● 作者/Michael P. Carvelli ● 譯者/周敦彥 ● 審者/馬浩翔

權責下授：明智的網攻

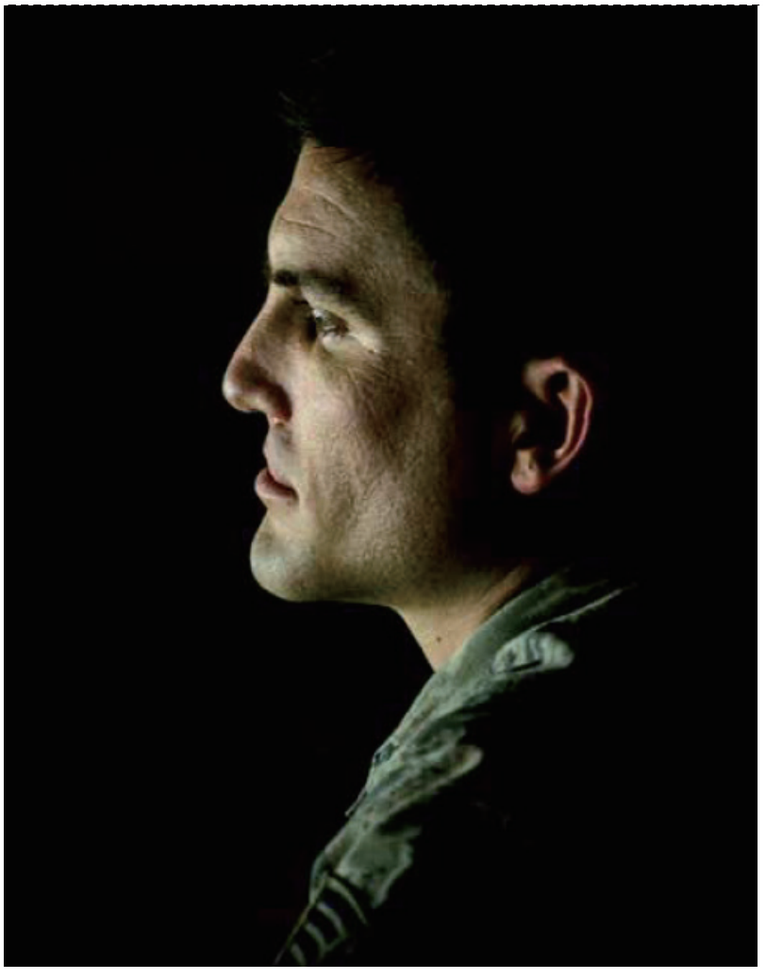
A Smarter Approach to Cyber Attack Authorities

取材/2018年第四季美國聯合部隊季刊(*Joint Force Quarterly*, 4th Quarter/2018)

在網路攻防中，發動攻擊的一方占有優勢，若然將權責賦予作戰層級指揮官，讓其得以發動具可逆效果的有限網攻，就能提供更多軍事行動選項，進而降低作戰成本與人員風險。

對於美國國防部以外的網路，國家最高權力機構擁有全部網路作戰的核准權。想要執行網攻的作戰指揮官，必須呈報需求並取得總統或國防部部長許可。[1] 倘若獲得批准，參謀首長聯席會議主席將授權美國戰略司令部，然後交由網路司令部司令執行。[2] 如此程序效率低落、繁瑣且無用冗雜。作戰指揮官當然會避免使用網攻，因為進行網攻的權限僅限於國家和戰略層級。美國應該將網攻權限下授給作戰指揮官，但要根據攻擊所產生的影響來設定限制。可以肯定的是，很難瞭解所有攻擊後果，但在如此情況下，必須先審慎權衡在網路中先發制人將會取得的重大優勢。國家預先核准網攻的機制，可以確保指揮官能獲得適切攻擊手段，同時也可顧及到國家領導人的擔憂。

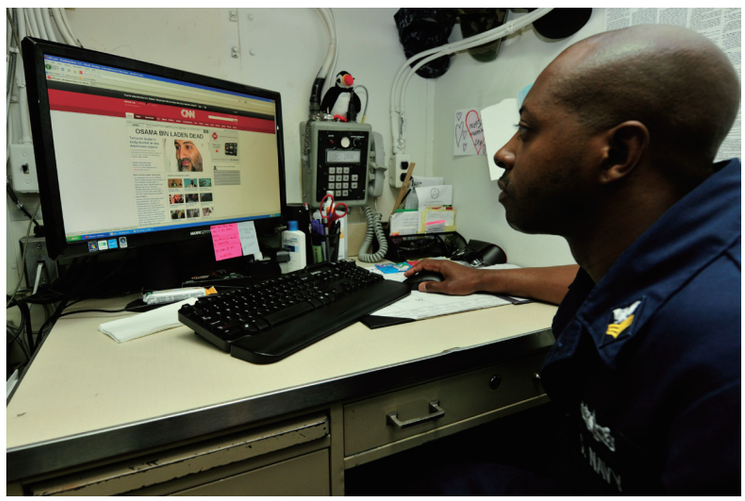
本文旨在說明有限授權網攻將如何使作戰指



2017年6月3日，網路戰人員在馬里蘭州密德河(Middle River)沃菲爾空軍國民兵基地(Warfield Air National Guard Base)的第27網路中隊(Cyberspace Squadron)作戰室監控即時網攻情形。(Source: USAF/J.M. Eddins, Jr.)

揮官遂行有效攻擊，同時減輕意外後果，並針對有限授權網攻提供相關建議。在過去幾年來，部分國防專業人士主張將網攻權限下授至作戰層級。[3] 本文說明下授網攻權限應如何權衡優勢及風險。藉由設定某些限制，將可確保作戰指揮官能安全對敵方發動網攻，並將產生意外後果的風險降至最低。

網路空間是美國國防部運作的最新領域，[4] 由三個層次組成，分別是實體層、邏輯層和網路角色層。[5] 實體層是由網路元素存在的陸地、海洋、空中及太空中的位置組成，包括支援網路的硬體、軟體、系統軟體和基礎設施(有線、無線、電纜線、衛星與光纖)，以及連接器(電線、電纜、無線電頻率、路由器、交換器、伺服器和電腦)。邏輯層由物理網路元件間存在的相互關係所構成(即以多個伺服器建構起一個網站，透過單一全球資源定位器[URL]存取)。網路角色層最為抽象，因為它採用邏輯層規則來開發個人或實體數位表現形式。這三個層次共同構成網路，聚合時就形成網路領域。網路非常複雜，很難在其中精確運用軍事力量，因為此領域是由物理和非物理成分所構成。[6] 此外，網路領域的性質會因無法預料方式而發生微小變化或中斷。[7] 由於網路複雜性及運用網路武器時所面臨風險，執行網攻的決定應該要受到限制。



網路具有即時性與無遠弗屆等性質，能讓使用者在第一時間獲取最新消息。 (Source: USN/Jonathan Sunderman)

近期敵人動向

然而，美國當面之敵已經展現其運用網攻的能力，而且完全不顧慮預期外影響所引發的效應。在過去二十年來，美國的對手在運用網攻方面表現出日益增強的技巧、速度和靈活性。1999年，中共駐貝爾格來德大使館意外遭到炸彈襲擊後，中共駭客攻擊美國政府網站，導致白宮直接關閉其官方網站。[8] 此次攻擊顯示，對手有能力藉由網攻破壞美國政府的系統。

2008年俄羅斯與喬治亞的戰爭中，俄羅斯在進入亞布卡薩(Abkhazia)和南奧賽提亞(South Ossetia)前，先透過網攻癱瘓喬治亞領導人的通信網路。[9] 此次攻擊切斷了喬治亞政府內部大部分通信及對外聯繫，並在喬治亞民眾間製造了恐懼和不滿。除了傳統衝突中有俄羅斯發動網攻外，另在打得不可開交的俄羅斯與烏克蘭間，俄羅斯聯邦安全局還跟私人軟體公司與駭客罪犯聯合攻擊烏克蘭的電網和金融體系。[10] 這種對烏克蘭發動搭配傳統攻勢的混合戰，顯示俄羅斯有意在戰爭和衝突中使用網攻。「伊斯蘭國」在 2015 年發動了一次網攻，當時該組織侵入美國中央司令部的推特帳戶，並發布了一張蒙面武裝分子的照片。[11] 這次攻擊展現了非國家行為者有能力在網路上攻擊美國並達到戰略效果。時任美國中央司令部司令的馬提斯(James Mattis)上將表示，「我們的敵人在網路上運作……進行計畫、協調、招募、訓練、裝備、執行及爭取支持等工作，以打擊[美國]及其盟友的利益。」[12] 明顯可看出，國家和非國家敵人擁有可削弱破壞美國國內外軍事與非軍事行動的能力，因此，國家領導階層此時應賦予作戰指揮官在此新環境中所需要的權限。

2017年2月，在堪薩斯州來利堡(Fort Riley)「危險焦點演習」(Danger Focus Exercise)期間，士兵在支援第1步兵師第2裝甲旅級戰鬥小組時執行網路作戰。(Source: US Army/Alvaro Luna)

當然，完全授權作戰指揮官執行網攻具有風險。網路是由物理(路由器、交換器、電纜)和非物理(軟體、作業系統)等元素組成，而這些元素都在不斷快速變化。同樣地，在執行任務前要完全瞭解網攻的第二層和第三層影響相當困難，聯合特遣部隊可能無法確定各種會發生的反應。

也許最廣為人津津樂道的意外後果是「奧林匹克網攻行動」(Operation *Olympic Games*)一案，更常被稱為「震網」(Stuxnet)蠕蟲。蠕蟲設計者企圖祕密破壞伊朗的離心機；然而，該電腦病毒造成目標無法逆轉的損害。[13] 該蠕蟲自行在全球傳播和複製，並在過程中對工業控制系統造成不可逆損害。雖然據稱美國和以色列透過其最優秀網路團隊聯手製造這種武器，但在釋放前無法完全知悉其所產生的影響。[14] 網路領域的性質──實體層、邏輯層和網路角色層中不斷變化──原本就無法完全瞭解網攻的散播方式。震網是一個國家級網攻的案例，權責單位和設計者是為了特定效果而製造，但是病毒卻意外擴散。

雖然震網提供一個重要的警示教訓，但是相關討論不應就此結束。更平衡的權責區分可以滿足決策者的合理顧慮及美軍需求。有限的網攻權責能確保作戰指揮官達成作戰目標，並避免因為不夠通盤瞭解而鑄下大錯。網攻使其得以獲得優勢，進而加速達成作戰目標。即便在無法知悉所有可能影響的狀況下，指揮官依然需要擁有權責，以有限制方式運用網攻。震網病毒若具有可逆效果，就只會對伊朗的離心機造成預期損害，同時避免導致更多意外

相較於傳統動能武器，可逆性網路武器具備相當大的優勢。(Source: AP/達志)

傷害。在將網攻權責下授給作戰指揮官時，必須要牢記此一經驗教訓：要考慮無法預期的影響。

規劃網攻

設計具可逆效果的網攻是限制作戰指揮官攻擊權責的最佳方法。創造具有可逆效果的網攻是可行的，例如，阻斷服務攻擊可使網站流量超過其處理能量，造成效能降低或暫時失效。而當攻擊者停止超負荷流量時，就會逆轉影響，恢復正常運作。

相較於傳統動能武器，可逆性網路武器具備相當大的優勢。這可以提供其他對象(敵人、盟國、公司或美國政府)逆轉損害的能力，使其能在遭遇非預期傷害時減緩網攻的影響。若能運用可逆轉損害來限制作戰指揮官的權力，則可確保一旦網攻影響達到致災程度(例如核武器指管、國家基礎設施)，還可以設法將對方系統恢復到先前狀態。基於可逆性的有限網攻權責，指揮官能減輕網攻不可預期的擴散影響，同時維持其搶先遂行有效攻擊的能力。作戰指揮官僅被賦予運用可逆效果的權責，使得攻擊所造成的任何意外後果，都能恢復到戰前狀態。

由於目前美國政府最高層級掌握網攻的權限，而授權機制促使指揮官傾向使用動能武器。以下想定說明這兩種武器的核准方式。[15] 使用空中投射的彈藥摧毀建築物，或在路由器上釋放電腦病毒以產生相同的預期效果。要攻擊路由器，指揮官需要獲得總統或國防部部長的批准。反觀作戰指揮官本身就擁有轟炸建築物的權限。此外，基於以下因素，批准動能攻擊的過程相對較短：對於傳統彈藥的「熟悉」、瞭解所產生的附帶損害及標準作業程序。相較之下，欠缺對網路武器的瞭解及需更長核准時間，促使指揮官會預先選擇動能攻擊。因為作戰指揮官有權批准轟炸行動，程序只需幾分鐘，而獲准執行網攻所需時間可能需要數小時到數天之久。前美陸軍網路司令部司令卡登(Edward Cardon)中將強調此觀點時表示，「運用網攻來達成目標不應該比使用動能武器更困難。但目前在某些情況下的確如此。」[16] 有限的網攻權責下授可排除這種選擇偏見，並鼓勵指揮官使用網路武器，因為他們擁有批准網攻及動能攻擊的權力。如果下授某種有限的權力，則作戰指揮官可以在炸彈和病毒間確實做出合理選擇。權責下授讓指揮官得以平等看待建築物和路由器，進而評估每個選項具備的優缺點。這同時也創造了一種環境，讓作戰指揮官不會一直選擇動能而非網路武器。

在明確界定的有限網攻授權範圍內率先攻擊敵人，讓作戰指揮官擁有作戰優勢，且不會造成無法接受的風險。如果設計者在網攻中只製造可逆轉的效果，作戰指揮官就可以搶先攻擊對手，因為其下屬無法改變的可能損害會減少。製造可逆轉網路武器，其效果可降低整體運作上的殘餘風險。因為人性中具有的攻擊本質，很難讓人去預測植入的電腦病毒將如何爆發。[17] 人類製造網路武器，而武器的任何調整都會改變其效果。此外，三個層次(實體層、邏輯層和網路角色層)的任何更改都將影響病毒擴散的方式。這些細微差別造成一旦釋放網路武器，就很難預測其擴散效應。為了解決這個問題，必須對網攻權責加以設

限，只能設計可逆轉效果以降低殘餘風險。如果武器效果擴及預定目標之外，甚至擴散到敵人的商業領域，則這種影響就可以逆轉，從而降低發生廣泛破壞的可能性。

無法完全瞭解網攻的困境，可能會在釋放網路武器後產生不成比例和無差別攻擊等影響。網路作戰和武器可能造成更嚴重的破壞，或在空間和時間上造成影響更為廣泛的後果。[18] 在《武裝衝突法》(Law of Armed Conflict)的規範下使用網路武器，必須要符合有所區別、獨特性和比例原則等前提。作戰指揮官及其參謀須瞭解炸彈對目標建築物影響與這三項要求之間的關係。由於無法完全掌握網路武器的影響，因此與炸彈相比，指揮官必須確定網路武器的附帶損害是可被接受的。設計具有可逆效果的網路武器，可以確保如果預期效果有誤，則下屬就可以控制其效果。運用炸彈就無非如此；一旦飛機投射炸彈，就會造成永久性損害。設計網路武器以產生可逆轉效果，可確保在攻擊敵人時符合有所區別、獨特性和比例原則等要求。

2017年9月8日，第1陸戰隊後勤群第7工兵支援營勤務連士兵，在加州布萊斯(Blythe)參加「深度打擊II演習」(Deep Strike II Exercise)。
(Source: USMC/Timothy Shoemaker)

網攻讓美國能免於承受動能武器造成的破壞成本，亦即重建或修復在衝突中受損的基礎設施。[19] 這種損害的代價可能非常龐大。然而，如果作戰指揮官有權進行有限網攻，相較於使用動能武器摧毀目標，則前者可以降低整體的成本。例如，指揮官可以運用網路武器來破壞電力系統，而不是用動能武器予以摧毀。相較於動能武器的實際毀壞，這使得發動攻擊者能藉由網路手段以更低成本修復損壞。可逆的網攻效果提供動能武器無法比擬的優勢，讓指揮官得以在不永久破壞重要基礎設施的情況下，創造有利條件。因此有限的網攻權責可視為節約成本的手段，但仍取決於預期攻擊的目標。

預先核准的網路權限

就決策者而言，預先核准的權責應該使其在下授更大權力給作戰層級指揮官時，能在某種程度上感到放心與自信，因為這相較於執行動能武器作戰，更能讓國家領導人掌握與控制全局。就美軍和作戰指揮官而言，擁有預先核准的網攻作為手段，能更迅速進行攻擊，並付出最低的生命與

金錢代價。有限的網攻權責增加國家高層可用的選項，而這些人會決定維護國家重要、核心與次要利益的最佳方式。國家高層賦予對軍事行動更大的控制權，有助於軍方實現戰略和政治目標，將網攻權責限制在可逆效果的範圍內，使國家和戰略高層能下決心去接受、轉移、避免或減輕軍事行動的風險。[20] 這種更大控制權的作為之一，就是預先核准能產生可逆效果的特定軍事行動。

國家高層需要預先核准的網攻有下列幾種類型：分散式阻斷服務攻擊、加密攻擊、程式碼混淆攻擊，以及資源欺騙攻擊。分散式阻斷服務攻擊運用成千上萬個被侵入的系統，以迫使網站故障關閉，或是將頻寬、記憶體與處理能力等資源消耗殆盡。[21] 不論用何種方式，攻擊者都會中斷系統，造成網站使用不便甚至難以信任等情形，最後導致伺服器關閉和延遲，直到重新恢復網站服務為止。[22] 加密攻擊透過只有攻擊者知道的加密技術，加密敵方的重要程式，之後攻擊者可將其解密。[23] 程式碼混淆攻擊是以只有攻擊者知道的方式，重新排列電腦系統的軟體和資料。攻擊者決定結束攻擊後，可以將系統重新排列恢復原狀。[24] 資源欺騙攻擊則是以假象損害欺騙對手。[25] 當攻擊者透露並未改變任何事物時，此一欺騙行動就隨著被攻擊者意識到所發生的事情而結束。上述各類型的網攻給予敵方可逆轉損害，可以在攻擊完成後中止殘餘效應。預先核准這些網攻，使國家高層在執行特定軍事行動前能有更完善的監督。

在朝鮮半島的想定中，作戰指揮官可以運用這四種類型的網攻來降低意外後果的風險，並提供各種選項以低於使用動能武器的成本來恢復北韓現有的基礎設施。據信美國網路司令部在2017年運用分散式阻斷服務，對北韓進行暫時且無破壞性的攻擊。[26] 美國網路司令部後來中止了該次攻擊，也沒有造成意外後果。加密攻擊北韓兩家煉油廠，可能會破壞該國的運輸和農業生產。[27] 如果美國使用這種類型的攻擊，將會中斷北韓的石油供應，進而對軍用車輛和糧食生產造成影響。當美國決定停止這種影響時，可以解密中止攻擊，讓石油恢復到正常供應水準。美國也可以使用程式碼混淆攻擊，這可獲得與加密攻擊相同的結果。雖然方法有所不同，但是產生效果相同。最後，如果美國決定動用軍事武力攻擊北韓，就可以使用資源欺騙攻擊。美國可在入侵行動中利用這種手段欺騙北韓軍方。如果美國以資源欺騙做出攻擊北韓基礎設施的假象，則北韓可能會因為誤以為遭受破壞而避開某些路線。這可以提供一個明顯的優勢，就是使用某些路線時，沒有北韓的優勢兵力在附近。所有這些預先核准的攻擊案例都減輕了意外後果，因其皆為臨時且不具破壞性。

預先核准的網攻可降低作戰成本及人員風險，同時增加敵方成本。依賴網路做生意的敵人可能會迅速虧損，耗盡財務資源。從攻擊者的角度來看，執行網攻，諸如分散式阻斷服務攻擊，成本大多不會改變，因為支出經費固定。例如，電力、連線、電腦，以及人員成本都是正常支出的一部分。相較於派遣

固定翼飛機轟炸建築物，網攻費用要低得多。網攻還可以減少人員身陷險境的機會。有人和無人駕駛飛機需要飛近目標才能投射彈藥，會使人員和高成本裝備暴露在遭受敵人砲火攻擊的危險之中。網攻不會面對這種實際的危險。此外，與飛機相比，網攻所需的維護和後勤需求更少。當國家高層選擇以軍事行動實現政治目標時，網攻的特性可降低風險和成本。

相反論點

有許多論點反對將網攻權限下授至作戰層級，但這些爭論都無法因應在這個新領域中的變化。有些人認為，網攻比動能武器攻擊更危險，因為網路本身存在著未知因素。網攻要求精準打擊無異是緣木求魚，因為時間和情報蒐集的需求無法和動能武器相提並論。數十年來的軍事行動證明，使用動能武器具有高準確度與精密度。網路武器的附帶損害，本質上比動能武器大，因為在釋放網路武器前，不可能完全知道會產生的意外後果。即便具有可逆轉效果，倘若網路武器是用來針對敵方的敏感網路，風險也會升高。然而此一論點經不起檢驗，因為網攻的運用和知識在軍民領域都呈現快速成長。網攻達到精密程度所需時間正在迅速縮短。隨著網路武器的擴散，附帶損害的評估也變得愈來愈準確。可逆轉的效果確保在發生附帶損害時可以恢復原狀，也因此降低了危害。最後，動能武器總會造成死亡和破壞，而網路武器則不必然如此。

其他人則認為，如果沒有大量資源，作戰指揮官及其所屬人員不可能設計網攻，並依此獲得具有可逆效果的可靠成果。他們表示無法設計足以信賴的可逆效果網路武器。這些批評者可能指出震網病毒中的錯誤，任其無意間在全球傳播和複製。[28] 他們認為情報界和戰略指揮官層級才有能力、資源及知識去理解設計網路武器的複雜性。網路不斷進化的本質，幾乎不可能快速設計網路武器。此一論點站不住腳，因為大多數國家的通信系統、電網等都使用全世界知名的商用軟體和系統，而「現成的」網路武器預期將可滿足這種需求。並非每種網路武器都是以獨立運作的方式獲致預期效果。作戰層級人員擁有強大的情報、作戰和通信部門，有能力評估敵方網路。如果現有人員無法執行網路作戰的規劃和攻擊，美國網路司令部下轄的其中兩類支援小組，可強化其計畫和攻擊能力，還有共27個戰鬥任務小組可支援各作戰司令部，協助在作戰規劃與應變作戰時產生綜合的網路效應。[29] 此外，還有25個支援小組為全國性任務和戰鬥任務小組提供分析和計畫支援。[30] 這兩類小組都可透過其所屬作戰司令部，來強化和協助作戰指揮官及參謀執行網攻。預先核准的網攻方式，讓作戰指揮官能在現有資源限制下攻擊敵人。

網路的本質要求軍事領導人需在法律、道德和資源限制範疇內動用武力。許多未知因素將為作戰指揮官在網路中運用軍事力量時，帶來具挑戰性但可克服的障礙。下授權責予作戰層級指揮官，而非限制其網攻權責來避免產生更大的風險，也符合決策者的最佳利益。作戰指揮官面對能削弱和破壞軍事能力的敵人，必須盡可能擁有更多工具來達成目標。有限的網攻權責能夠增加

可運用的工具。作戰指揮官需要擁有網路武器，俾藉由軍事行動以謀求國家利益。在網路中，攻擊占有較佳優勢。[31] 賦予作戰指揮官攻擊敵人能力的最佳方式，包括下授具備可逆效果的有限網攻權責。可逆效果降低了軍事行動中的固有風險，並減輕意外後果。國家高層以預先核准網攻的方式，可獲得更大的軍事行動控制權，在危機發生時，也得以有更多軍事行動選項。國家高層需要將有限網攻權責授予作戰指揮官，俾利其實現與重要、核心和次要國家利益一致的作戰、戰略及政治目標。

作者簡介

Michael P. Carvelli美陸軍少校係駐阿富汗美軍總部聯合工程計畫參謀。

Reprint from *Joint Force Quarterly* with permission.

註釋

1. The Department of Defense (DOD) includes cyber attacks in a larger category referred to as "offensive cyberspace operations." This article refers to all offensive cyberspace operations as cyber attacks. DOD defines *offensive cyberspace operations* as "Missions intended to project power in and through cyberspace." See Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), GL-5.
2. Maren Leed, *Offensive Cyber Capabilities at the Operational Level* (Washington, DC: Center for Strategic and International Studies, 2013), available at <www.csis.org/analysis/offensive-cyber-capabilities-operational-level>.
3. Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander," *Joint Force Quarterly* 66 (3rd Quarter 2012), 22–27, available at <http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-66.aspx>; James E. McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly* 10, no. 4 (Winter 2016), 46–63, available at <www.airuniversity.af.mil/SSQ/>; Musa A. Samad, "Cyber Operations: Putting MAGTF Commanders in Control," *Marine Corps Gazette* 99, no. 7 (July 2015), 20–23, available at <www.mca-marines.org/gazette/2015/07/cyber-operations>.
4. 美國國防部將網路空間定義爲「資訊環境中的全球網域，其中包含資訊技術基礎設施及網民資料的互聯網，如網際網路、電腦網絡、電腦系統、內嵌處理器以及控制器。」See JP 3-12, GL-4.
5. Ibid., I-2–I-4.
6. Paul W. Phister, "Cyberspace: The Ultimate Complex Adaptive System," *The International C2 Journal* 4, no. 2 (2010), 13, available at <www.dodccrp.org/files/IC2J_v4n2_03_Phister.pdf>.
7. Ibid.
8. Jeffrey Hunker, *Cyber War and Cyber Power: Issues for NATO Doctrine*, Research Paper No. 62 (Rome: NATO Defense College, November 2010), 3, available at <www.files.ethz.ch/isn/124343/rp_62.pdf>.
9. Richard M. Cromwell, *War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21*st *Century Warfare* (Newport, RI: U.S. Naval War College, 2010*)*, 18.
10. Natalia Zinets, "Ukraine Charges Russia with New Cyber Attacks on Infrastructure," Reuters, February 15, 2017, available at <www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN>.
11. Helene Cooper, "ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts," *New York Times*, January 12, 2015, available at <www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html>.
12. *Statement of General James N. Mattis, U.S. Marine Corps, Commander, U.S. Central Command, Before the Senate Armed Services Committee on the Posture of U.S.*

Central Command, 112th Cong., 1st sess., March 1, 2011, 39, available at <www.armed-services.senate.gov/imo/media/doc/Mattis%2003-01-11.pdf>.

13. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, available at <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>; Kim Zetter, "Report: Obama Ordered Stuxnet to Continue after Bug Caused It to Spread Wildly," *WIRED*, June 1, 2012, available at <www.wired.com/2012/06/obama-ordered-stuxnet-continued/>; John Naughton, "Stuxnet: The Worm That Turned Obama into a Hypocrite?" *The Guardian*, June 9, 2012, available at <www.theguardian.com/technology/2012/jun/10/stuxnet-us-internet-freedom-policy-john-naughton>; Rowan Scarborough, "In Classified Cyberwar against Iran, Trail of Stuxnet Leak Leads to White House," *Washington Times*, August 18, 2013, available at <www.washingtontimes.com/news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to-/>.
14. Ibid.
15. This scenario was adapted from the one provided by Carter, Fieck, and Undersander, "Offensive Cyber," 25–26.
16. Lieutenant General Edward Cardon, USA, panel member, "CMF #11: The Future of Army Public-Private Partnership and Cyberspace," Association of the United States Army, Washington, DC, October 5, 2017, available at <www.dvidshub.net/video/486234/cmf-11-future-army-public-private-partnership-and-cyberspace>.
17. Bimal K. Mishra and Dinesh Saini, "Mathematical Models on Computer Viruses," *Applied Mathematics and Computation* 187, no. 2 (2007), 929.
18. Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in *2012 4*th *International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 2012), 323, available at <https://ccdcoe.org/cycon/2012/proceedings/d1r3s2_fanelli.pdf>.
19. Leed, *Offensive Cyber Capabilities at the Operational Level*, 8.
20. Norman T. Sheehan, "A Risk-Based Approach to Strategy Execution," *Journal of Business Strategy* 31, no. 5 (2010), 31–32, available at <www.researchgate.net/profile/Norman_Sheehan2/publication/242020919_Making_risk_pay_The_board's_role/links/559eefee08ae03c44a5cdef5.pdf>.
21. Lech Janczewski and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2011), 263.
22. Ibid.
23. Neil C. Rowe, "Towards Reversible Cyberattacks," U.S. Naval Postgraduate School, Monterey, CA, available at <http://faculty.nps.edu/ncrowe/rowe_eciw10.htm>.
24. Ibid.
25. Ibid.
26. Karen DeYoung, Ellen Nakashima, and Emily Rauhala, "Trump Signed Presidential Directive Ordering Actions to Pressure North Korea," *Washington Post*, September 30, 2017.
27. Tony Munroe and Jane Chung, "For North Korea, Cutting Off Oil Supplies Would Be Devastating," Reuters, April 13, 2017, available at <www.reuters.com/article/us-northkorea-nuclear-china-oil/for-north-korea-cutting-off-oil-supplies-would-be-devastating-idUSKBN-17F17L>.
28. Rowe, "Towards Reversible Cyberattacks."
29. *The DOD Cyber Strategy* (Washington, DC: DOD, April 2015), available at <www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.
30. Ibid.
31. William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (2010), 99, available at <www.dtic.mil/dtic/tr/fulltext/u2/a527707.pdf>.