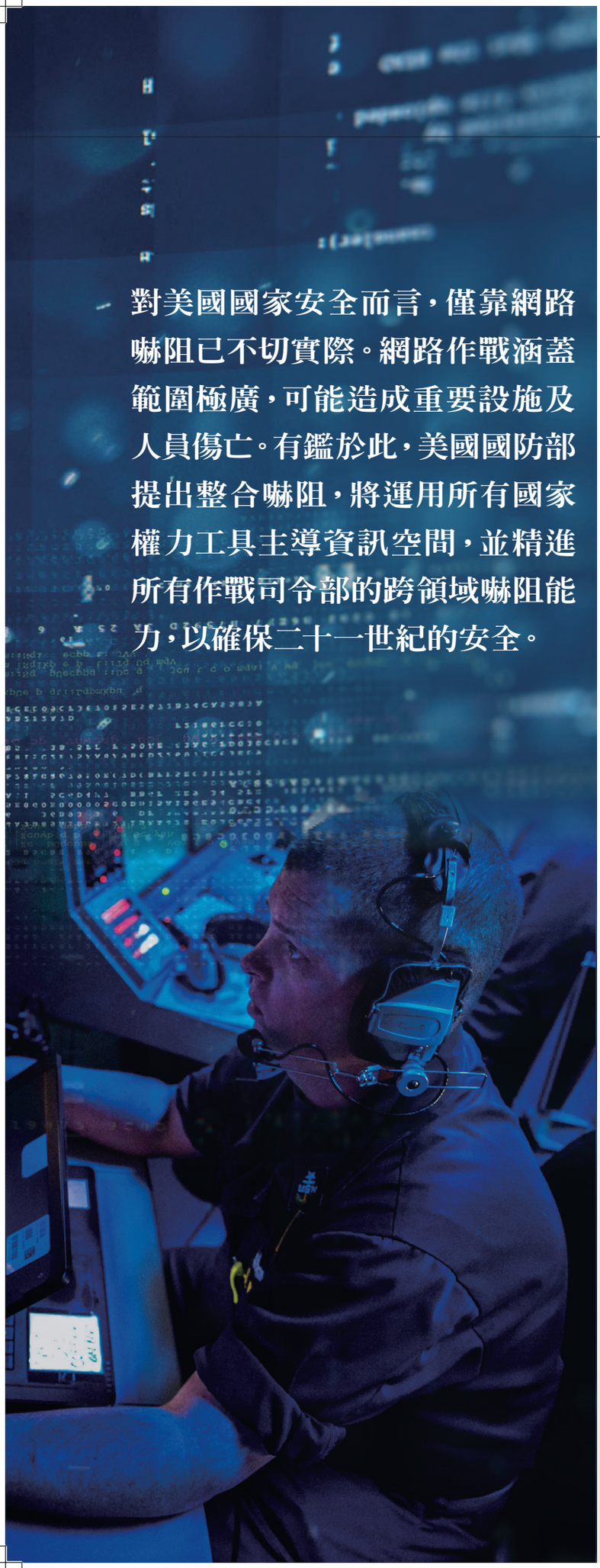
作者/James Van de Velde　譯者/李永悌　審者/丁勇仁

獨木難支：網路嚇阻

Cyber Deterrence Is Dead!
Long Live "Integrated Deterrence"!

取材/2023年第2季美國聯合部隊季刊(*Joint Force Quarterly*, 2nd Quarter/2023)

(Source: USN/Edward Guttierrez III)



對美國國家安全而言，僅靠網路嚇阻已不切實際。網路作戰涵蓋範圍極廣，可能造成重要設施及人員傷亡。有鑑於此，美國國防部提出整合嚇阻，將運用所有國家權力工具主導資訊空間，並精進所有作戰司令部的跨領域嚇阻能力，以確保二十一世紀的安全。

美國國會、部分戰略專家及眾多學者對網路嚇阻(Cyberspace Deterrence)的要求顯得極度不切實際。[1] 其中有許多人士要求美國防部(Department of Defense, DOD)完全運用干擾敵方電腦程式碼的簡單威脅來阻止敵方軍事/影響作戰(Influence Operations)，或是竊取美國的智慧財產(Intellectual Property, IP)，並儘可能破壞敵方軍事系統或民用基礎設施的功能。惟此種戰略思維實在過於天真，因為此類威脅並不足以確實阻止惡意的網路活動，而且這些活動程度上往往並未達到武裝衝突。[2]

各級指揮官遂行網路作戰(Cyberspace Operations)[3]「以保護網路空間的行動自由、完成聯合部隊指揮官的目標、阻滯敵方的行動自由，並促成其他作戰活動」。[4] 惟網路作戰並非魔法，而嚇阻行動亦非幻術。儘管報復行動(亦即懲罰)在程度上必然略大於初期行動，但仍必須合乎比例；不符比例的行動恐將引發報復。(例如，由於中共竊取了谷歌[Google]的原始碼、美國人事管理局[Office of Personnel Management]的資料、部分國防科技，或是即將推出的蘋果智慧手機設計，美國國防部因而無法關閉位於中國大陸的電網或飛航管制系統。)

網路作戰涵蓋的領域相當廣泛，從對網站的輕微干擾及網路釣魚攻擊獲得資訊(亦即間諜活動)，到破壞諸如電網、水壩、淨水設施、選舉系統、飛航管制、通信網路等重大基礎設施的功能皆有，並可能在許多情況

2021年10月8日，美軍聯合部隊指揮部網路部門–空軍(Joint Force Headquarters Cyber–Air Force)第800網路防護小組組長，於英國皇家空軍費爾福基地(Royal Air Force Fairford)的第9遠征轟炸中隊B-1B槍騎兵(Lancer)轟炸機前拍攝宣傳照。(Source: USAF/Colin Hollowell)

下造成大規模的二次傷亡(Secondary Casualty)。

惟正如海上或空中嚇阻一樣，美國國防部無法透過網路嚇阻影響敵方在網路領域的所有行為。例如國防部無法以威脅俄羅斯軍事據點或各大城市進行空中嚇阻攻擊，來中斷俄羅斯對烏克蘭分離主義分子的支援。海上嚇阻也是如此：期待僅威脅以海上載臺進行懲罰，即可改變中共對臺威脅或其建島/主權擴張活動，是不可採信之事。同樣地，希望僅以威脅透過網路空間進行懲罰，即可阻止俄羅斯的混合戰(Hybrid Warfare)或間諜活動，或阻止中共的影響作戰或智慧財產權竊取，都是錯誤的想法。這些活動在程度上未及武裝衝突。有些敵方的網路活動可透過美國的網路作戰進行嚇阻，但有些活動則更難以透過威脅於網路進行懲罰加以嚇阻。

美國通常試圖透過執法機制(起訴個別的俄羅斯或中共網路行為者)或外交照會(Démarche)來阻止對手利用網路空間遂行智慧財產權竊取或影響作戰。總之，美國試圖透過起訴書及

外交抗議等措辭嚴厲的文書，來阻止對手進行未達武裝衝突的惡意網路行動。

截至目前為止，敵方尚未進行任何的「網路珍珠港」(Cyber Pearl Harbor)事件──亦即關閉/攻擊美國重大基礎設施或軍事部隊。[5] 首先，敵方沒有理由在承平時期如此為之。此類攻擊在承平時期沒有任何作用，而且必將遭到美國嚴厲報復，不是網路攻擊，就是實際攻擊。其次，網路嚇阻攸關戰略層級，並且能確實代表一定程度的可信懲罰。一旦敵國關閉了美國的重大基礎設施，例如大部分電網，美國也極可能會關閉該攻擊國的電網，或是其他重大基礎設施，透過網路空間展示美國的戰略嚇阻能力。

總之，網路作戰(分散式阻斷服務[Distributed Denial of Service]、智慧財產權竊取、間諜活動或影響作戰)的規模越小，整個美國政府就越有可能採取不對稱行動進行懲罰。網路活動的規模越大(襲擾參與衝突的軍事部隊、對基礎設施進行戰略網路攻擊)，就越有可能進行對稱(網路)作戰行動。

網路領域是否有所不同？

網路空間裡的競爭每天都在發生。網路武器對基礎設施造成的影響與可能影響絕對真實：這些網路武器可讓武器系統失效，並使重大基礎設施──諸如飛航管制、鐵路、交通號誌、電網、水力發電大壩、淨水系統、大眾媒體網路、通信網路及金融系統等──停止運作或受到干擾。網路武器可能無法輕易殺死大量人員──儘管大規模電網中斷或對航空公司的攻擊可能確實會導致數以百計或千計的人員死亡──但並不代表其效果僅止於擾亂程度。其運用形式可為武裝衝突，並可能影響一國對其武器系統或通信的信心，或影響其補給軍方或照顧平民的能力。如今社會極度依賴電腦系統，成功破壞這些系統將可立即影響人民的日常生活。

美國亦每日疲於應付來自中共、俄羅斯、真主黨(Hizballah)、伊朗、所謂的伊斯蘭國(Islamic State)、蓋達組織(al Qaeda)、塔利班(Taliban)，以及駭客犯罪組織的傳統(即非網路)挑戰。而諸如此類的挑戰皆與網路有關。儘管美國國防部已將網路視為第五個作戰領域(其餘領域分別為陸地、海洋、空中及太空)，但不應將網路作戰視為獨立於其他領域以外的軍事選項。[6] 美國將運用軍事部隊在所有領域以自己選擇的方式與組合遂行自我防禦。因此，儘管網路領域每天都發生敵方活動──而且數量遠高於其他領域，尤其是程度未及武裝衝突的活動──而更加敵對，但其實與其他領域並無不同。

嚇阻的基本原則確實適用於網路空間

嚇阻係以拒止(Denial，防止敵方的攻擊企圖)與懲罰(Punishment，對實施攻擊的攻擊者加諸令其無法接受的成本)為基礎。以往美國的網路嚇阻作為幾乎都是防禦性。若無拒止與懲罰這兩項要素，嚇阻將會不具效力，或以失敗收場。[7]

僅以拒止來遂行嚇阻，終究是不可能的事。受害者將一直處在試圖察覺敵方的存取活動，並阻止專為入侵受害者網路並秘密進行惡意行動所編寫的入侵程式碼的慘況。簡言之，完美的網路

2022年3月21日負責網路與新興科技事務的美國副國家安全顧問(Deputy National Security Advisor for Cyber and Emerging Technology)紐柏格(Anne Neuberger)在白宮記者會期間說明最新情況，指出美國政府憂心俄羅斯政府可能正準備對美國重大基礎設施發動網路攻擊。(Source: Reuters/Leah Millis)

防禦不可能單獨存在，正如對空防禦本身並不足以嚇阻所有來自四面八方的空中攻擊。

而透過成本強加(Cost Imposition)進行嚇阻亦不容易。許多網路應變行動的效果微乎其微，而美國對國際法堅定不移的承諾，使其更難以考慮透過網路空間，實施可能侵犯目標主權或第三方主權的行動。

嚇阻的達成不能僅透過強而有力、具威脅性的公開(宣示性)聲明來實現。透過部署多種具核武能力，並使用強大且數量充裕的指揮與管制網路的武器系統、將核子武器納入更廣大的作戰目標、制定使用此類核子武器的單一整體作戰計畫、在戰區前沿部署美軍部隊作為絆索，以及強力宣示導致衝突的明確與檯面下的紅線等作為，將使核子嚇阻變得更加可信。美國政府最高層經常運用核子部隊；沒有人會懷疑美國的決心。有效的嚇阻必須能同時展現防禦與攻擊能力(例如演習和科技展示)，俾向敵方發出

警訊。

惟核子嚇阻與網路嚇阻之間的差異相當大。就核子嚇阻而言，美國必須阻止的是單一核爆。而就網路嚇阻而言，美國應付的是長久以來持續存在的問題，以及一系列從小規模(影響作戰)到戰略性(基礎設施攻擊)的惡意活動。[8]

在網路領域，美國無法直接在航空展或武器展上對全世界運用或展示其網路能力，因此不會劃定明確的紅線，而是選擇以身作則，不竊取他國專利資訊，或是攻擊另一個國家的基礎設施與重要資源。遺憾的是，美國面臨極為真實的風險，亦即忽視了真正的網路攻擊，例如2014年11月，北韓攻擊新力(Sony)公司，以及2015年4月法國電視國際五臺(TV5 Monde)遭受阻斷服務(Denial-of-Service)攻擊——更遑論中共大規模竊取美國資產及工業的智慧財產權——並稱其為「惡意毀損」(Vandalism)。

規範的建立源自各國相互接受且實行的做法。這些規範成為海洋法(Law of the Sea)、美國在太空的行為，以及在海上面對軍艦的基礎，並進而成為習慣國際法(Customary International Law)。因此，無論曾發出多少次外交照會，只要針對美國的網路入侵懸而未決，就會開始獲得國際社會一定程度的接受。因此，良好的網路嚇阻政策須仰賴國際論壇上以書面形式頒布的國際規範，以及對不可接受的活動進行明確執行且確實廣為周知的因應作為。

成功的嚇阻是建立規範、抑止效益與施加成本的成果。各個軍事領域對作戰皆有不同貢獻；在不同領域行動會有不同的成本與效益。若無法影響此一領域，無論其他國家制定的規範是好是壞，美國最終必然會對此規範有所反應。儘管大多數國家傾向尊重承平時期在陸上、海洋、空中及太空等領域的傳統行為規則，但如今許多利用網路空間的敵人卻視傳統的行為、戰爭及主權規則為無物。

透過所有領域嚇阻動能衝突與惡意網路作戰

網路嚇阻對不同的人而言有著不同的意義。敵方的惡意網路活動不見得要以牙還牙加以嚇阻；其他領域的行動及政府一體做法(包括制裁、公眾關注、外交及民營部門活動)造成的成本強加，都能夠阻止此類行為。同樣地，美國的網路作戰行動也可能會嚇阻敵人在網路領域外(亦即其他領域)的惡意活動。因此，美國嚇阻惡意網路活動時除了運用網路能力，還應該考慮使用動能能力或其他權力工具，同時運用動能與網路能力嚇阻傳統動能衝突。

因此，不應將網路嚇阻界定為網路對網路的行動，而是——像其他所有領域一樣——應納入更廣泛的嚇阻模式中，該模式將涉及所有軍事領域，以及美國政府的外交、執法及經濟部門。鑑於網路是所有領域的命脈，網路作戰亦有助於範圍更大的戰略(動能)嚇阻。能於陸上、空中、海上及太空等領域運用網路能力嚇阻敵人，是至關重要的事。總之，美國必須利用網路作戰嚇阻敵方的惡意網路活動與動能衝突。因此，更有助於理解嚇阻與網路空間的說法，可能就是透過網路空間進行嚇阻(Deterrence Through Cyberspace)。

學術著作使用跨領域嚇阻(Cross-Domain Deterrence)一詞來說明以某一領域的能力對敵方所選擇的行動方案遂行抑制效益或施加成本作為，藉以限制對手在另一領域行為的情況。[9] 能運用所有外交、資訊、軍事、經濟、財務、情報與執法(Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement, DIMEFIL)等國家權力工具的嚇阻戰略，將可跨領域影響現有/潛在敵人的認知與行動，並將產生更完善的嚇阻戰略。

嚇阻與衝突升高

根據定義，對惡意事件的懲罰在程度上必須超過該惡意事件的價值，否則攻擊者將繼續發動此類事件。若攻擊者將面臨無法承受的損害卻仍無所畏懼，則嚇阻將會失敗。故根據定義，以懲罰為基礎的嚇阻具有升高衝突的特質。因此，美國一方面必須規劃對潛在攻擊者施以逐步增加的損害，俾使嚇阻奏效。另一方面，美國對於敵方小型網路行動所造成異常損害，卻也無法加以威脅，因為這些活動僅會造成微小的影響，或是取得少量資料與智慧財產。而對所有領域而言也同樣如此：對海、空域的小規模侵犯，無法透過大規模的動能或網路破壞威脅來加以嚇阻。如此極度不成比例的方式因應，帶來的恐怕不是管控衝突，而是升高衝突，因此並不可靠。

為解決此一現實，美國國防部已展開長期進行的行動戰略：持續執行全方位網路作戰以對抗敵方的活動與目標。持續執行代表國防部將制壓敵方的網路計畫與目標──透過不斷面對網路敵人來阻止敵方對美國重大基礎設施進行智慧財產竊取或影響作戰行動，或部署其能力的企圖。在網路空間中製造此種爭執，將可藉告知網路上敵人其將為惡意活動付出代價，而產生一定程度的嚇阻作用。在此戰略實施之前，美國尚未對未達武裝衝突的活動進行任何懲罰、爭執或採取任何重大抵抗。(既然網路敵人無需為這些活動付出任何代價，而且還能獲得大量利益，那麼他們又有何理由停止惡意活動？)因此，現今的爭執源自於透過網路長期且逐步導入一定程度的嚇阻；持續執行就是實施網路嚇阻作戰。

網路效應(Cyberspace Effects)永遠無法與核武或大規模動能攻擊的效應相提並論。因此，衝突由網路效應升高為核子戰爭的風險很小。截至目前為止，網路效應即便會引起衝突升高，其程度也不大。惟令人遺憾的是，對衝突升高的恐懼導致許多人有錯誤的看法；許多決策者與學者皆畏懼網路作戰，認為此類行動將使衝突升高至動能階段。此種看法不僅違反直覺，也不符合歷史事實。

整合嚇阻

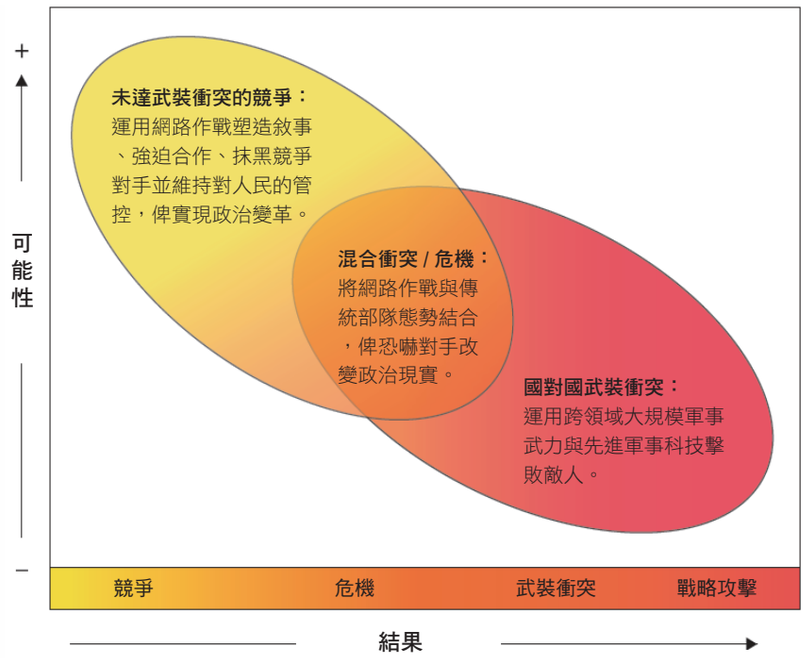
2021年4月30日，美國國防部長奧斯汀(Lloyd Austin)在印太司令部的演說中提到：

> 我們的挑戰在於確保美國在所有潛在衝突領域中長期維持強大的嚇阻能力……我們將利用現有能力建立新能力，並以嶄新的網路化方法──與盟國及夥伴國攜手共同──運用所有的新能力。嚇阻……目前遍及多個領域，必須掌握所有

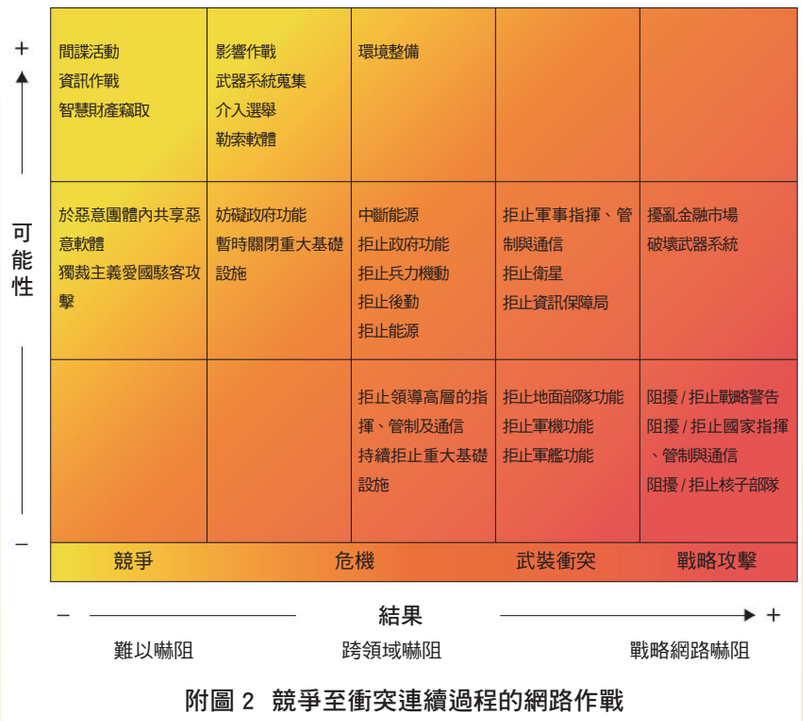
領域，才能確保美國二十一世紀的安全。目前的嚇阻行動要求所有人進行更多的協調、創新及合作。在此種整合嚇阻(Integrated Deterrence)之下，美軍並不一定要獨樹一格，而是要支持美國外交與精進能運用所有國家權力工具的外交政策。

美國需要的是技術、作戰構想與能力三者的正確組合——一種以網路化方式共同交織起，並且可信、靈活、強大到足以另任何敵人望之卻步的組合。美國必須為自己創造優勢，為敵人創造困境。此種真正的整合嚇阻代表以不同的方式運用目前擁有的某些能力。這代表為現有的能力發展出新的作戰構想。而這也代表未來將對所有領域投資量子運算(Quantum Computing)與其他尖端能力。[10]

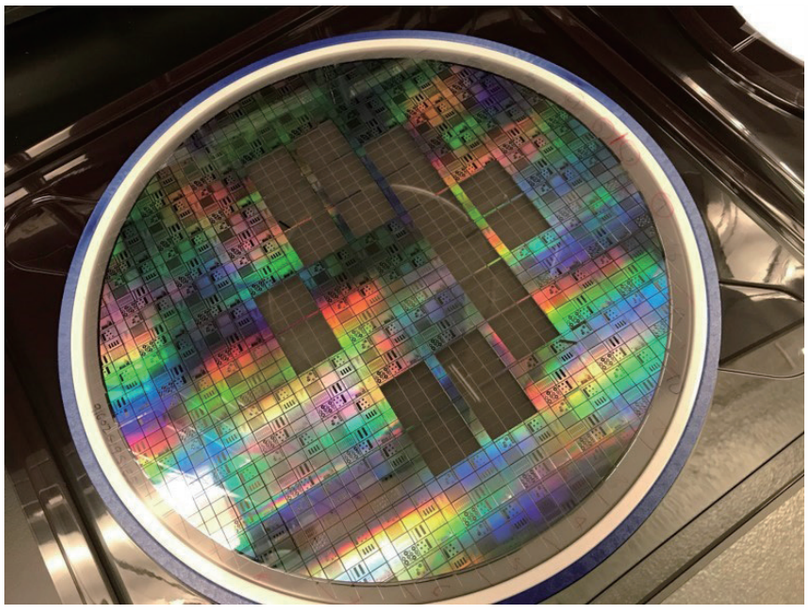
根據奧斯汀的說法，今日的嚇阻將利用所有國家權力(外交、資訊、軍事、經濟、財務、情報及執法)工具，於所有司令部推動跨領域嚇阻，並結合量子運算與人工智慧等新興科技，



附圖 1　競爭至衝突的連續過程



附圖 2　競爭至衝突連續過程的網路作戰



美國應整合作戰構想、尖端科技及現有能力，投注心力研發光子積體電路等量子運算相關科技，方可強化整合嚇阻態勢。

(Source: U.S. Naval Research Laboratory Optical Sciences Division)

俾提供決策優勢。

整合嚇阻之目的在於擴大核子嚇阻模式(Nuclear Deterrence Paradigm)，並透過利用所有國家權力工具、主導資訊空間與精進所有聯合作戰司令部的跨領域嚇阻等作為，來涵蓋所有領域與競爭範圍的嚇阻機制。其中將納入盟國與夥伴國，並運用新興科技與概念。據推測，整合嚇阻可能更須要因地制宜，能針對敵人與狀況想定與解決特定政治環境的嚇阻方法。其目的在支援美國各種國家安全能力，並與之密切合作，同時善加利用盟國與夥伴國的支援。

網路作戰本身不太可能改變敵人在高階武裝衝突中的行為，且各國在此類衝突中將進行大量的動能衝突。此外，敵方在能夠主導衝突(亦即敵方在特定情況下擁有區域傳統霸權)，或其擁有更大政治利益的情況下，將不太可能改採嚇阻行動。惟因網路作戰歷來並未於競爭階段誘使衝突升高，因此可能特別適用於在危機中發出警訊與嚇阻武裝衝突。

於危機中運用網路發揮嚇阻作用

若能在危機爆發初期發揮網路效應，迫使敵人在對抗中付出代價，將可對敵人產生重大影響。改變敵人的成本主張(Cost Proposition)或許可做為衝突升高管控(Escalation Control)的手段。而除了單純的成本強加外──透過展現行動的能力與意願──為敵方的決策帶來不確定性，將產生顯著的嚇阻作用。

若能在衝突升高初期與實際的動態衝突開始之前運用網路效應，其效果可能最為有效。發展一系列動能與網路能力，將可為指揮官提供多種可用於嚇阻敵人，並展現美國降低衝突決心的選項。

網路效應可以逆轉，不會直接破壞基礎設施或造成人員傷亡，且其不會造成實體破壞或生命損失的特質，可作為使敵方保留顏面的退場機制，因此可將其視為較美國國防部現有其他選項更不易升高衝突的選擇。當敵人意識到美國可能已

對其網路發揮影響力，但卻未造成人員傷亡時，即有可能傾向於在危機中緩解緊張局勢。否則，動能式(與公開)的因應作為恐將迫使敵方做出回應。

同樣地，由於網路作戰為非動能式而且可逆，因此可做為較和緩的衝突升高動作，而且比動能選項的風險更小。最高統帥肩負在危機中(Mid-Crisis)選擇最適當行動以實現危機內嚇阻(Intra-Crisis Deterrence)的責任。擁有此類非動能選項，至少可讓最高統帥能在敵人可能認為美國利益尚未面臨危機之時，發出美國利益已面臨一定程度危機的警訊。

因此，大部分的網路作戰行動可能會發生在任何衝突升高的初期，並將在危機階段(武裝衝突之前)發揮最重要的嚇阻作用，同時可能會隨著雙方加強網路防禦與後續產生效用的企圖受阻之後而迅速縮小規模。由於實體基礎設施遭到破壞與開始運用網路防禦措施，這些行動可能將在武裝衝突階段失去效力。以敵武器系統為目標的網路作戰較適合於武裝衝突階段實施，惟在危機階段嚇阻

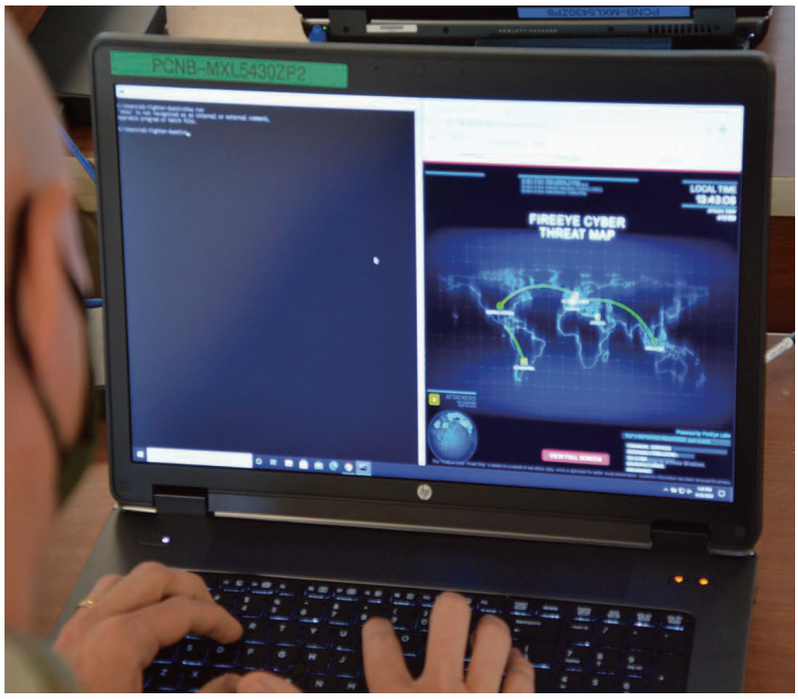
2019年3月8日，沉默獵殺(Tacet Venari)演習期間，參演人員於德國蘭斯坦空軍基地駐歐洲美國空軍區域訓練中心(U.S. Air Forces in Europe Regional Training Center)的訓練狀況。(Source: USAF/Renae Pittman)

敵人或對敵釋放訊息時則幾乎沒有用處。

網路能力可分為透明能力或非透明能力。透明能力可藉由刻意暴露美國的網路存取活動與能力來嚇阻敵人，揭露敵方的網路漏洞並使其失去信心。非透明能力可使敵方承受先發制人的風險，並在必要時支援衝突升高管控。

此外，與非透明網路效應有關的責任歸屬不明(Ambiguity of Attribution)，將進一步限制衝突升高與動能報復的可能性。謹慎運用網路效應，並做到無法直接且明確地對美國究責，將可讓人摸不清誰是此效應的始作俑者。如此一來將使敵人猶豫是否應發起報復性與升高衝突式的因應作為。因此，網路作戰可在衝突發生之前標鎖定非戰鬥目標，以展現問題的利弊得失並表明美國決心，進而使敵方中斷軍事作戰行動的計畫與執行。

網路作戰特別適合在危機或對抗中以不對稱的方式進行，俾產生不可預測性──此為嚇阻的另一項原則。此類行動將表現出美國願意參與問題與揭露敵方意想不到的弱點，同時不會造成重大的實體損害。而對敵方發出的訊息則是：最好在事件升級為動能衝突之前、在施加額外代價前，以及在保留顏面的退場機制排除前停止行動。網路作戰因此是避免大規模衝突的最佳手段。



2020年9月20日，網路之盾(Cyber Shield)20號演習期間，美軍軍職專長代號25D的資訊網路防禦人員(Cyber Network Defender)與賓州國民兵(Pennsylvania National Guard)於賓州印地安城峽堡(Fort Indiantown Gap)演練網路防禦。(Source: Pennsylvania National Guard/Angela King-Sweigart)

因此，若能在危機或衝突初期，透過關閉特定敵武器系統或干擾諸如基礎設施、社群媒體或對國家有重大價值之機構等特定高價值民用(反制價值[Counter-Value])目標等方式遂行網路作戰，進而在敵人心中造成出其不意與懷疑，則網路作戰即有助於避免武裝衝突。此類行動可能因而有助於所有領域的衝突升高管控(跨領域嚇阻)。

一部分美國網路任務部隊(Cyber Mission Force, CMF)應將重點自對稱的網路對網路

(Cyber-on-Cyber)與反制兵力(Counter-Force)選項轉移至戰略嚇阻與衝突升高管控任務。此種轉變將重新平衡網路任務部隊的任務，提供強大的戰略效果，俾支援全球與區域戰略嚇阻及衝突升高管控任務。確保網路任務部隊能在衝突各階段發揮作用：阻止敵方侵略、管控衝突升高，以及在嚇阻失敗的情況下在衝突中取勝；對此而言，任務的重新平衡至關重要。必須慎選敵對目標，才能管制衝突升高，同時不激化水平或縱向升高衝突。

透過網路空間遂行強力嚇阻的先決條件

提供作戰人員強大可靠的網路有助於作戰成功。此種準備工作可透過證明軍事作戰行動將持續進行並且不受潛在敵方網路行動的影響，進而產生嚇阻效果。必須讓敵人相信當其於網路空間採取違背美國利益的行動時，恐將面臨不利的最終狀態。另一方面，一旦潛在敵人得知美軍因網路能力的喪失而無法執行指定任務時，則恐將促使敵人有勇氣持續針對美國國防部網路遂行網路作戰。

由於網路空間是所有領域的命脈，因此不能成為美國國防部行動弱點的來源。強化後的網路能有效抵禦網路攻擊與網路非法運用，故可讓潛在敵人付出更多代價。設計於降級狀態(Degraded States)下運作的韌性網路(Resilient Networks)是遂行嚇阻的先決條件，並可在潛在敵人心中灌輸其行動徒勞無功的想法。

若敵方認為其活動不易遭到偵知而不計後果地採取行動，則嚇阻即無效力可言。因此，正確與及時地發現敵對行為者，對究責敵方的行為或意圖而言至關重要。若敵人知道美國國防部能正確、快速地追究網路空間行動的責任，則將投鼠忌器。因此，究責能力對強大的嚇阻至關重要。為能提升情報與刑事調查能力，必須加強研究與發展。

一旦確定責任歸屬，美國國防部就必須制定適當的政策與權責來防止、或於必要時回應網路空間中的敵對行為。若國防部當局能以迅速、統一的因應作為保護國家，即可嚇阻潛在敵人。

為加強美國國內的網路防禦，美國國防部必須繼續發展與領導國際集體防禦夥伴關係。國際聯盟可額外為國防部提供偵測惡意網路活動的能力，並可阻止行為者在夥伴國的地理區域內建立安全避難所。此外，美國應激勵所有友好的外國政府解決源自其境內的惡意網路活動。

網路能力正迅速演進。為能繼續成為網路空間的關鍵參與者，美國國防部不僅必須採用新興科技，同時還需要發展新能力以增強實力，進而有效增進更大的嚇阻功效。

零組件首先為商業應用而開發，進而再運用於武器系統的情形已日益普遍。全球供應鏈與研究發展流程已開創出各式科技並使其流通──而與此相關的危險是，惡意行為者可能為其戰略目的而試圖轉移或影響供應鏈。美國必須發展出解決美國國防部供應鏈網路遭破壞問題的策略。

於網路空間展示美國國防部的能力與毅力，已成為至關重要之事。國防部必須將其偵察、防禦及應付敵對行為的高超能力宣揚周知，否則嚇阻將無法奏效。戰力展示與軍事演習是常見於實體

領域的兵力展示方法；而無論何時何地，只要可行，也應適時在網路領域進行類似的行動。

因此，美國網路司令部可能需要有更多的工作團隊。充足的兵力將可為美國提供機會、選擇、交叉教育(Cross-Education)、能力共享、存取能力、可信度，以及更多的歷史知識與經驗。當然，透過網路空間進行嚇阻的目標在於避免衝突。有效的網路嚇阻包括辨識敵人，以及為敵方提供退場機制，以避免升高衝突。因此，美國國防部應研究網路部隊的最佳運用方式：於衝突時，網路部隊以對抗敵方軍事系統為目標(此情況可能永遠不會發生)，或在未達武裝衝突時持續運用網路部隊，俾製造爭端與阻撓敵方的影響作戰、竊取智慧財產權、介入選舉及全般資訊作戰等作為。惟就從事上述競爭性任務的網路團隊而言，何者為較佳的運用──或平衡──方式？

結論

為達嚇阻敵方行動之目的，網路作戰已和其他國家權力要素共同成為美國總統的可行選項。網

註釋

1. 例如美國網路空間日晷委員會(Cyberspace Solarium Commission)在其2020年3月11日的最終報告中提出了「分層網路嚇阻」(Layered Cyber Deterrence)戰略。請參見Cyberspace Solarium Commission, available at <https://www.solarium.gov/>. 根據聯戰出版品(Joint Publication, JP)1-02號《美國防部軍事與相關術語辭典》(*Department of Defense Dictionary of Military and Associated Terms*)(Washington, DC: The Joint Staff, November 8, 2010, as Amended Through February 15, 2016)，67頁，嚇阻(deterrence)為「透過以無法接受的反制行動帶來可信的威脅以及/或相信行動的代價超過已知利益等手段來阻止行動」。而網路空間(Cyberspace)則定義為「資訊環境中的全球性領域，此領域係由相互依賴的資訊科技基礎設施與常駐資料網路所組成，其中包括網際網路、電信網路、電腦系統以及嵌入式處理器和控制器等」。 JP 1-02, 58.
2. 請參見Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (Summer 2017), 381–393; Timothy M. McKenzie, *Is Cyber Deterrence Possible?Perspectives on Cyber Power*, CPP-4 (Maxwell AFB, AL: Air University Press, 2017), available at <https://media.defense.gov/2017/nov/20/2001846608/-1/-1/0/cpp_0004_mckenzie_cyber_deterrence.pdf>.
3. 網路作戰(Cyberspace Operations)的定義為「網路能力的運用，其主要目的為於網路空間或透過網路空間達成目標」，JP 1-02, 58。
4. JP 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), ix, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf>.
5. 美國總統政策指令(Presidential Policy Directive)第21號「重大基礎設施的安全性與韌性」(Critical Infrastructure Security and Resilience)指出了對美國政府至關重要的16個重大基礎設施部門，包括：化學，商業設施，通信，重點製造業，水庫，國防工業基礎，緊急服務，能源，金融服務，糧食與農業，政府設施，醫療保健與公共衛生，資訊科技，核反應器、材料與廢棄物，運輸系統，以及用水與廢水系統等。
6. 美國防部並未使用「網路作戰」(Cyber Warfare)一詞，是因為「作戰」(Warfare)是由美國總統與國會決定的政策條件。美國國防部對網路作戰的非官方定義請參見"Joint Terminology for Cyberspace Operations," Office of the Vice Chair of the Joint Staff, 16, available at <https://info.publicintelligence.net/DoD-JointCyberTerms.pdf>: 「全部或部分透過網路手段進行的武裝衝

路領域與所有領域一樣，無法單獨決定衝突的勝負或管控危機。而正如所有的領域，網路領域亦可彌補其他美國國力工具的不足，並協助作戰人員在衝突期間處置軍事目標。惟網路領域可能具有特別強大的跨領域效應，以及其他領域無法提供的危機控管能力。幸好網路效應似乎不會升高衝突──這對涉及網路選項的危機計畫作為而言算是正面的要素。

儘管所有軍事領域可在戰略層級提供一定程度的嚇阻，卻很難在武裝衝突層級以下發揮嚇阻作用。網路領域也不例外。透過不斷接觸利用網路空間破壞國際規範的惡意行為者，將可達網路嚇阻的最佳效果。唯有透過持續執行此種接觸，才能實現任何程度的嚇阻。

作者簡介

James Van de Velde 博士為美國國防大學艾森豪國家安全與資源戰略學院教授。他也是美國國家情報大學副教授，並在約翰霍普金斯大學高級國際關係學院擔任兼任教師。

Reprint from *Joint Force Quarterly* with permission.

突。為阻止假想敵在衝突中有效使用網路系統與武器，而採取的軍事作戰行動。其中包括網路攻擊、網路防禦及網路賦能(Cyber Enabling)行動。」(並非所有網路攻擊都是網路戰，但所有網路戰都是武裝衝突。)

7. 請參見*Deterrence Operations, Joint Operating Concept*, vers. 2.0 (Washington, DC: DOD, December 2006), available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_deterrence.pdf?ver=2017-12-28-162015-337>.
8. 競爭的構想請參見Air Force Doctrine Publication 3-05, *Special Operations* (Washington, DC: Headquarters Department of the Air Force, February 1, 2020), available at <https://www.doctrine.af.mil/portals/61/documents/afdp_3-05/3-05-afdp-special-operations.pdf>.具體而言，關於競爭連續過程(Competition Continuum)，請參見*Special Operations Forces Within the Competition Continuum* (Maxwell AFB, AL: Curtis E. LeMay Center for Doctrine Development and Education, 2020), available at <http://www.doctrine.af.mil/Portals/61/documents/AFDP_3-05/3-05-D03-SOF-Competition-Continuum.pdf>.
9. 請參見Celeste A. Drewien, "Cross-Domain Deterrence" (presentation at U.S. Air Force Academy, Colorado Springs, CO, April 26, 2019), available at <https://www.osti.gov/servlets/purl/1644932>; King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica, CA: RAND, 2018), available at <https://www.rand.org/pubs/perspectives/PE259.html>; Jon R. Lindsay and Erik Gartzke, ed. *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019); Vincent Manzo, *Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?*INSS Strategic Forum No. 272 (Washington, DC: NDU Press, December 2011), available at <https://inss.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf>; Tim Sweijs and Samuel S. Zilincik, "The Essence of Cross-Domain Deterrence," in *NL ARMS Annual Review of Military Studies 2020*, ed. Frans Osinga and Tim Sweijs (The Hague: T.M.C. Asser Press, 2020), available at <https://doi.org/10.1007/978-94-6265-419-8_8>.
10. Lloyd Austin, "Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command," April 30, 2021, Camp H.M. Smith, HI, available at <https://www.defense.gov/news/Speeches/Speech/Article/2592093/secretary-of-defense-remarks-for-the-us-indopacom-change-of-command/>.