同中國大陸在OEWG於2019年成立時所作陳述：各國應對其領土內的ICT (Information and Communication Technology)基礎設施、資源以及與ICT相關的活動行使管轄權。[65] 及至2022年時由於俄烏戰爭阻礙東西方國家就網路規範共識凝聚，不過可以確信的是，OEWG已成為中國大陸與俄羅斯等國大力推行其所倡議的網路主權模式處理數據空間爭議的主要管道；[66] 而這樣的發展也顯示中、俄兩國更能擺脫過去西方國家主導的國際秩序而另立門戶，國際法層面之網路規範仍然無具體共識。[67]

二、國內法層次問題

由於國際間缺乏對於網路行為的具體共識，造成我國國內法的規範便顯得特別重要。過去在國際關係研究中，無論將「國際規範」視為國際慣習、習慣法或是國際法，國際規範皆廣泛的被認為是用來律定行為，並轉而被內化成為國際行為體身分認同與個別利益不可分割的一部分；[68] 也因此國際規範往往不同於國內法，在法律實務上被視為軟性法律。然而，若單就國際成文法學理研究而言，在法學的研究上就國內法或國際法孰重孰輕、孰優孰劣的問題，一直有著「一元論」與「二元論」之不同立場。「一元論」認為無論是國際法或國內法，均是用來規範人類行為整體秩序，故當條文產生爭議時國際法位階應優於國內法。主「二元論」則認為兩者並無必然位階關係，國際法須經國內立法機關制定成國內法後（國際條約審認）方能成為國內法遵循。因此當現行國際社會缺乏就網路攻擊行為達成明確共識的國

62 黃志雄，〈國際法視角下的「網絡戰」及中國的對策——以訴諸武力權為中心〉，《現代法學》，2015年5月，頁145-58。

63 聯合國大會，《從國際安全角度看資訊和電信領域的發展不限成員名額工作組(A/AC.290/2019/1)》（紐約：聯合國，2019）。

64 黃志雄、劉欣欣，〈2020年上半年聯合國資訊安全工作組進程網路空間國際規則博弈〉，《中國資訊安全》，2020年7月，頁68-71。

65 China, "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security," <https://www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf>（檢索日期：2022年9月15日）

66 Dennis Broeders, Liisi Adamson, and Rogier Creemers, "A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace," *The Hague Cyber Norms*, 2019, pp. 1-20.

67 姚宏旻，〈型塑網路主權與爭辯網路治理：中國大陸就全球網路規範的戰略敘事運用〉，《中國大陸研究》，第64卷第2期，2021年9月，頁107-39。

68 Peter Joachim Katzenstein, *The Culture of National Security: Norms and Identity in World Politics* (Columbia University Press, 1996), p. 5.

際條文，則依照國際慣例，解讀特定國家在網路上的軍事行動，主要便須仰賴該國國內法對網路行動的定義作為理解依據，這迫使得本文須詳加討論我國國內法如何定義網路行動。

目前我國軍事單位在網路上的作業行為，主要涉及「國防法」、「通訊保障及監察 法」與「國家情報工作法」，以下僅就軍事行動與情報行動兩方面來分析。

(一)視網路攻擊為「軍事行動」時

首先，依「國防法」精神，國軍主要任務為作戰、演習、訓練及災害防救。當國家發布緊急狀況時國軍依法執行作戰、保衛國家安全。平時則依法律律定執行包含演習及訓練等戰備整備任務，並視需要執行災害防救等任務。也因此如果將網路攻擊行為視為軍事行動，勢將涉及思考制定相對應程序律定「自衛反擊權」的合理授權。同時，就網路空間的地理特性而言，許多網路攻擊可能皆是源自於境外區域時，若經授權對境外地區發動網路攻擊，我國亦須考量資通電軍的軍事行為是否有升高區域衝突之疑慮。

其次，由於網路世界相互構聯，且資訊裝備在網路中僅以IP呈現，故在「經常戰備時期」對各網路裝備缺乏明確能見度前提下，是否有可能不慎侵入國人持有之資訊設備。且由於資通電軍未具司法警察身分，依我國「通訊保障及監察法」律定，對國人之電信監偵須「由檢察官依司法警察機關聲請或依職權以書面聲請該管法院核發」。在現行法令規範下，若資通電軍執行網路入侵行動可能構成侵害人權與違反法令之疑慮。由於前述之法令限制，目前國內各單位之網路攻防演練，都是經行政院預先核定之訓練計畫，方能符合我國「國防法」平時戰備演訓之規範。

(二)視網路攻擊為「情報行動」時

在國際上，英國自2016年成立的國家網路安全中心(National Cyber Security Centre, NCSC)屬國家情報機關政府通信總部(Government Communication Headquarter, GCHQ)，而美國網路戰司令部亦屬國家情報機構之一環，其指揮官又同時肩負國家安全局長頭銜；而北約所資助的塔林手冊2.0，亦認為平時的網路間諜活動並不違反國際法規範。[69] 故常為人所忽略，這些西方國家均將網路活動定義為如傳統電訊偵查(SIGINT)手段的情報部門行動而非正規軍事行動。

西方國家之所以這樣設計可能源自以下兩種考量。首先，認為情報活動自古以來就是國家確保生存的手段，且這樣的行動必須貫穿平戰時，由於沒有明確國際規範認定間諜行為違反國際法，所以當間諜行為遭他國發現時，他國通常採「國內法」處理間諜案，也因此過去美國司法部僅能以司法起訴中共解放軍駭客。[70] 其次，負責界定國際間電訊行為的國際電信聯盟，在其國際電信聯盟憲章第37條雖然律定成員國須採取一切

69 同註57，p. 35.

70 Hon-min Yau, "Explaining Taiwan's Cybersecurity Policy Prior to 2016: Effects of Norms and Identities," *Issues & Studies* 54, no. 02, 2018, pp. 1-30; Ellen Nakashima, "*Russia's apparent meddling in U.S. election is not an act of war, cyber expert says*," Washington Post, 7 February 2017, <https://www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/>（檢索日期：2022年9月15日）

可能的措施，確保國際通信的機密性，但條文也允許各成員國依本國法律或其他國際條約向特定單位透露國際通訊之內容；[71] 也因此在合適的跨國合作協議安排與國內法保障下，跨國監聽是允許的。最後，無論間諜行為對他國如何具侵犯事實，但都不是聯合國認定的為侵略行為之一，所以即便如何不友善，只要未跨越造成實體破壞門檻，屬情報活動的網路攻擊行為，都不具備視為戰爭行為的風險。[72]

2020年我國已修訂「國家情報工作法」，並將資通電軍執行情報相關任務時視為「準」情報機關，即便「通訊保障及監察法」規範情報機關首長得核發通訊監察書，但授權監聽範圍僅涵蓋外國籍人民，由於網路世界相互構連且難於即時確認裝備用途與身分之特性，故若不慎侵入本國籍人民資訊設備，仍須依「通訊保障及監察法」補正監聽司法程序，並在監聽完成後具文當事人。[73] 最後，由於資通電軍在此規範下為執行情報間諜活動的軍事人員，國際上許多國家內部法律規範下，主張情報人員不受武裝衝突法保障，故我國也須整體規劃未來對於這類軍事人員作業安全保障的可能衝擊應處。[74]

柒、政策反思

綜整以上戰略理論學理探討、網路作戰空間特性、網路攻防限制與現行國內外法遵體制研析等面向檢視後，本文對於我國網路安全政策之未來策進，有以下4項建議：

一、謹慎以對網路攻擊能力之效果、強化網路防禦能量

國際關係攻擊與防禦理論(offense-defense theory)論述顯示，當執政者認為科技將使攻擊方佔優勢時，由於擔憂受制於人，便造成加強軍備競賽增加嚇阻能力，但衝突反而隨之而來。[75] 這種「攻勢崇拜」(cult of offense)的思維主導下，第一次世界大戰的戰史已顯示，當執政者「主觀」的認定科技能力能使攻擊具優勢，卻未能「客觀」的檢視科技與地理兩因素對於當時作戰的影響時，悲劇便容易產生發生。[76] 也因此當各國政府認定網路攻擊優於網路防禦時，便易於集中資源投注於網路攻擊，而忽略了許多基本網路防禦措施的重要性。然而，有越來越多西方研究顯示網路攻擊能力效果受到誇大，[77] 以及網路嚇阻能力有所限制，[78] 網路戰略學家不經思索主張網路空間是攻勢的優勢空間

71 ITU, "*Constitution of the International Telecommunication Union*," International Telecommunication Union, <https://www.itu.int/council/pd/constitution.html>（檢索日期：2022年9月15日）

72 Michael Schmitt, "*Classification of cyber conflict*," Journal of conflict and security law 17, no. 2 (2012): 245.

73 羅添斌，〈臺灣情報機關增為11個　這些單位都是！〉，《自由時報》，2020年3月2日，<https://news.ltn.com.tw/news/politics/breakingnews/3110449>（檢索日期：2022年9月15日）

74 M.D. Evans, *International Law 5th Edition* (Oxford University Press, 2018), pp. 40-76.

75 Robert Jervis, "Cooperation under the security dilemma," *World politics* 30, no. 02, 1978, pp. 167-214.

76 Stephen Van Evera, "The cult of the offensive and the origins of the First World War," *International security* 9, no. 1, 1984, pp. 58-107.

77 同註48。

78 同註50。

仍是不精確的假定，[79] 網路的「攻勢優勢」是主觀認知而非客觀事實，[80] 特別是在前述分析中顯示，當網路攻擊效益現尚不明顯，故我國在網路安全的投資思維上不能偏廢。

二、國內法令須對網路攻擊之情報或軍事任務予以明確區隔

經分析也發現，我國對於軍方於網路活動之法制作為仍待強化。西方歐美等國家除將網路作戰部隊置於情報部門，其中美國則更透過《聯邦法典》第10篇(Title 10)規範軍事行動，並以第50篇(Title 50)規範情報行動；美國國防部依法需將視軍事行動的網路攻擊於48小時通知國會，並可將具產生實體破壞的網路攻擊迂迴定義為情報行動的隱蔽行動(covert action)。[81]（依國軍軍語辭典亦稱為隱蔽作業）反觀我國目前對於網路軍事任務的執行法規缺乏明確規範，對於網路情報作業的法制規範模糊。這樣的發展就國內影響性而言，除不利我國軍事機關在執行任務尚有所依循，界定明確權責，同時在對保障人民權利的考量下，也可能使軍事機關誤觸侵害人民權利之爭議。除此之外，對國際社會而言，如果我國未能在網路軍事作為與情報作為間予以明確界定，原本預期透過網路攻擊能量強化國防的作法，亦可能在無國際法、國內法規範模糊下，造成軍事挑釁之錯誤意象解讀。顯然的，未來我國須對網路攻擊之情報或軍事兩種不同任務賦予明確法制區隔，以消彌爭議解讀空間。

三、在各國就網路作戰國際規範發展成熟前，我國網路活動應以主張情報活動為主

可以確認的是，目前國際社會對於如何建立國際規範解讀網路攻擊的軍事行為尚未有共識，無論是聯合國UNGGE或是OEWG等工作小組，亦或學術界在塔林手冊的探討，目前僅維持認為攻擊他國關鍵基礎設施是違反國際法的行為，然而對於多大程度違反國際法以及各國應如何反制，目前仍有賴各國政府片面的政治性解讀，並沒有一定應對作法。也因此未來我國如果將網路攻擊行動聚焦在情報目的上，便可以迴避他國假借宣稱遭到網路軍事攻擊的法律戰疑慮。正如同前美國情報總監克拉珀(James Clapper)在2015年人事行政局遭據稱是中國大陸駭客竊取大量資料時所作之陳述：「雖然人事行政局事件被媒體描容為攻擊事件，但實際上並非如此，並沒有認任何系統遭破壞或設定遭竄改，實質上僅只是資料遭竊取」，[82] 顯然網路的情報作業即便是一種非常不友善行為，但還距「戰爭行為」仍有相當法理距離。

四、我國網路戰略之強化，亦應包含純技術能量以外的投注

最後，這也顯示我國對於網路能量之強化不能僅著重在技術能量的建立。由於網路空間之於人類各層面的活動已非過去所能比擬，並涉及軍事戰略、國家安全、經濟活動、法律規範與國際互動各層次，未來我國

79 同註22，p. 41.

80 同註56。

81 Michael E DeVine and Heidi M Peters, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief* (Congressional Research Service, 2018).

82 C-Span, "Hearing on Worldwide Cybersecurity Threats (47:10)," *C-SPAN*, <http://www.c-span.org/video/?328021-1/hearing-worldwide-cybersecurity-threats>（檢索日期：2022年9月15日）

應鼓勵政府、學者及智庫對於新興數位議題的理解與討論，透過多方面向的觀察與激盪，發展我國於網路空間領域的全面整合戰略。

捌、結　　語

後疫情時代對於資訊科技大量的運用現象，以及俄烏戰爭期間網路攻擊運用的實際觀察，恰可為我國現行網路安全戰略提供一良好反思契機。本文引入近年國際重大事件的實證性證據，透過詳加檢視網路作戰的地理及科技等限制，並對網路行動攻勢優勢與法理脈絡作出比較與分析。本文惕勵網路安全研究的戰略學者，應立基於網路空間的實際地理與科技特性執行因地制宜的分析，並對過去逕自假借來自實際空間軍事作戰的普遍設想分析提出風險示警；由於對網路空間執行戰場情蒐與戰果評估有其限制，故吾人對於過去網路作戰牢不可破的刻板印象亦須作出適度修正。換言之，若我國戰略研究學者未能與自身安全環境連結，進而作出因地制宜與因時制宜的持續性學理反思，則可能陷於不假思索的刻板印象而不自知，並允許攻勢主宰網路戰場的主流認知持續主宰大眾思維。如此將易使政府決策者僅僅著重於攻勢能量的建立，而忽略在戰略發展、法規建立與守勢能量之衡平投資，這亦顯示出我國若在未能謹慎檢驗網路戰略設想的各面向基礎前提下執行策略構思，則後續數位國土防衛的政策規劃就有可能產生偏頗。

除此之外，由於國際社會對於網路戰爭(Cyber War)的行為規範結構仍然非常浮動，因此我國亦需持續投入關注國際社會對這新興科技與國際安全領域的討論，並與時俱進的精進各項法規作為，以避免陷於釋放國際社會錯誤政治訊息而不自知的窘境。總之，網路空間是臺灣的一個新領域，科技及地理對該領域的影響皆與過去實際空間的作戰分析假定不同，也因此我國絕不能逕行沿用舊有領域之戰略設想，需要更為審慎與全面地對待這一新數位作戰場域。換言之我國確實需要吸引與投入更優質人才於該領域之研究，以增強我國網路安全，但若將這樣的資源僅僅專注於吸引更多具有深厚攻勢技術知識的駭客人員，則將是一種政策偏廢的謬失。

（收件：111年9月15日，第1次修訂：111年11月14日，第2次修訂：111年12月5日，接受：112年3月8日）

參考文獻

中文部分

專書

王湘穗、喬良，1999。《超限戰》，北京：解放軍文藝出版社。

許秀影、劉豐豪、張瑞勇，2010。《前瞻國軍對次世代網路之應用》，桃園：國防大學。

黃光國，2013。《社會科學的理路（第三版）》，臺北：心理出版社。

期刊論文

呂兆祥，2015。〈共軍網路作戰對我資電作戰之影響〉，《國防雜誌》，第30卷第6期，頁1-27。

姚宏旻，2021。〈形塑網路主權與爭辯網路治理：中國大陸就全球網路規範的戰略敘事運用〉，《中國大陸研究》，第64卷第2期，頁107-139。

戴政龍，2013。〈中共「網軍」發展與網絡攻防：兼論我國資通安全之政策規劃〉，《戰略與評估》，第4卷第4期，頁97-120。

黃志雄，2015。〈國際法視角下的「網絡戰」及中國的對策—以訴諸武力權為中心〉，《現代法學》，2015年5月，頁45-58。

黃志雄、劉欣欣，2020。〈2020年上半年聯合國資訊安全工作組進程網路空間國際規則博弈〉，《中國資訊安全》，2020年7月，頁68-71。

官方報告

聯合國大會，2019。《從國際安全角度看資訊和電信領域的發展不限成員名額工作組(A/AC.290/2019/1)》，日內瓦：聯合國，頁1-2。

聯合國大會，2015。《關於從國際安全的角度看資訊和電信領域的發展政府專家組(A/70/174)》，日內瓦：聯合國，頁1-16。

網際網路

岳陽市中級人民法院，2011/09/17。〈彭宇華、李明哲顛覆國家政權案〉，《微博》，<https://www.weibo.com/3960688335/FlijUcKOA?from=page_1001063960688335_profile&wvr=6&mod=weibotime&type=comment#_rnd1508944658512>。

羅添斌，2020/03/24。〈臺灣情報機關增為11個　這些單位都是！〉，《自由時報》，<https://news.ltn.com.tw/news/politics/breakingnews/3110449>。

外文部分

專書

Altheide, C., and H. Carvey, 2011. *Digital Forensics with Open Source Tools*. New York: Elsevier Science.

Arquilla, John, 1996. *The advent of netwar*. Santa Monica, CA: RAND Corporation.

Arquilla, John, and D. Ronfeldt, 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation.

Clarke, Richard A, and Robert K Knake, 2011.

Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke, 2010. *On Cyber Warfar*e. London: Chatham House.

Dinniss, Heather Harrison, 2012. *Cyber Warfare and the Laws of War*. Cambridge University Press.

Evans, Malcolm David, 2018. *International Law 5th Edition*. Oxford: Oxford University Press.

Gray, Colin S, 2013. *Making Strategic Sense of Cyber Power: Why The Sky is Not Falling*. Pennsylvania, U.S.: Strategic Studies Institute, US Army War College.

Katzenstein, Peter Joachim, 1996. *The Culture of National Security: Norms and Identity in World Politics*. Columbia University Press.

Kramer, Franklin D, Stuart H Starr, and Larry K Wentz, 2009. *Cyberpower and national security*. Washington, DC, US: Potomac Books, Inc..

Lambeth, Benjamin S, 2001. *NATO's air war for Kosovo: A strategic and operational assessment*. Rand Corporation.

Rid, Thomas, 2013. *Cyber War Will Not Take Place*. Oxford, UK: Oxford University Press.

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

Schneier, B, 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, US: W. W. Norton.

Schreier, Fred, 2012. *On cyberwarfare*. DCAF Horizon 2015 Working Paper Series. Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Singer, P.W., and A. Friedman, 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know?* Oxford, UK: Oxford University Press.

Zetter, K, 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York, US: Crow Publishing Group.

期刊論文

Broeders, Dennis, Liisi Adamson, and Rogier Creemers, 2019. "A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace." *The Hague Cyber Norms*, pp. 1-20.

Bucci, Steven, P, 2009. "A most dangerous link." *US Naval Institute Proceedings* 135, no. 10, pp. 38-42.

Cavelty, M. D, 2008. "Cyber-terror-looming threat or phantom menace? The framing of the US cyber-threat debate." *Journal of Information Technology & Politics* 4, no. 1, pp. 19-36.

Dombrowski, Peter, and Chris C Demchak, 2014. "Cyber war, cybered conflict, and the maritime domain." *Naval War College Review* 67, no. 2, pp. 70-96.

Erwin, Sandra I, 2016/08/08. "Defense CIO: Cybersecurity Improving but Innovation Lags." *National Defense*, August, pp. 1-20.

Geers, K, 2010. "A brief introduction to cyber warfare." *Common Defense Quarterly*, no. Spring 2010, pp.16-17.

Heilmann, Sebastian, 2016. "Leninism upgraded: Xi Jinping's authoritarian innovations." *China Economic Quarterly* 20, no. 4, pp. 15-22.

Jervis, Robert, 1978. "Cooperation under the security dilemma." *World politics* 30, no. 02, pp. 167-214.

Kreisher, Otto, 2007/12. "Risk to One Is Risk to All." *Sea Power* 50, no. 12, 3.

Ma, Ying-han, 2018. "Military Cyber Threats and Responses." *Defense Security Brief* 7, no. 2, p. 6.

Milevski, Lukas, 2011. "Stuxnet and Strategy: A Space Operation in Cyberspace." *Joint Forces Quarterly* 63, no. 4, p. 6.

Romney, Gordon W, Jeremiah K Jones, Brandon L Rogers, and Philip MacCabe, 2005. "IT security education is enhanced by analyzing Honeynet data." Paper presented at *the Information Technology Based Higher Education and Training*, 2005. ITHET 2005. 6th International Conference, pp. FJOIlO-F3D/l4.

Schmitt, Michael, 2012. "Classification of cyber conflict." *Journal of conflict and security law* 17, no. 2, pp. 245-60.

Segal, Adam, 2017. "Chinese cyber diplomacy in a new era of uncertainty." Hoover Institution, *Aegis Paper Series* 1703, pp. 1-23.

Slayton, Rebecca, 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3, pp. 72-109.

Smythe, Charles, 2020. "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance." *Yale Journal of International Affairs* 15, p. 98.

Susanto, Heru, Mohammad Nabil Almunawar, and Yong Chee Tuan, 2011. "Information security management system standards: A comparative study of the big five." *International Journal of Electrical Computer Sciences* IJECSIJENS 11, no. 5, pp. 23-29.

Van Evera, Stephen, 1984. "The cult of the offensive and the origins of the First World War." *International security* 9, no. 1, pp. 58-107.

Yau, Hon-min, 2019. "A critical strategy for Taiwan's cybersecurity: a perspective from critical security studies." *Journal of Cyber Policy* no.01, pp. 1-21.

Yau, Hon-min, 2020. "Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation?". *Issues & Studies* 56, no. 03, pp. 1-20.

Yau, Hon-min, 2018. "Explaining Taiwan's Cybersecurity Policy Prior to 2016: Effects of Norms and Identities." *Issues & Studies* 54, no. 02, pp. 1-30.

Yau, Hon-min, 2020. "Framing Cyber Security in Taiwan: A Perspective of Discursive Knowledge Production." *Korean journal of defense analysis* 32, no. 3, pp. 457-474.

官方報告

Curtin, NP, 2004. "Military operations: recent campaigns benefited from improved communications and technology, but barriers to continued progress remain." In GAO Reports, pp. 1-547.

DeVine, Michael E, and Heidi M Peters, 2018. Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief. Congressional Research Service, pp. 1-14.

Keaney, Thomas A, 1993. Gulf War air power survey. Vol. 4: Office of the Secretary of the Air Force, pp. 1-538.

Polyakova, Alina, and Chris Meserole, 2019. "Exporting digital authoritarianism: The Russian and Chinese models." In Policy Brief, Democracy and Disorder Series, 1-22. Washington, DC: Brookings, pp. 1-22

Przetacznik, Jakub, and Simona Tarpova, 2022. "Russia's war on Ukraine: Timeline of cyber-attacks." Brussel, Belgium: European Parliamentary Research Service, pp. 1-7.

US DoD, 2011. Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011. Washington, DC, US: Department of Defense, pp. 1-14.

US DoD, 2015. The DoD Cyber Strategy. Washington, DC, US: Department of Defense, pp. 1-33.

報紙

Broad, William J., and David E Sanger, 2017/03/14. "U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight." New York Times, <https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html>.

Crerar, Pippa, 2018/10/04. "Russia accused of cyber-attack on chemical weapons watchdog." The Guardian, <https://www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body>.

Fleishman, Glenn, 2000/12/14. "Cartoon Captures Spirit of the Internet." New York Times, <https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html>.

Heath, Brad, 2021/02/15. "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president." Reuters, <https://www.reuters.com/business/media-telecom/solarwinds-hack-was-largest-most-sophisticated-attack-ever-microsoft-president-2021-02-16/>.

Nakashima, Ellen, 2014/02/15. "Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyberspying." Washington Post, <https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html>.

Nakashima, Ellen, 2017/02/07. "Russia's apparent meddling in U.S. election is not an act of war, cyber expert says." Washington Post, <https://www.washingtonpost.com/

news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/>.

Perlroth, Nicole, 2021/09/14. "Apple Security Update Closes Spyware Flaw." New York Times, <https://www.nytimes.com/2021/09/13/technology/apple-software-update-spyware-nso-group.html>.

Srivastava, Mehul, 2022/05/10. "Prospect of Russian cyber war may have been 'overhyped', says UK spy chief." Financial Times, <https://www.ft.com/content/d5657df5-a962-4acf-b0bd-b892c6b15361>.

Uberti, David, and Catherine Stupp, 2021/05/10. "Colonial Pipeline Hack Sparks Questions About Oversight." Wall Street Journal, <https://www.wsj.com/articles/colonial-pipeline-hack-sparks-questions-about-lax-cyber-oversight-11620689340>.

Wu, Sarah, and Eduardo Baptista, 2022/08/05. "From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit." Reuters, <https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/>.

網際網路

C-Span, 2015/09/10. "Hearing on Worldwide Cybersecurity Threats (47:10)." C-SPAN, <http://www.c-span.org/video/?328021-1/hearing-worldwide-cybersecurity-threats>.

China, 2015/09. "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." <https://www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf>.

Dudu Mimran Blog, 2015/02/10. "The Emergence of Polymorphic Cyber Defense." <https://www.dudumimran.com/2015/02/the-emergence-of-polymorphic-cyber-defense.html>.

Economist, 2022/03/01. "Cyber-attacks on Ukraine are conspicuous by their absence," Economist, <https://www.economist.com/europe/2022/03/01/cyber-attacks-on-ukraine-are-conspicuous-by-their-absence>.

European Union, 2022/09/15. "Cyber Resilience Act." European Union, <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.

ITU, 1994/10/01. "Constitution of the International Telecommunication Union." International Telecommunication Union, <https://www.itu.int/council/pd/constitution.html>.

Microsoft, 2022/01/15. "Destructive malware targeting Ukrainian organizations." Microsoft, <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>.

MOFA, 2017/07/03. "Ministry of National Defense launches new cybersecurity command." Taiwan Today, <https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=

117794>.

National Cyber Security Centre, 2018/02/14. "Russian military 'almost certainly' responsible for destructive 2017 cyber attack." National Cyber Security Centre, <https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack>.

Thim, Michal, 2015/09/05. "Taiwan's Invisible Frontier: Cyberspace." Thinking Taiwan Foundation, <https://taiwan-in-perspective.com/2015/09/05/taiwans-invisible-frontier-cyberspace/>.

Thomas Rid, 2012/02/27, "Cyber war-Think again," Foreign Policy, no. 192 (2012), <https://foreignpolicy.com/2012/02/27/think-again-cyberwar/>.

Viasat, 2022/03/30. "KA-SAT Network cyber attack overview." Viasat, <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>.