● 作者/Josiah Dykstra, Chris Inglis and Thomas S. Walcott ● 譯者/黃文啟 ● 審者/彭耀祖

善用殺傷性與網路武器

Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat

取材/2020年第四季美國聯合部隊季刊(*Joint Force Quarterly*, 4th Quarter/2020)

網路武器發展正在改變戰爭型態，有必要將其與殺傷性武器融合，使其成爲新的戰略能力，以發揮聯合作戰整體效能。

2020年7月25日，1名航電技術下士正在巡弋菲律賓海的雷根號航艦飛機野戰保修廠內，進行標定系統維修工作。(Source: US Navy/ Jason Tarleton)

戰爭幾乎與人類歷史同樣久遠，進行方式主要是透過實體力量破壞、削弱或摧毀有形資產。長久演進下完備了武力展示及嚇阻、量敵用兵和戰爭規則等準則與原則，而上開成就皆奠基於實體武器的可預期性及重複性。然而新興的網路戰卻顯示，過去殺傷性武器時代的假定事項並不全然適用。例如，迥異於實體飛彈和炸彈，電腦病毒的運用很難預測其精確效應、衡量敵我戰力比、或判斷伴隨而生的附帶效果。本文將探討殺傷性武器與網路武器的差異，並明確區隔與管理；以及對戰略層級軍事準則、計畫作為、兵力投射和防禦作戰的深遠影響。

若要打贏現代衝突，必須從個別與整體角度，充分瞭解殺傷性武器與網路武器的特質。截至目前，有關網路武器的探討，皆置重點於「易逝性」（Perishability）──換言之，很難達成一般殺傷性武器的相同精準（更別提可信度）戰果。對於軍事領導者和決定軍事行動目的與手段的決策高層而言，殺傷性武器與網路武器之間的差異，使其必須立即重新評估運用方式及其效益，而此種評估必須仰賴明確界定傳統與網路作戰環境的異同。作者所提出的戰略架構雖非完美，卻仍適用於所有國力手段；本文繼而說明殺傷性武器和網路武器的區別，並釐清兩者差異性和戰

網路武器與殺傷性武器的融合，將能在現代戰場上發揮強大的作戰效應。(Source: US Army Cyber Command/ Edric Thompson)

略影響力。

本文針對攻擊性殺傷力與網路力量在三大關鍵領域進行比較：分別為武器特質、目標獲得和政策／作為。[1] 這些主題會在作者所列舉的18項個別差異中呈現。武器特質包含本身既有特性以及所產生效果。目標獲得則強調對於攻擊目標所產生不同程度的影響。政策與作為則涵蓋當前環境與武器成熟度的差異。

作者在分析這些領域的過程中指出，軍事幹部應牢記3項有助武器選擇與運用的綱要性問題，這些對於殺傷性武器與網路武器一體適用：

武器在有限的計畫作為與任務執行時間、操作人員熟稔度和後勤支援等限制條件下，能否獲致所望戰果？

武器影響能否僅侷限在所望目標，避免損及對無關對象和資產？

武器的使用是否有助局勢穩定或是造成反效果、是否衝擊組織緩解情勢、和／或是否破壞敵所望戰果？

這些問題的答案，雖部分取決於實際狀況，但也在於深入瞭解武器特性，作者將陸續加以詳細討論。

為了詳盡討論內容，吾人必須思考武器的定義。遺憾的是，美國國防部並未在準則中將武器明確定義，即便在其他定義中確實使用「武器」一詞。因此，作者首先從辭典中找出「武器」的定義為「在戰爭或戰鬥中用於攻擊或降服敵人的任何手段」。[2] 一般而言，武器在傳統上都是用於發揮殺傷與非殺傷性效應。美軍聯戰準則JP 3-12「網路空間作戰」(JP 3-12, *Cyberspace Operations*) 定義「網路空間戰力」為「一種專門在網路空間或範圍內發揮效應的裝置或程式，包含軟體、韌體或硬體的任何組合應用」。[3] 本文作者所考慮的網路空間戰力不同於(卻相去不遠)為達成所望效應而破解系統的一種機制。美軍聯戰準則JP 3-0「聯合作戰」敘明網路空間攻擊是一種非殺傷性戰力；其他例證包含電子戰攻擊、以資訊支援軍事行動及非殺傷性武器等。JP 3-0指出，火力乃「運用既有武器或系統，對某個目標發揮特定作為」。[4] 網路攻擊行動也是一種火力類形，足以在網路空間中發揮明顯拒止效果（亦即削弱、破壞或摧毀等），或促使實體環境中產生拒止效果」。

在以下段落中，作者將介紹並區隔18項特質，並將其依據網路武器與殺傷性武器的特性、目標獲得及政策與作為等差異分組列出。

武器特質上的差異

目前許多針對網路武器的討論，都將重點置於網路領域的基本特質，諸如全球網際網路；硬體、軟體與構型等組成要件的高度動態交互作用；以及操作者在接觸所望目標之存取路徑所存在的脆弱性等。當代網路武器的討論，也同樣觸及其高度易逝性與短暫壽期。[5] 這些特徵在今日都已為世人所普遍瞭解，但卻仍不足以做為比較網路武器和殺傷性武器的基礎。下列其他差異性，更有助於激發戰術與戰略思維。

殺傷性武器幾乎是立即接敵和產生效應(藉由武力)，而網路武器則是將接敵和產生效應區分兩個不同行動，且兩者間通常有很大的時間差(在某

些個案中，網路接敵得耗數週或數月才能產生所望效應)。在「聯合作戰接敵概念」(Joint Operational Access Concept)中，「作戰接敵」(Operational Access)被定義為「對某個作戰區域投射軍力的充分行動自由，」。[6] 殺傷性武器可以為兵力投射創造此種接敵途徑，並對敵方造成反介入與區域拒止效果。網路武器一般都是將接敵和效應區分，且兩者通常須挹注相當大的力量，才能對特定目標及其環境建立接敵管道。例如，「阻斷服務式攻擊」(Denial-of-Service Attacks)所用的方式，就是由入侵者對運作中網路開闢接敵路徑。「破壞資料式攻擊」(Data Destruction Attacks)則是以其他手段控制路徑，例如遠端刺探或社交工程等手段，但其成功關鍵仍在於攻擊者能否對所望目標建立存取路徑。上開所言欲表達的是，網路武器需要高度專案規劃、前置作業、和／或結合特定目標及創造路徑的能力。[7]

殺傷性武器幾乎總是造成無法復原的物理性損害，而網路武器所造成的損害有時則可完全可復原。雖然像橡膠子彈之類的小部分武器造成的損害可快速復原，但絕大多數武器是蓄意要造成永久性或復原緩慢的損害。網路武器亦可對實體世界造成永久性損害，例如震網案中(伊朗)離心機設備的毀損，而其他網路武器造成的結果則可由攻擊者或受害者復

表：殺傷性武器與網路武器的差異

	殺傷性武器	網路武器
武器特質	創造接敵路徑	運用接敵路徑
	難以逆向工程及改變目的	恐導致他方仿傚
	永久效果	效果或可逆轉
	局部效應	恐擴及全球
	效果一致性	具不同程度效應
	使用量與效果規模成正比	效果因使用方式而不同
	單一效果	可規範其效果
	可預期性	易受環境影響
	使用門檻高	使用門檻低
目標獲得	單一目標選擇	多重目標選擇
	環境需求條件低	高度預置能力（系統針對性）
	積極管制	臨機執行
	概略性目標選擇	精準式目標選擇
政策與作為	須具豐富操作經驗	毋須豐富經驗
	攻擊企圖明顯	攻擊企圖不一
	受限武裝衝突規範	各層級均具價值
	可明顯溯源	溯源程度不同
	可靠性高	可靠性不一

2019年9月，美軍第7陸軍訓練指揮部於「彎刀連結19號演習」實彈射擊課目中，第173空降旅319空降砲兵團第4營C連所屬砲手及砲班人員於德國葛瑞芬渥爾訓練場輸入M777榴彈砲的射擊諸元。(Source：US Army/ Thomas Mort)

原。舉例而言，當阻斷式服務停止後，目標系統便會恢復正常，而用在勒索軟體的加密程式，只要能輸入正確解鎖密碼就能復原。事實上，勒索軟體是因其可逆性而產生效用，此類攻擊讓受害者無法正常存取資料及程式，並進而迫使其主觀認為不得不支付贖金。更重要者，可逆性對網路武器而言是優勢或是限制，完全取決於使用者目的。

殺傷性武器很難逆向工程或再利用，因為一般在使用過後都會造成嚴重破壞而無法重複使用。然而網路武器通常由易於複製的軟體所構成，更易於被觀察、分析和重複使用，因為只要複製軟體並重新仿造其運用條件即可。如同前文所述，建立路徑的時間差距及網路武器運用的影響，許多網路攻擊可運用數位系統監控資料與軟體流通和儲存的回放能力，來進行觀察和複製，造成即使是攻擊結束後，網路武器仍有很高的可能性會被敵方完整複製並進行研究。部分專家將此種情境比喻為玻璃屋中的生活，認為運用網路作為攻擊手段，必須先做好防禦準備和部署，因為敵

人必定會以其人之道，還治其人之身。[8] 現實環境中，武器載臺可以部署於遠離目標之處，以免受破壞。殺傷性武器的彈藥是消耗品，且在使用後很難、無法甚至沒有必要復原或再利用。[9]

雖然現實環境中，部分武器──包含核生化武器──會精確限制使用者對實體衝擊，但殺傷性武器皆可量化局部效應，故會受到現實環境條件限制。即便像核武在設計製造時，無法限定僅摧毀特定區域的某磚造建築物，但在結構與運用上卻仍能規範其實際作用範圍。然而，網路力量卻兼具局部和擴散效應，並取決於武器、目標和網路空間結構。綜觀網路武器運用的短暫演進史，那些看似局部和劫持性的網路攻擊，卻往往擴及全球網際網路。2017年夏季，源至俄羅斯的「培塔」(Petya)勒索軟體攻擊，正是此種情況的極佳例證。雖然外界普遍認為，這是一場俄羅斯針對烏克蘭政府系統的攻擊行動，[10] 但這種病毒卻很快散播歐洲各非政府系統──甚至癱瘓了「快桅」(Maersk)航運公司的全球資訊科技系統和全球指揮管制系統，其他擴散效應也讓烏克蘭以外地區受到影響。[11]

殺傷性武器的一致、固定性效應，反應了其單一目標及實體環境的(諸如地心引力和空氣密度)相對穩定的特質。網路武器則可能發揮不同效應，端視程式碼設計從隱晦(所謂間諜軟體)到極端明顯(如勒索軟體)的細微程度。同樣地，殺傷性武器的固定性效應，意味著無法針對特定目標發揮指定效果。而網路武器則能適度調整，並細緻、輕易地進行改變或量身設計，以便對特定裝置或晶片發揮客製化效應。

現代軍事作戰在計畫與危機處理方面必須保持靈敏度與適應力，包含彈性調整行動強度與廣度。殺傷性武器通常藉由增加使用數量或酬載量大小修正攻擊方法。由於彈藥屬消耗品項，殺傷性武器在投射後僅能衝擊單一目標。雖然特定區域投射的殺傷酬載數量可依狀況增加，但通常仍須比對酬載密度、速度和殺傷效應。網路武器藉修改其程式設計，就可以對付單一或多重目標，因而能發揮既有且彈性修正。勒索軟體就是一種可重複對付多重目標的網路武器。保守推論，倘欲防禦殺傷性武器，須付出相當代價；若欲反制網路武器而規劃多重目標防護作為，諸如使用防毒軟體等，相較之下就更為符合成本效益。[12]

軍事計畫人員可在不同程度效應的武器選項從中獲益。殺傷性武器可發揮固定效果，指其效果在武器製造時就已預先設計。網路武器當然也可針對預劃行動或所望戰果進行設計，但在使用時相較殺傷性武器，卻可能發揮更精準效應。吾人可輕易設想，能刪除特定檔案的網路武器，也能快速且輕易地刪除其他任何單一或數個檔案。結論是，若要防護網路武器如防護殺傷性武器一般程度，就必須作更多的準備。

殺傷性武器可產生預期結果，因為變數在事前已被充分瞭解。物理定律及對於殺傷性武器的效應，都是先行完成研究與記錄，而環境變數對於殺傷武器效能的影響也具有高度可預期性及量化程度。網路效應則極易受到環境影響，從目標軟、硬體的微妙變化，或使用者群組設定，到鏈結攻擊者與目標的全球動態連網行為等，都可能對其影響，主因其高度依賴特定的軟體設定值。

2020年2月5日，美陸戰隊網路空間司令部所屬人員，正在密德堡(Fort Meade)洛斯威爾大樓的作戰中心執行勤務。
(Source: US MC/ Jacob Osborne)

最後，吾人要關注殺傷性武器與網路武器入手的難易度。目前，入門等級的網路武器日益普遍，並成為不同等級侵略者廣泛分享的商品。方便取得、成本低廉且操作簡單等特質，意味著網路武器易被許多國家和非國家行為者所採用。這些可以免費取得(如容易取得的Metasploit軟體)或公開市場可取得(如Core Impact軟體)等工具，都能輕易變成網路攻擊的武器。對於美國而言，此種情況既是負擔，也是機會，因為愈來愈多美國網路武器曝光後，敵人便能取得更多武裝，但也正是如此，敵人將被迫去抑制美國規模經濟能負擔得起的更多平臺，進行網路攻擊反而會付出更高代價。綜上，若以不同角度觀之，美國就多數殺傷性武器成本、專業或取得容易度方面，仍遠超出許多敵人許多。

目標獲得差異

在目標獲得範疇的首要差異是武器與目標比例。就打擊點

而言，殺傷性武器只用於對付單一目標。雖然目標範圍和大小可能有所不同，但就算是殺傷性大規模毀滅性武器仍然有其時空限制。相較之下，網路武器所發揮的能力，可以在不同時空影響多重目標，在某些案例中甚至將攻擊目標作為下一波行動的跳板。網路武器使用時不會被消耗，除非有人開發並植入修補程式──即便如此，此軟體也不一定適用於全球性攻擊行為。

另一個重要差異則是對目標的射程。殺傷性武器只需要針對目標進行最小程度的前置作業即可發揮效果──這對遠距遙射型殺傷性武器更是如此。實際地理範圍對於網路就沒那麼重要，但複雜的數位環境需要在實際戰場空間進行大量前置作業和準備，才能使網路攻擊順遂。

目標獲得亦受到目標(偵獲與鎖定問題)和武器(解決問題)控制程度的影響。精確的目標獲得即積極的目標選定管控，對於達成軍事目的與避免附帶損害十分重要。網路武器可能需要同時進行臨機和選擇目標獲得。「震網病毒」(Stuxnet)就是這樣的研究個案，此種武器係用於探索許多系統，卻只攻擊符合目標條件的系統，並迴避不符標準的目標。[13] 這就是臨機途徑而非對所有受感染系統進行主動管制的例證，進一步顯示出途徑與效應之間的差異。

在細密度與精確度方面區隔殺傷性武器與網路武器的差別，才能突顯網路武器在概略目標獲得與精準效果的長處。「震網病毒」僅搭配(相對)粗略的目標獲得途徑，即可針對特定目標發揮精確攻擊效果。精確的目標獲得需要精良的技術和準確的情報。[14] 幾乎沒有殺傷性武器可以將粗略途徑與精準攻擊效應搭配併用。

政策與作為上的差異

目前，網路武器的使用經驗，尚未如殺傷性武器般成熟。殺傷性武器的開發、分析與運用，皆已有豐富經驗；且多為數十年甚或數百年的精進和應用逐漸演進而來。例如，1964年成立的「聯合彈藥效能技術協調小組」(The Joint Technical Coordinating Group for Munitions Effectiveness)，便是專責提供聯合彈藥效能準則所需之武器效能參數。網路武器目前尚無類似組織存在。不僅如此，各國軍隊在訓練和使用殺傷性武器方面皆經驗老道。相較近期才出現的網路武器，尚未累積足夠經驗值。因此，對於將網路融入戰略武器項目一說，仍存有遲疑和不確定。

使用各類研發完成的武器，可向敵人傳達不同訊息。殺傷性武器所代表的含意，向來十分明確。衝突情勢一旦升高，便意味著雙方在某種程度上，已洞悉對方欲從中獲得何種利益。動用武力是現代國家最後的手段。然而，網路武器卻可以傳達較隱晦的訊息，不論就其所望效應、與特定行為者(攻擊者)的關連性、抑或能否清楚判別企圖等，均屬不易。假如網路武器只是整體殺傷性攻擊的輔助手段，上開情況就可能發生；但如果網路攻擊是讓敵人付出代價並傳達明確戰役訊息，則相反。

網路武器在衝突和對峙的各階段皆可發揮特殊功用，且當運用於未達武裝衝突門檻的行動時，更是格外有效。全球持續性的灰色地帶網路衝突，在未來仍很可能發生。[15] 相較之下，殺傷性

武器卻是不能運用在武裝衝突以外──這點可能是殺傷性武器和網路武器最明確且重要的差異。2019年6月，媒體報導美國「網路司令部」(Cyber Command, USCYBERCOM)對伊朗發動網路攻擊，以反擊其侵略行為。[16] 雖然這場攻擊搭配了殺傷性武器攻擊計畫，但選擇網路攻擊，意味者美國摒除了殺傷性武器，也可能情勢顯示網路攻擊較不會升高危機，故非殺傷性選項仍是反制伊朗並對其傳達訊息的手段之一。

對於一般國家而言，明確找出殺傷性武器使用者並不難。但欲在網路空間找出攻擊者卻仍是個難題，因為許多工具和基礎設施都可以被輕易混淆與操弄。[17] 網路武器因其客製化使用方式，故需要強大的能力方能隨時揭露攻擊者。

當領導人和決策者在衡量武器選項時，有時是依據其個人信賴感。現代軍事領導人對於殺傷性武器具有高度信心，是因為擁有足夠經驗和訓練。而目前網路武器在效應與效能方面，僅能提供程度不等的可信度。故持續性的實戰作為，加上模式模擬科學與技術，有助累積必要經驗，並提高網路武器效能的信賴感。

網路武器擔任戰略能力的演變過程

國家整體安全需要在不同衝突階段，思考並統

2020年4月22日，美空軍特種戰術單位人員於佛羅里達州英格林訓場訓練時，跨越空曠地接近第二座目標建築物。

(Source: USAF/ Rose Gudex)

合運用所需全部國力。必須強調的是，網路直到近年才成為美國可用的完整國力和戰略能力。此發展若在周延的思維與深入探索，以及法律、政策與戰略方面獲致重要成果後即可能做到，但要讓網路成熟至足以在戰爭殺傷領域中樹立長期經驗值，可能仍有待努力。網路日益成熟，尤其是在政策與作為方面，將持續左右未來戰爭整體型態的發展。

2018年，「國防科學委員會」(The Defense Science Board, DSB)所屬「網路戰略能力專案小組」(Task Force on Cyber as a Strategic Capability)認定，美國國防部「必須跳脫網路的戰術層級，並瞭解其戰略能力」。[18] 專案小組也針對網路戰力和殺傷力進行比較，其中包括可能之意外和附帶損害。「國防科學委員會」最終結論指出，任何具有特定效應的手段，其戰略能力均具備以下共同特質：

- 可對目標本身、效率和/或意志(即可左右敵人意志且令其畏懼)，創造明顯且持久的效果。
- 完整發展且成熟，且能在合理時間內發揮所望效果(能迅速滿足政策與聯戰指揮官需求)。
- 可在合理時間內重複作為(能以一次性戰術打擊外的手段支持戰役行動)。

對於將理想付諸實現，過去二年所達成的四項階段性成果，已具有指標性意義。第13號國家安全總統備忘錄〈美國網路作戰政策〉已闡明必要政策，[19] 而2019年〈國防授權法〉則提供法制基礎，[20] 〈國防部網路戰略〉則提供所需準則。[21] 不僅如此，「網路司令部」已升格為聯合作戰司令部層級，現任司令中曾根上將(Paul Nakasone)已開始依據持久接戰準則，行使上述最新權限。[22] 這些階段性成果顯示，美國有意志和能力運用網路戰力，並結合其他力量，以保護本身在網路空間不受傷害。

殺傷力與網路戰鬥整合的未來發展

為取得打贏與預防現代戰爭的能力，亟須理解殺傷性與網路戰相結合所衍生的特定風險與機會。不同於殺傷性行動，網路攻擊日益普遍，且獲得某些國家支持，並成為獨立行為者的手段。但即便傳統戰爭已開始融合網路戰力——例如，俄羅斯在入侵烏克蘭前，就先對烏國重要基礎設施發動網路攻擊。美國必須儘快整合網路戰力，以發揮最大的可能效益。

本文所探討殺傷性武器與網路武器的差異，顯示出兩者雖然不同，卻可相輔相成，若整體運用，甚至可能發揮加乘戰力。部分研究人員推論，若將兩種武器結合，甚至還能讓軍事力量更上層樓。聯戰準則3-12（JP 3-12）似乎就支持此種假設論點，其內容指出「網路攻擊戰力，雖然可在單獨背景下運用，但通常在結合其他火力手段時方能發揮最佳效果」。[23] 惟目前尚無充分經驗檢驗這種直觀式的主張。網路武器和殺傷性武器本身就擁有極為強大的力量，且能獨立達到所望軍事目的。假如軍事力量的終極目的，是為了完全避免武裝衝突，則網路戰力就能創造許多獨特機會，發揮各種不同效應。

精細研究體認這兩種武器的異同，能讓軍事領

導人更充分整合殺傷性與網路武器。個別言之，傳統武力與網路領域或許無法嚇阻或阻止現代敵人，因此必須針對兩大領域的差異，找出新選項。軍隊已經開始學會以適當方式、地點和時間運用網路武器。此種知識未來將可讓指揮官決定這兩大領域相輔相成的運用模式。

許多未知的問題都是有關如何整合殺傷性和網路戰鬥。藉由展現甚至擴大可能效應，殺傷性與網路複合式武器系統和作戰行動，將衍生出有關戰爭行為的新問題。無人系統就是整合性武器的一個指標性例證：一種具有殺傷效果的網路控制系統。無人系統所攜帶的殺傷性彈藥展現其相對的殺傷性特質，包含鎖定、發揮預期與永久性效應。目標獲得、政策與作為，似乎也完全呼應殺傷性武器的攻擊特質；然而，敵人在攻擊無人機或其操控系統時，理論上亦能創造精準、可變化、可逆轉且難以溯源的效應。不同於對無人機所發動的實體攻擊，上開特性讓敵人更難以確實掌握無人系統控制權；此種情況可能會延遲防禦性反制作為。此外，無人系統也衍生出合理軍事目標的定義：是遙控操作員？操作員所在位置？操作員與無人機間的通信傳輸手段？亦或是武器系統組件的開發者？

不論從個別或共同角度而言，網路武器和殺傷性武器都已成為可用的國家戰略力量，並對達成國家目標提供全新契機。由於網路戰演進史甚短，許多機會仍必須仰賴深化對網路武器的瞭解。隨著領導者對網路武器擁有愈來愈多的經驗和專業知識，整合戰鬥和灰色地帶選項便可獲得強化。本文所列舉殺傷性武器與網路武器的差異，是瞭解並運用網路戰力獨特與整體特質的必要基礎。

作者簡介

Josiah Dykstra博士係現任美國國家安全局「網路安全共同作業中心」技術研究員。

Chris Inglis係現任美海軍官校網路安全研究榮譽教授。

Thomas S. Walcott係現任美軍網路司令部「網路國家任務部隊」技術主任。

註釋

1. 雖然作者在本文內容中主要置重點於攻擊性（拒止、削弱、破壞、摧毀和操控）能力，但網路與殺傷性效應也可成功用於防禦與嚇阻；相關內容廣泛見於各種文獻。網路嚇阻也是學界與政府廣泛研究的重點，使其成爲一個實作與理論上快速演進的領域。See, for example, Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," Orbis 61, no. 3 (2017), 381–393, available at <www.sciencedirect.com/science/article/pii/S0030438717300431>. See also Defense Science Board, Task Force on Cyber Deterrence (Washington, DC: Department of Defense, February 2017), available at <https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf>.
2. "Weapon," OED Online, Oxford University Press, June 2019.
3. Joint Publication (JP) 3-12, Cyberspace Operations (Washington, DC: The Joint Staff, June 8, 2018), I-4, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf>.
4. JP 3-0, Joint Operations (Washington, DC: The Joint Staff, October 22, 2018), III-30, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf>.

5. Christopher A. Bartos, "Cyber Weapons Are Not Created Equal," U.S. Naval Institute Proceedings 142/6/1 (2016), 30–33, available at <https://calhoun.nps.edu/handle/10945/49618>.
6. Joint Operational Access Concept, Version 1.0 (Washington, DC: The Joint Staff, January 17, 2012), ii, available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joac_2012.pdf>.
7. See also N.C. Rowe, "Towards Reversible Cyberattacks," in Proceedings of the 9th European Conference on Information Warfare Security, ed. Josef Demergis (Thessaloniki, Greece: University of Macedonia, 2010).
8. Eric Rosenbach, Living in a Glass House: The United States Must Better Defend Against Cyber and Information Attacks, Testimony Before the Senate Foreign Relations Committee, Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, June 12, 2017, available at <https://www.foreign.senate.gov/imo/media/doc/061317_Rosenbach_Testimony.pdf>.
9. 確實有可能想像複製一顆子彈，但很難想出這樣做的好處爲何。很難想像飛彈爆炸之後要如何完整加以重製。
10. "Alert (TA17-181A): Petya Ransomware," U.S. Department of Homeland Security-Cybersecurity and Infrastructure Security Agency, July 1, 2017, available at <https://www.us-cert.gov/ncas/alerts/TA17-181A>.
11. "Global Ransomware Attack Causes Turmoil," BBC News, June 28, 2017, available at <https://www.bbc.com/news/technology-40416611>.
12. 兩項重點：第一，這假定係指已知武器（亦即，已知其參數，並瞭解其防禦手段）。第二，網路武器代表造成效應的程式碼，其與促成效應的管道面向截然不同，針對所有可能管道面向所進行的防護作爲，應該相當昂貴，且不見得能有效執行。
13. Ralph Langner, To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve (Arlington, VA: The Langner Group, November 2013), available at <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>.
14. Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," Journal of Cybersecurity 3, no. 1 (March 2017), 59–68, available at <https://academic.oup.com/cybersecurity/article/3/1/59/3097802>.
15. Defense Science Board, Summer Study on Capabilities for Constrained Military Operations (Washington, DC: Department of Defense, December 2016), available at <https://dsb.cto.mil/reports/2010s/DSBSS16_CMO.pdf>.
16. Julian E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyberattacks on Iran," New York Times, June 22, 2019, available at <www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html>.
17. See Alexander Kott, Norbou Buchler, and Kristin E. Schaefer, "Kinetic and Cyber," in Cyber Defense and Situational Awareness, ed. A. Kott, C. Wang, and R.F. Erbacher (New York: Springer International Publishing, 2014), 29–45, available at <https://arxiv.org/pdf/1511.03531.pdf>.
18. Task Force on Cyber as a Strategic Capability: Executive Summary (Washington, DC: Department of Defense, June 2018), available at <https://www.hsdl.org/?abstract&did=813604>.
19. Joint Hearing to Receive Testimony on the Cyber Operational Readiness of the Department of Defense, Committee on Armed Services, Subcommittee on Cybersecurity, September 26, 2018, available at <https://www.armed-services.senate.gov/imo/media/doc/18-60_09-26-18.pdf>.
20. H.R. 5515, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," available at <https://www.congress.gov/bill/115th-congress/house-bill/5515/text>.
21. Summary: Department of Defense Cyber Strategy 2018 (Washington, DC: Department of Defense, 2018), available at <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>.
22. Paul M. Nakasone, "A Cyber Force for Persistent Operations," Joint Force Quarterly 92 (1st Quarter 2019).
23. JP 3-12, V-19.