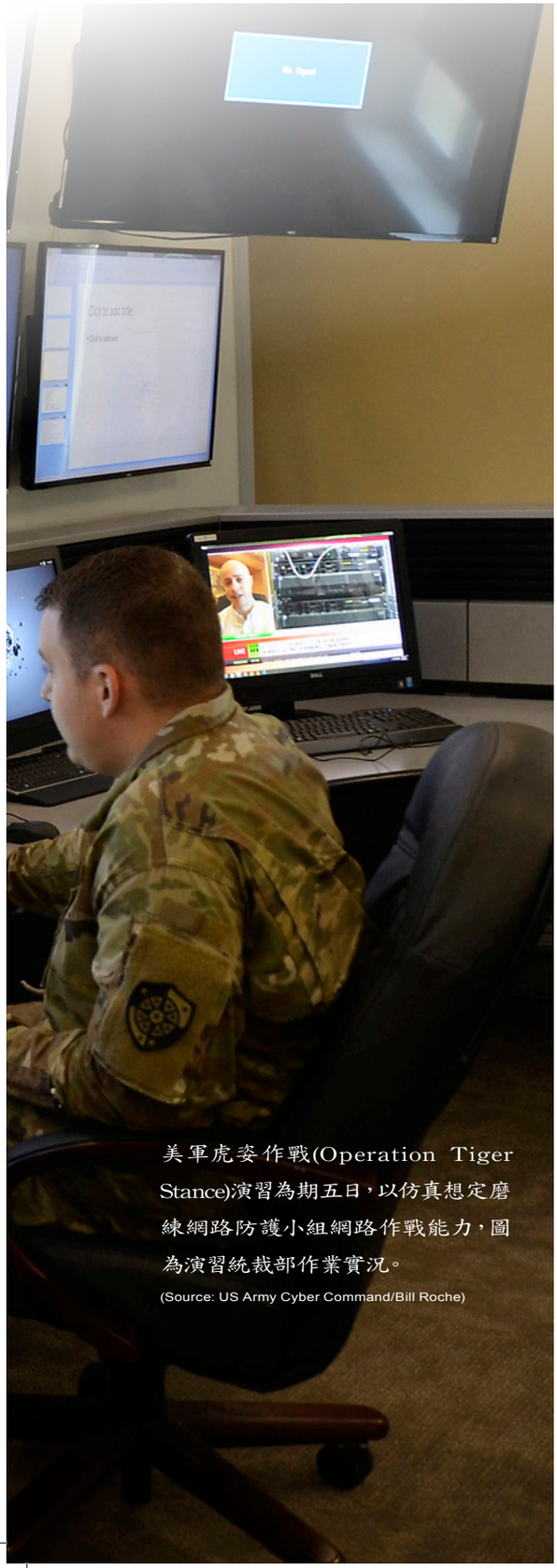
● 作者/Ryan Tate ● 譯者/黃文啟 ● 審者/丁勇仁

透明的網路嚇阻

Transparent Cyber Deterrence

取材/2022年第四季聯合部隊季刊(*Joint Force Quarterly*, 4th Quarter/2022)



美軍虎姿作戰(Operation Tiger Stance)演習為期五日，以仿真想定磨練網路防護小組網路作戰能力，圖為演習統裁部作業實況。
(Source: US Army Cyber Command/Bill Roche)

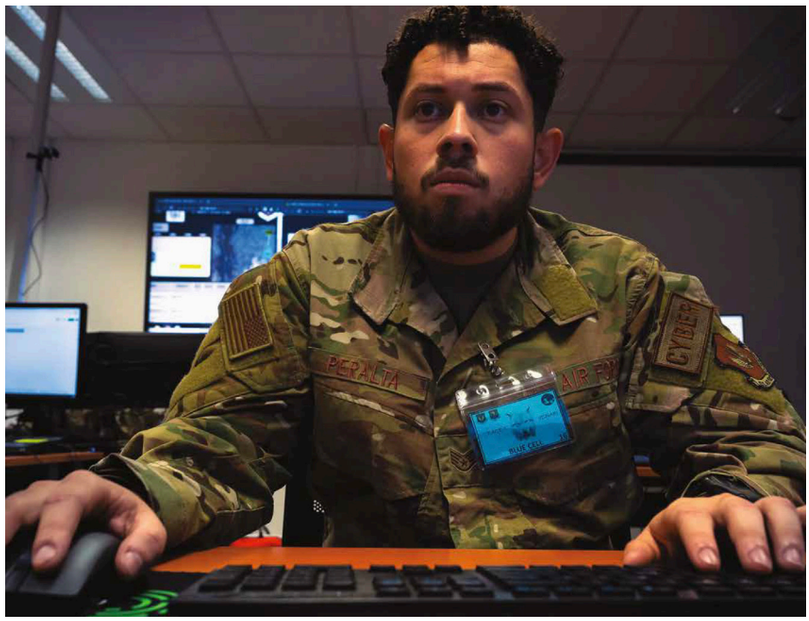
網路惡意攻擊與相關犯罪行爲已對美國及其友邦之安全構成嚴重威脅，欲打擊是類行爲者，美國及相關國家應主動出擊，並妥適揭露相關資訊，以有效發揮嚇阻效果。

美國目前不斷遭受來自他國資助惡意網路行為者的攻擊。美國「網路安全暨基礎設施安全局」(Cybersecurity and Infrastructure Security Agency, CISA)指出，這些惡意網攻活動估計每年造成美國經濟高達2,420億美元的損失。[1] 網路安全公司邁克菲(McAfee)與戰略暨國際研究中心(Center for Strategic and International Studies)的共同報告顯示，大多數美國及其盟國所遭受的網路攻擊，來自俄羅斯、中共、北韓及伊朗等國，這些國家的政府已與各種國家及非國家惡意網路行為者建立了共生關係。[2] 美國國家網路戰略要求透過「網路及非網路手段讓對手付出代價」以建立嚇阻力量。[3] 美網路司令部(U.S. Cyber Command, USCYBERCOM)雖然擁有龐大的網路攻擊能力，但網路空間的本質卻導致其對網路嚇阻的貢獻模糊不清。針對堅決、強悍且往往有利可圖的行為者而言，網路嚇阻仍未見具體作為。美國政府必須思考其他可以讓惡意網路活動付出更高代價的選項，方能加以嚇阻。

2020年「網路空間日晷委員會」(Cyberspace Solarium Commission)、國務院對美國總統建議事項及國防部專案小組研析等，都提議採取各項重要行動，以維護網路嚇阻力量。然而，諸如溯源問題與遭破壞風險等根本性網路空間挑戰，都阻礙相關工作的落實。美國網路司令部司令兼國家安全局局長中曾根(Paul Nakasone)上將，說明戰略效果「來自於網路戰力的運用——而非僅是擁有力量」。[4] 近年網路攻擊戰力的運用

顯現出有各種嚇阻的新選項。嚇阻雖為美國國防戰略的核心項目，然惡意網路行為者對美國的攻擊行為卻始終未受到懲罰。網路攻擊能力應如何輔助網路嚇阻力量呢？

公開揭露是網路攻擊戰力嚇阻惡意網路行為者的必要手段，已納入美國戰略指導，同時從近年各種網路空間行動，亦證明確實可以做到。揭露網路攻擊戰力的針對性運用，可以左右惡意網路行為者的成本獲益決策。手段運用加上揭露作為——亦即透明網路嚇阻——能提高惡意行為者必須面對直接對其造成影響的後果之預期性。此種透明化概念可以藉由嚇阻惡意網路活動的範圍與主動性，並且鼓勵同道盟國採取類似行動，達到形塑國際行為的效果。透明網路嚇阻係基於嚇阻理論、政府內部與學術界針對網路嚇阻的建議事項、以及近年美國與歐洲針對俄羅斯干預美國選舉，以及「黑暗面」(DarkSide)、「僵屍網路」Trickbot與Emotet等全球網路犯罪行為所做的網路空間輔助報復行動。本文將檢視惡意網路活動的戰略問題、運用網路攻擊能力的網路嚇阻框架、以及美國的戰略方針。接續再針對透明網路嚇阻概念提出建議，並簡要分析該概念的合宜性、可接受性、可行性、各項風險及相關影響等。



2022年5月19日，美空軍第52通信中隊任務防禦小組督導官波拉爾塔(Joseph Peralta)上士，於德國蘭斯坦空軍基地「沉默獵殺」(Tacet Venari)演習中負責鑑別網路破壞徵候。(Source: USAF/Jared Lovett)

惡意網路活動的戰略性問題

國家與非國家行為者基於各種理由所採取的網路活動，最終損及美國的力量，並以不對稱手法侵蝕美國的競爭優勢。美國國務院政策專家高曼(Emily Goldman)主張，美國當前所面對的危機在於各種威脅的數量、多元性及精密度不斷提高，且其行為已從刺探，轉向擾亂性及破壞性攻擊。[5] 國家資助的惡意網路活動包含智慧財產間諜行為、資助非法活動與削弱競爭者的網路犯罪、秘密影響宣傳活動、以及針對重要基礎設施所發動的擾亂性攻擊。中曾根上將針對美國目前在網路空間所遭遇的戰略挑戰摘述如下：

> 今日實力相當和實力相近競爭者不斷在網路空間採取對付美國的行動。這些活動都不是個別的駭客行為或意外，而是戰略層級戰役行動。網路空間讓美國的對手獲得發動持續性、非暴力行動的新方式，藉由未達引發武力反制門檻條件的行為，侵蝕美國軍事、經濟及政治實力，創造累積性戰略影響。[6]

未來惡意網路活動的擴散，不論其是否具有金錢或戰略動機，都對美國國家利益構成威脅。據邁克菲公司指出，惡意網路活動所造成的生產力損失，傷害國家安全並損害經濟。[7] 美國雖然擁有所有實力手段的優勢，但惡意網路行動仍能不斷破壞並侵蝕美國的經濟與科技競爭優勢。國家資助的惡意網路活動，範圍涵蓋網路空間間諜行為、鼓動網路犯罪(例如，在主權領土範圍內容許勒索軟體行動)、針對重要基礎設施的破壞性攻擊、以及破壞民主體制與程序嚴整性的種種行為。例如，路透社報導指出，北韓就是運用惡意網路活動聚斂其核武與飛彈計畫所需資金。[8] 惡意網路活動的成本獲益優勢，正是造成其泛濫的主因。

網路行為者所需付出之操作成本及承擔之風險很低，而報酬卻相當可觀。英國德勤(Deloitte)顧問公司估計，網路犯罪每月的操作成本僅約544到3,796.9美元。[9] 相較之下，美國聯邦調查局估計，網路竊取行為平均每次卻會造成5,000美元的損失。[10] 惡意網路活動獲益之處並非僅止於成本效率。網路空間的設計具有五大優勢：可選擇規模、具有從任何地點行動的能力、可取得獲致所望精確度的工具、利用各種工具掩飾必然的奇襲效果與重複使用性、以及因為來源不明而得以避免報復的能力。[11] 美國聯邦調查局局長瑞伊(Christopher Wray)表示，美國必須「改變罪犯及某些國家的成本獲益算計方式，因為他們相信自己可以破壞美國的網路、竊取美國財富和智慧財產、同時讓美國的重要基礎設施陷於危險，卻完全毋須承擔任何風險」。[12] 美國雖然可以提高惡意網路行為

2021年11月10日，美空軍第333訓練中隊網路戰軍官薛利(Alexis Shirley)少尉和克里斯波(Trisha Crisp)少尉，於密西西比州基斯勒空軍基地史丹尼斯大樓的網路脫逃室完成網路任務。(Source: USAF/Seth Haddix)

者直接運用網路攻擊能力所應付出代價，但欲左右其決定需要置重點於提高這些行為者所須付出成本的期望值。

網路嚇阻框架

嚇阻理論的精義在於，預期因遭報復所付出之代價將遠超過惡意活動利益，即可能嚇阻惡意網路行為者。美國國會、國務院與國防部的諮詢團隊，近期針對網路嚇阻提出多項建議。2020年「網路空間日晷委員會」論定，網路嚇阻需要明確傳達各種後果、使付出代價超過認定利益、具可信度的能力與決心、危機升級管理、溯源能力，以及何時必須「志願性自行追溯網路行動」的政策。[13] 美國國務院強調網路行為者必須確信其將面對各種後果，以及大眾與個人溝通、更有效溯源、直接鎖定網路行為者及夥伴國協同報復的必要性。[14] 美國國防部「網路嚇阻專案小組」(Task Force on Cyber Deterrence)提議，應採取鎖定惡意網路行為者最珍惜事物的嚇阻行動。此舉可以藉由運用多重國力手段、傳達反制能力與意志、以及不預期效應的風險管理，諸如危機升級或工具遭破壞。該專案小組預測，此種安排將促成網路空間規範成為美國正當性的重要事項。[15] 政府提出的各項建議都已包含學者們辯論的重要議題。

學者們爭辯網路空間嚇阻的可行性，同時闡述網路嚇阻必須解決某些一再重複出現的主題。戰略大師奈伊(Joseph Nye)表示，網路嚇阻取決於心理認知、溯源、不確定性及危機升級風險，而且必須考量其相互糾葛與各種規範。[16] 學者古德曼(Will Goodman)主張，真實世界的例證顯示，網路嚇阻確實可行，但其挑戰包含溯源、匿名性、規模針對能力、再保證程度、危機升級及明確傳達訊息等多項議題。[17] 另一方面，分析專家費舍凱勒(Michael Fischerkeller)及政治學教授哈克內特(Richard Harknett)則主張，網路空間的獨特性讓低於動武門檻的嚇阻行為無效，兩人推論持續互動可以鼓勵穩定競爭。[18] 牛津大學學者塔迪歐(Mariarosaria Taddeo)則推論，網路空間在溯源性、可靠傳達訊息、危機升級、效應不確定性和比例原則等方面的特質，使嚇阻行為效用受限。[19] 溯源性、可信度、明確傳達訊息、可擴展性、環境不確定性、錯誤認知、危機升級、遭破壞風險、意外效應及規範問題等，都是學者普遍爭議的主題。交互運用政府與學界的建議事項，可以成為建立有用框架的依據。

有效嚇阻需要能力、可信度及訊息傳達。能力是發揮可造成重大代價之針對性、比例性及可擴展性效應的力量。可信度意味著惡意網路行為者相信，能力與使用能力的決心確實存在。訊息傳達是對網路行為者，以及盟國與夥伴國等目標明確傳達意圖，將針對特定惡意網路活動施加某些後果的機制。

關鍵輔助能力包含溯源、情報及行動能力。溯源是充分追蹤特定行為者從事惡意網路活動的能力，以利進行針對性報復，而不受網路空間混淆與匿名特質影響。情報可以幫助網路空間溯源作為、評估各種效果和反應，以及辨識網路行為者的利益和認知。避免遭溯源而被報復，是惡意網路行為者確認其網路活動具備有利成本獲益衡量的關鍵要素。行動能力則是運用訊息傳達適

切運用各種戰力的能力，以影響惡意網路行為者的決策，同時消弭風險與建立正當性。

網路嚇阻的主要風險為破壞行為、意外效應及危機升級。破壞行為是意外洩露機敏網路的能力與弱點，或是情報的來源與方法。網路的不確定性與變動性，讓各種行動很容易產生不預期效應與認知的模糊性及操弄。危機升級包含激化衝突的意外反應。透明網路嚇阻應解決上述諸般因素，以提高惡意網路行為者的預期代價，同時支持美國的戰略。

戰略層級做法

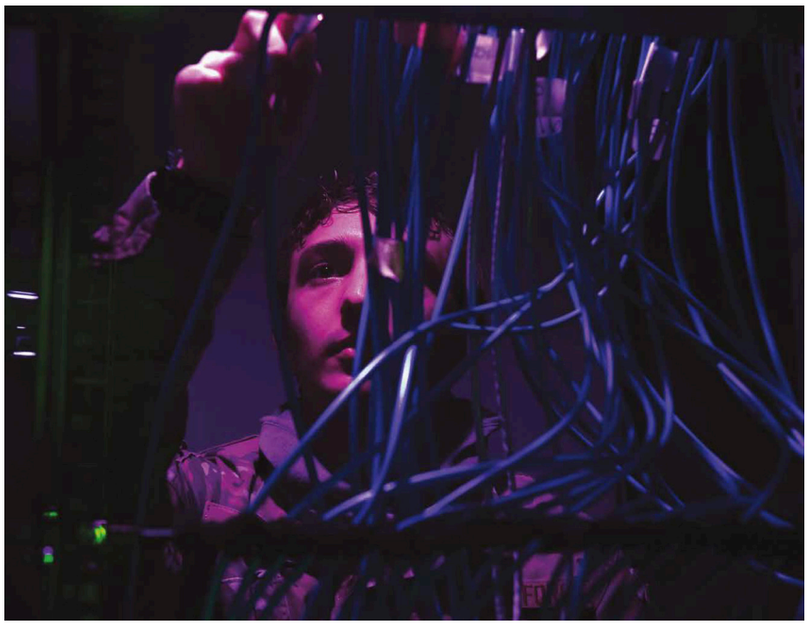
美國國家安全將嚇阻列為優先重點。[20] 拜登總統的指導方針，是要讓惡意網路行為者付出適切的代價，同時結合盟國與夥伴國力量，打造全球網路空間行為標準。[21] 美國前總統川普所公布的《2018年國家網路戰略》(*2018 National Cyber Strategy*)追求「協同盟國與夥伴國──嚇阻且在必要時懲罰使用網路工具從事惡意目的者」，內容包含「建立國家在網路空間負責任行為共識」，以及「不負責任行為應承擔後果」。其內容指出：

> 所有國家力量手段均應用於預防、反應及嚇阻對付美國的惡意網路活動。此舉包含外交、資訊、軍事(殺傷與網路手段)、金融、情報、公眾溯源和執法能力。美國將確立並規劃各項整體戰略與志同道合夥伴共同追溯及嚇阻惡意網路活動，以便在惡意行為者傷害美國及我方夥伴時，能對其施加快速、代價高昂及透明的後果。[22]

透明網路嚇阻必須能促成美國盟國與夥伴國建立一套明顯可見的系統，可對惡意網路行為者加諸符合比例原則的後果，以形塑網路空間的全球行為規範。

美國在網路空間外，確實已經對惡意網路活動造成快速、代價高昂及透明的後果。美國司法部近期宣布，起訴四位對美國及其盟國從事惡意網路活動的中國大陸籍人士。[23] 美國財政部也對特定俄羅斯企業與個人進行廣泛金融禁令，以報復2020年對「太陽風」(SolarWinds)公司的攻擊事件。[24] 針對網路干預美國選舉的報復行為，包含刑事起訴及經濟制裁俄羅斯「網路研究局」，公開15個姓名與相關活動。[25] 美國採取的經濟與法律之報復行動，揭露有關惡意網路行為者身分、所屬企業及從事活動等驚人細節。[26] 此舉顯示，毋須損及機敏情報，美國仍然可解密與公開充分資訊，以追溯惡意網路行為者，並公開說明其所從事的活動。然而美網路司令部如何以攻擊行動讓惡意網路行為者付出代價，相關細節仍鮮少公開。[27]

美網路司令部有能力「在全球各地，連續不斷地大規模與對手競爭並加以挑戰」。[28] 前美國國家安全顧問波頓(John Bolton)在2018年證實，美國當時曾發動網路攻擊行動，以捍衛美國選舉的嚴整性。[29] 2019年，中曾根上將於參議院軍事委員會中聲明，網路司令部已讓俄羅斯付出代價，並「改變其對未來行動的風險算計」。[30] 美國國家情報總監所解密的情報，說明俄羅斯於2018年影響美國大眾認知的惡意活動，評估俄羅斯情報單位「並未如上次美國總統大選，長期滲透美國選舉基礎設施」。[31] 美國國防部新聞消息報導，網路



2021年11月29日，第62網路中隊戰力發展管理士史樂米(Robert Sleme)上兵，於科羅拉多州巴克利太空軍基地維護硬體設施，以確保教學訓練成效。
(Source: US Space Force/Andrew Garavito)

司令部曾於2020年總統大選發動超過2,000次的行動。[32] 公開紀錄顯示，美國網路戰力在捍衛近期美國選舉方面，發揮了嚇阻惡意網路活動的效果，然相關細節及嚇阻影響力皆屬機密。

相較於美國司法部與財政部所宣布的消息，美網路司令部網路空間攻擊行動卻沒有足夠的細節資料能得知其影響及目標。限制透明度其中的一個理由，是為了將情報或能力洩露的機率降至最低。然而透明度不足，也限縮了惡意網路行為者瞭解美國網路戰力對其利益所構成威脅的必要資訊。雖然保持秘密，但網路司令部的行動仍提供兩項重要觀察心得。第一是在可接受風險的條件下，網路司令部運用網路攻擊能力獲取網路戰果對抗惡意網路工具或手段。第二是網路司令部具有極多之手段，使惡意網路行為者付出代價——換言之，其能執行大規模網路攻擊行動。考量具備此種戰力，透明度該有多重要呢？

透明度可以提供成功嚇阻所需之訊息傳達。公開揭露追溯特定惡意網路活動及其後果的資訊。此舉可以傳達針對不可容忍行為在網路空間將遭受直接報復的可靠威脅訊息。如此可展現美國有能力讓惡意網路行為者付出重大代價，以及反制特定惡意活動的決心。此項概念運用嚇阻理論，並落實政府與學界的建議事項。若持續努力，透明網路嚇阻將可樹立正當性並符合美國戰略指導方針，以形塑全球行為規範。

透明網路嚇阻

透明網路嚇阻結合網路戰力運用與資訊揭露(亦即透明度)，以事後行為公開宣布的方式，說明所招致報復的活動、特定目標與其正當性，以及行動的成果等。鎖定惡意行為者網路空間資產(例如數位基礎設施及帳號等)，使網路空間攻擊行動付出代價，也可直接影響惡意網路活動的成本獲益考量。揭露資訊可使能力與意願等資訊具有可信度。此種做法能將破壞、危機升級及錯誤認知降至最低，同時使採取行動前深思是否值得。單靠網路空間的效

果很難影響網路行為者的決心，因為網路空間本身的能見度原本就不高。

毫不模糊地揭露網路空間效果，可傳達己方將會使用能力的企圖，同時讓各種不同的行為者預判會付出代價。透明度亦可樹立正當性，記錄特定行為者之行動。針對威脅國家利益(諸如重要基礎設施)的特定活動，採取一致性報復作為，可以傳達絕不容忍這些活動的訊息。網路空間報復活動不太可能嚇阻所有惡意性活動，諸如網路間諜行為等。因此揭露資訊是對無法容忍之活動採取正當報復行為、形塑國際行為規範及確保嚇阻可信度的必要條件。

分析

透明網路嚇阻的能力、可信度及訊息傳達，可以促進美國與夥伴國建立一套透明系統，使惡意網路行為者承受符合比例的後果，以形塑全球網路空間規範。針對合宜性、可接受性、可行性及風險的分析顯示，透明網路嚇阻可以發揮效用。合宜性分析可探討能力、可信度及訊息傳達如何由美國與夥伴國建立一透明系統，使惡意網路行為者承擔符合比例的後果，以利於網路空間落實並形塑全球行為規範。可接受性分析置重點於遭受損害、意外效應、危機升級及符合道德原則與夥伴實踐等方面的風險。可行性分析評估美網路司令部因應溯源、情報、計畫及執行透明化連續行動的各項需求事項，如此可消弭遭受損害、意外效應及危機升級等方面的風險，且在道德條件上非常適合跨部會及國際夥伴國間之合作，並能幫助網路司令部在溯源、情報及計畫方面之能力。

合宜性：網路攻擊能力可以讓人付出代價，扭轉惡意網路活動的成本獲益計算。美國「網路基礎設施安全局」(CISA)估計，每次意外網路損害包含直接支出、金錢損失及經營受阻等項目，損失概估數值為5萬6,000至190萬美元。[33] 此規模的代價使多數惡意網路活動承受財務上的損失。[34] 中曾根上將讚許美網路司令部削弱惡意網路行為者，以及其獲致決定性成果方面的能力。[35] 網路攻擊擾亂營運、造成直接損害、導致昂貴的修復與設備更換，以及信譽損失(例如，被迫掩飾)。但嚇阻真正重要的目的是使之預判相關後果。

美國聯邦調查局及歐洲刑警組織(Europol)所公布的消息，都會附加近期瓦解惡意網路活動的網路空間行動。2020年某次網路空間行動就遏止了自2016年以來猖獗的「高階」殭屍網路Trickbot。[36] 研究人員回報Trickbot活動降低了68%，但判斷這只是暫時性效果，若欲建立持久性嚇阻，必須針對其數位基礎設施進行打擊，同時公布行為者的相關資訊。[37] 2021年1月，歐洲刑警組織宣布在八個國家採取行動，重創網路犯罪鏈Emotet的網路基礎設施，此一行為者就是2020年攻擊美國各州與其地方政府的幕後主謀。[38] 由於Emotet變得「更慎選攻擊對象」，因此研究人員判斷其網路滲透率降低80%，且採取許多前所未有的調整。[39] 2021年4月，在俄羅斯網路犯罪集團使用勒索軟體攻擊「殖民管線公司」(Colonial Pipeline)後不久，美國聯邦調查局宣布，某項網路行動直接從「黑暗面」駭客組織取回價值230萬美元的加密貨幣。[40]

據報導指出，「黑暗面」的基礎設施遭到嚴重

打擊，且因為其附屬組織與之保持距離，該組織遂宣布將避免攻擊公共目標。[41] Trickbot、Emotet及「黑暗面」後來雖然展現各自不同程度的韌性，但執法機關的行動仍降低其復原後活動的範圍與規模。這些個案顯示，網路空間採取透明化方式反擊，對於讓網路行為者的資產付出代價，以及左右各種行為者的決策至關重要。較強的嚇阻力量需要讓人付出超越短暫失能的代價。美網路司令部可以讓人付出此種代價，且將此種力量與透明度結合，使長期藉行動與國家保護而得利的惡意網路活動行為者，判斷若其遭鎖定後將承受更大的代價。

透明度必須克服網路空間既存的不確定性、匿名性及混沌性等問題。針對各種具有限能見度之新興軍事科技的研究發現，能力的運用是傳達威脅訊息最不含糊的方式。[42] 網路攻擊能力的運用可以展現技能，而公開揭露則可克服認知上的挑戰。公開宣示可對其他行為者造成有效威脅、造成聲譽損害，同時降低其淡化、否認或操弄事件的成功機率。[43] 公開網路報復行動的第一手消息，可使後果與特定惡意活動產生連結，並促成所望的行為規範。

2021年11月7日，第919特種作戰通信中隊無線電頻率技術士瓦利(Icy Walley)上兵，於佛羅里達州杜克基地連接天線纜線至鞭形天線。

(Source: USAF/Michelle Gigante)

透明網路嚇阻可形塑全球網路空間行為規範，相關規範則是對可接受行為的普遍期待。世界銀行報告指出，在有堅強領導、責任制度及正當性的條件下，志願性政府結盟關係可使某些議題公開揭露而培養出全球行為規範。[44] 相關且可靠的證據是建立可接受性及獲得支持的關鍵要素。[45] 公開揭露可透明化相關後果及惡意活動，以促成對於構成合法報復之無法容忍行為的全球論述。2019年，美國負責國際安全暨防止核擴散的助理國務卿福特(Christopher Ford)在歐盟致詞中提及：

> 對於規範的瞭解有助於確定負責任國家在應處網路空間惡劣行為方面的政策選項—此即為規範性公約落實要求規範的方式。後果的議題是同道國家新興的合作領域，而這點正是美

國『國家網路戰略』所要求的事項。[46]

揭露訊息可展現嚇阻能接受的攻擊能力，更鼓勵志同道合國家做出類似貢獻。

Trickbot與Emotet行動的透明化，使違法者承擔後果的志願性聯盟得以建立。微軟公司協同全球電信大廠，取得對Trickbot採取更多打擊行動的法院命令。[47] 歐洲刑警組織對Emotet採取的報復行動，正是安全機關在八個國家所採取的網路空間行動、執法作為及公開宣布訊息，以提高違法者所付代價的典型例證。學者史帝文斯(Tim Stevens)在其針對嚇阻與網路空間行為規範的研究中主張，以行為規範為基礎的「嚇阻共同體」可以提高嚇阻的成功機率，並在符合實質利益的條件下，鼓勵權力的行使。[48] 史氏進一步指出，全球規範性框架若無協同一切的可靠力量支持，根本無法嚇阻那些最有可能進行惡意網路活動的非國家行為者。[49] 聯合國「政府資訊暨電信安全專家小組」推論：

志願性、無拘束力的國家行為規範，可降低國際和平、安全與穩定的風險……行為準則反應國際社會的各種期待、建立負責任國家行為的標準、同時讓國際社會可以評估各國的活動及企圖。[50]

以公開方式讓惡意網路行為者負起責任，可以協助同道國的合作關係，同時促成可遏阻無法容忍行為國際體制的建立，同時以累積性方式提高惡意網路行為者所需付出的代價。美國可以運用網路攻擊能力讓違法者承擔嚴重後果，並可透過公開揭露方式，使相關行動成為嚇阻力量，以形塑全球行為規範。

可接受性：揭露網路攻擊行動的傷害及公布有關目標的情報，而不致損及所使用的方法或資訊，確有其可能性。傳統思維認為揭露訊息會損害機敏性之能力。然而，美國聯邦調查局、歐洲刑警組織及美國財政部等機關公開宣布的消息，都證明公開特定目標所須付出的代價，可以滿足公開溯源及合法性的需求，同時還可保護所運用方法與情報管道。同時，美網路司令部為捍衛美國選舉所採取的行動規模，顯示在不損及各種能力條件下，發揮重大效應的能力。最後，事後資訊揭露所公開的資訊，也只不過是原本就會遭到網路攻擊曝光的情報與管道。透明度還可促成更多的風險消弭作為。

透明度可以消弭因為網路空間不確定性及有限能見度所造成的意外效應風險。揭露訊息是對目標對象直接傳達所望效應、針對目標與實際成果，以及哪些活動會遭到報復等事項。如同美國聯邦調查局例證所示，正當性可降低企圖的不確定性，因而降低情勢升級的風險。揭露訊息的其中一項顧慮，是其可能產生溯源錯誤而遭控訴的風險，或是因為聲譽損害之報復行為，此種個案較為適合的做法，應為有限度或私下的傳達訊息。分析專家費舍凱勒及政治學教授哈克內特主張，根本沒有必要恐懼危機升級，因為惡意網路活動早已對國家安全構成挑戰，且網路空間的競爭性互動只會穩定局勢，而非升高風險。[51] 美國在冷

戰時期採取的行動證明，創新的軍事力量運用所傳達之強烈訊息，並不必然會升高危機。[52] 揭露資訊有助於確保觀察者可獲得充分數據以評估美國舉措，包含正當性、目標及行動等可減少不實陳述的證據。

透明網路嚇阻高舉武裝衝突法的必要性、比例性及區分性原則，同時確保適切協調與計畫作為可保護夥伴國利益。對網路行為者實體設施發動網路空間攻擊，同時消除對合法但不知情網路代管服務的間接損害。例如，美國聯邦調查局及歐洲刑警組織所採取的行動，修復僵屍軟體的存取，以及解除使用者裝置遭惡意行為者控制且不致損及代管網路服務公司。密切協調執法機關是確保有關第三方恪遵國際法的根本要件。最後，美網路司令部對各部會應保持密切合作，以鎖定各種目標，並在公布任何消息檢討情報資料前，將意外效應降至最低。透明度亦能鼓勵國際夥伴國評估各種報復手段，同時建立其遵循國際行為規範的習慣。

可行性：美網路司令部及其所屬單位擁有充分能力，可以發揮針對性、比例性及適切程度的網路空間效果，讓惡意網路行為者付出重大代價。該司令部網攻團隊可以削弱、擾亂、摧毀或操控敵手的資訊、系統及網路。[53] 網路司令部下轄一支擁有6,200人的網路任務部隊，包含由網路國家任務小組及網路戰鬥任務小組所組成的網路攻擊部隊。[54] 網路司令部亦擁有多個作戰指揮部。[55] 除此之外，網路司令部與國家安全局位於同一營區，可以獲得美國情報機關的資源，以支援其訊息傳達、創造效果及溯源工作等。[56] 然美國網路司令部行動的公開揭露仍然需要微幅增加人力，以執行計畫與協調資訊公布等事宜。

藉由這些資源，美網路司令部擁有充分力量嚇阻惡意網路行為者。歷史學者華納(Michael Warner)針對該司令部的網路攻擊能力提供摘要說明，自2016年伊斯蘭國極端組織的社群媒體顛覆活動，到2018年以「全新層次」的規模與範圍，鎖定干預美國大選行為者。[57] 捍衛美國2018及2020年選舉的行動，證明其追溯惡意網路活動及執行適切規模行動之能力。[58] 中曾根上將對美網路司令部讓惡意網路行為者付出針對性代價的能力提出保證。[59] 簡言之，網路司令部擁有計畫、情報及組織，能造成不同程度的效應使惡意網路活動承受適切後果，以及具備追溯重要網路活動的資源。

風險：公開揭露資訊可以降低損害風險、意外效應及危機升級等情事。但是仍有解密情報不足或報復選項太少的風險。絕大多數網路空間攻擊行動公開揭露資訊的早期計畫作為，可以獲得最多的未來選項。針對性報復行動可創造遠超過惡意網路行為者成本獲益門檻的最佳機會。雖然此舉需要大量資源，但即使是偶爾展現能力，亦能左右敵手的決策行為。最後，跨部會協調以消弭情報互惠與政軍的風險，仍是一項重要需求。最終，更大的風險在於姑息惡意網路行為者，放任其繼續採取各種活動破壞美國經濟。

影響層面：執法與經濟行動雖然具有力量，但卻無法以足夠高的代價嚇阻惡意網路行為者，尤其是那些不在法律管轄範圍內的對象。美國聯邦調查局及歐洲刑警組織以公開宣布詳細說明具體代價及有關惡意網路行為者的具體情報，在打

2022年6月16日，第103空中管制中隊官兵於康乃迪克州奈提克所舉行的2022「網路洋基演習」，擔任藍軍通信連絡官。
(Source: Air National Guard/David Pytlik)

擊重大勒索軟體行動展現其成果。兩大機關成功運用多國、公營—民間嚇阻團體打擊網路犯罪者，卻未曾損及機敏情報或能力。然而網路犯罪者仍持續在某些國家支持下賺取報酬與利益，不斷重新適應並學習如何躲避法律追緝。針對重要基礎設施及其他國家安全利益所進行的惡意網路活動，應讓違法者面對更嚴重的後果。

美軍的網路空間行動應直接針對網路行為者的網路空間設施施以無比高昂之反制代價，來處置無法容忍的惡意網路活動。此種行動可以傳達強烈訊息，讓違法者瞭解進行威脅美國及其盟國利益的惡意網路活動，絕不符合成本效益。美網路司令部的各項作為應能輔助司法及其他反制措施、鎖定最重大的惡意網路行為者，藉威脅其重要基礎設施、選舉，或是其他國家利益，以增加惡意網路活動可能付出的代價(亦即，絕非僅予以癱瘓)。

透過網路嚇阻可以創造各種

機會，維護資訊環境的各項優勢。運用網路攻擊能力以適切、透明的方式使違法者面對各種後果，可以在網路空間發揮網攻的相對優勢、迫使目標對象在所有地方處於守勢，同時嚇阻其他惡意網路行為者傚优。揭露資訊可以掌握主動，取得正當報復行為的話語權。其可公開說明美國所採取的行動，以證據顯示必須對惡意網路行為者進行報復。資訊公開可以削弱行為者捏造其他故事，並淡化所承受後果的能力。如前所述，報復使其付出的代價必須沉重，同時預告還有後續調查及復原等重大第二波效應。網路攻擊能力是讓不易受外交、司法或經濟行為影響的網路行為者付出代價之手段。除此之外，若展現克制或保留的手段選項，對聲譽損害相當重要時，公開揭露資訊的一致性可提供私下對某些敵手傳達訊息的能力。不僅如此，透明度還能鼓舞志同道合盟國在網路空間恪遵可接受行為。此舉將可營造一個有決心與能力讓惡意網路行為者付出代價的嚇阻共同體。

結語

惡意網路行為者違法妄為卻不受懲罰，盡享網路空間的廉價益處且往往得到某些國家的支持。惡意網路活動的累積性效應已威脅國家安全。針對國家利益所進行的惡意網路活動，諸如攻擊重要基礎設施等，應讓其承受更嚴重後果。戰略家李德哈特曾說過：「誤以為侵略行為可以收買，不論是就個人或國家而言，都是非常愚蠢的事情……侵略行為只能加以阻止。侵略者對於武力的迷信，使其更容易感受堅強對抗武力的嚇阻效果。」[60] 網路攻擊能力是讓網路行為者付出代價的手段，而這些人越來越敢抵抗外交、法律或經濟手段。運用網路攻擊能力，美國可以改變此類行為者的成本獲益決策，同時形塑國際行為規範。

近年網路空間行動顯示，美國可以確實追溯惡意網路活動，藉網路攻擊能力使違法者承擔嚴重後果，以及藉審慎考量的大眾訊息傳達，將這些行動轉化為嚇阻力量。透明網路嚇阻將透明度與網路攻擊能力結合，讓進行惡意網路活動行為者付出沉重代價。藉由公開相關後果、行為者及其活動的證據，可發揮攻勢作為在網路空間的相對優勢，迫使報復對象必須四處防備。此種證據很難加以忽略，因而能影響其他行為者的成本獲益決策。高昂代價報復行動的期望值，正是嚇阻惡意網路活動範圍與侵略性的必要手段。

透明網路嚇阻可以落實美國戰略指導方針、運用訊息揭露將嚇阻可信度發揮至最大，並將網路空間行動既存風險降至最低；同時亦可形塑網路空間行為規範。美國必須展現網路攻擊能力，以左右惡意網路行為者的成本獲益決策。一套透明的做法，也可在盟國間宣揚論述、推動國際行為規範，以及對欲藉攻擊美國及其盟國與夥伴國進而達成符合成本效益之惡意網路行為者及其協力對象等，造成戰略兩難之局面。

作者簡介

Ryan Tate中校以本文獲得2022年美國參謀首長聯席會議主席論文獎。

註釋

1. *Cost of a Cyber Incident: Systematic Review and Cross-Validation* (Arlington, VA: Cybersecurity and Infrastructure Security Agency [CISA], 2020), 11, available at <https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_ Incidents_Study-FINAL_508.pdf>.
2. Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime* (Washington, DC: Center for Strategic and International Studies, 2020) 3, 27–32, available at <https://www.csis.org/analysis/hidden-costs-cybercrime>.
3. *National Cyber Strategy of the United States of America* (Washington, DC: The White House, 2018), 3, available at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy. pdf>.
4. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019), 12.
5. Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, eds., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, Newport Paper 45 (Newport, RI: U.S. Naval War College, 2020), 35–36.
6. Nakasone, "A Cyber Force for Persistent Operations," 10–11.
7. Smith and Lostri, *The Hidden Costs of Cybercrime*, 4.
8. Michelle Nichols, "North Korea Took $2 Billion in Cyberattacks to Fund Weapons Program: UN Report," Reuters, August 5, 2019, available at <https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX>.
9. *Black-Market Ecosystem: Estimating the Cost of "Pwnership"* (London: Deloitte, December 2018), 21, available at <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf>.
10. *Internet Crime Report 2020* (Washington, DC: Federal Bureau of Investigation, Internet Crime Complaint Center, 2020), 3, available at <https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf>.
11. Schneider et al., *Ten Years In*, 49.
12. "FBI Strategy Addresses Evolving Cyber Threat: Director Wray Emphasizes Closer Partnerships to Combat Cyber Threats and Impose Greater Costs to Cyber Actors," video, 16:47, Federal Bureau of Investigation, September 16, 2020, available at <https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620>.
13. Angus King and Mike Gallagher, *United States of America Cyberspace Solarium Commission Report* (Washington, DC: Cyberspace Solarium Commission, 2020), 26–34, available at <https://www.solarium. gov/>.
14. "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats," Department of State, Office of the Coordinator for Cyber Issues, May 31, 2018, available at <https://2017-2021.state. gov/recommendations-to-the-president-on-deterring-adversaries-and-better-protecting-the-american-people-from-cyber-threats/index.html>.
15. *Final Report of the Defense Science Board Task Force on Cyber Deterrence* (Washington, DC: Department of Defense Science Board, 2017), 1–7, available at <https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf>.
16. Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017), 44–71.
17. Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010), 102–135. 古德曼 (Will Goodman) 曾擔任佛蒙特州參議員雷希 (Patrick Leahy) 及美國國防部國土防衛暨全球安全助理部長的顧問。
18. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (May 2017), 381–393.
19. Mariarosaria Taddeo, "The Limits of Deterrence Theory in Cyberspace," *Philosophy & Technology* 31, no. 3 (October 2018), 339–355.
20. *Interim National Security Strategic Guidance* (Washington, DC: The White House, 2021), 9, 18.
21. Ibid., 18.
22. *National Cyber Strategy*, 21.
23. "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," press release, Department of Justice, July 19,

2021, available at <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>.

24. "Treasury Sanctions Russia with Sweeping New Sanctions Authority," press release, Department of the Treasury, April 15, 2021, available at <https://home.treasury. gov/news/press-releases/jy0127>.
25. "Russian National Charged with Interfering in U.S. Political System," Department of Justice, October 19, 2018, available at <https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system>; "Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities," press release, Department of the Treasury, December 19, 2018, available at <https://home.treasury.gov/news/press-releases/sm577>.
26. "Sanctions Related to Significant Malicious Cyber-Enabled Activities," Department of the Treasury, available at <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities>.
27. "U.S. Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise," press release, U.S. Cyber Command, April 15, 2021, available at <https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/>.
28. Nakasone, "A Cyber Force for Persistent Operations," 12.
29. "John Bolton on National Security Strategy," C-SPAN, video, 57:36, October 31, 2018, available at <https://www.c-span. org/video/?453856-1/john-bolton-discusses-national-security-strategy&start=1573>.
30. General Paul Nakasone, Commander of U.S. Cyber Command, *Statement Before the Senate Armed Services Committee*, 116th Cong., 1st sess., February 14, 2019, available at <https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf>.
31. *Foreign Threats to the 2020 U.S. Federal Elections: Intelligence Community Assessment* (Washington, DC: National Intelligence Council, declassified March 10, 2021), 3, available at <https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf>.
32. David Vergun, "Cybercom's Partnership with NSA Helped Secure U.S. Elections, General Says," March 25, 2021, *DOD News*, available at <https://www.defense.gov/Explore/News/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/>.
33. *Cost of a Cyber Incident*, 9–16.
34. *Internet Crime Report 2020*, 3; *Black-Market Ecosystem*, 21.
35. Nakasone, "A Cyber Force for Persistent Operations," 11.
36. "Attacks Aimed at Disrupting the Trickbot Botnet," *Krebson Security*, October 2, 2020, available at <https://krebsonsecurity. com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/>.
37. Adam Kujawa et al., *State of Malware Report 2021* (Santa Clara, CA: Malwarebytes Inc., 2021), 18, available at <https://www. malwarebytes.com/resources/files/2021/02/mwb_stateofmalwarereport2021.pdf>; "Recent Trickbot Disruption Operation Likely to Have Only Short-Term Impact," *Intel471*, October 13, 2020, available at <https://intel471.com/blog/trickbot-disruption-microsoft-short-term-impact/>.
38. "World's Most Dangerous Malware Emotet Disrupted Through Global Action," press release, Europol, January 27, 2021, available at <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>; National Cyber Awareness System, "Alert (AA20-280A): Emotet Malware," CISA, October 24, 2020, available at <https://us-cert.cisa.gov/ncas/alerts/aa20-280a>.
39. "Collaborative Global Effort Disrupts Emotet, World's Most Dangerous Malware," *Check Point*, January 28, 2021, available at <https://blog.checkpoint.com/2021/01/28/collaborative-global-effort-disrupts-emotet-worlds-most-dangerous-malware/>; Kujawa et al., *State of Malware Report 2021*, 18.
40. "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," press release, Department of Justice, June 7, 2021, available at <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

41. "The Moral Underground? Ransomware Operators Retreat After Colonial Pipeline Hack," *Intel471*, May 14, 2021, available at <https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>.
42. Evan Braden Montgomery, "Signals of Strength: Capability Demonstrations and Perceptions of Military Power," *Journal of Strategic Studies* 43, no. 2 (2020), 317–324.
43. Nye, "Deterrence and Dissuasion in Cyberspace," 48, 60.
44. Johanna Martinsson, *Global Norms: Cre-ation, Diffusion, and Limits* (Washington, DC: World Bank, Communication for Governance and Accountability Program, 2011), 4, 8, avail-able at <https://openknowledge.worldbank. org/bitstream/handle/10986/26891/649860WP00PUBLIC00Box361550B0GlobalNorms.pdf?sequence=1&isAllowed=y>.
45. Ibid., 22.
46. Christopher Ashley Ford, "Rules, Norms, and Community: Arms Control Discourses in a Changing World," remarks by Assistant Secretary of State for International Security and Nonproliferation to the European Union Conference on Nonproliferation, Brussels, December 13, 2019, available at <https://2017-2021.state.gov/rules-norms-and-community-arms-control-discourses-in-a-changing-world/index.html>.
47. "Trickbot: U.S. Court Order Hits Botnet's Infrastructure," *Threat Intelligence*, Symantec Enterprise, October 12, 2020, available at <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption>.
48. Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33, no. 1 (2012), 148–170.
49. Ibid., 165.
50. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (New York: United Nations General Assembly, July 22, 2015), 7, available at <https://digitallibrary.un.org/record/799853?ln=en>.
51. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review* (2019), 267–287.
52. Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review* 3, no. 2 (Spring 2020), 94–109, available at <https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/>.
53. Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), II-7.
54. "Cyber Mission Force Achieves Full Operational Capability," U.S. Cyber Command, May 17, 2018, available at <https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/>.
55. "A Command First: CNMF Trains, Certifies Task Force in Full-Spectrum Operations," U.S. Cyber Command, June 7, 2021, available at <https://www.cybercom. mil/Media/News/Article/2647621/a-command-first-cnmf-trains-certifies-task-force-in-full-spectrum-operations/>.
56. Michael Warner, *U.S. Cyber Command's First Decade*, Aegis Series Paper No. 2008 (Washington, DC: Hoover Institution, 2020), 9, available at <https://www.hoover.org/research/us-cyber-commands-first-decade>; "Joint Statement on Advancing State Behavior in Cyberspace," Department of State, September 23, 2019, available at <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace>.
57. Warner, *U.S. Cyber Command's First Decade*, 14–18.
58. General Paul Nakasone, *Posture Statement Before the Senate Armed Services Committee*, 117th Cong., 1st sess., March 25, 2021, available at <https://misi.tech/docs/Nakasone_03-25-21.pdf>.
59. General Paul Nakasone, *Statement Before the Subcommittee on Intelligence and Emerging Threats and Capabilities, House Armed Service Committee*, 117th Cong., 2nd sess., March 4, 2020, available at <https://www. congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf>.
60. Basil H. Liddell Hart, *Strategy*, 2nd ed. (New York: Penguin, 1991), 359.