The Tactical Defense Becomes Dominant Again

戰術防禦重返軍事主流之研究

譯者簡介

劉宗翰中校，政治大學戰略與國際事務碩士，現任國防部政務辦公室史政編譯處編譯官。

本文作者：哈姆斯(T.X. Hammes)博士為美國國防大學國家戰略研究所戰略研究中心特聘研究員。

本文出處：美國聯合部隊季刊(Joint Force Quarterly)，2021年第四季，第103期，頁10～17。

It has become widely accepted that the convergence of technological advances is leading to a revolution in military affairs or perhaps even a military revolution.[1] One of the unanswered questions concerning this shift is whether it will lead to continued dominance by the offense or a period of defensive dominance. Offense dominance means that battle requires much greater resources to defend than attack. Defense dominance reverses that balance. Investing in the wrong side of the competition is a rich nation's game that the United States may no longer be

1 雖然「軍事革命」(Military Revolutions)鮮少出現，但其影響力遠大於「軍事事務革新」(Revolutions in Military Affairs)，參見MacGregor Knox and Williamson Murray, eds., The Dynamics of Military Revolution, 1300-2050 (New York: Cambridge University Press, 2001)。

 DOI：10.6892/AB.202210_58(585).0004

able to afford. Against peer competition at scale, misguided investment could lead to strategic defeat. In fact, the answer to this question should guide force development and posture and therefore must be a part of the national security discussion.

各項科技進展的融合有助於開啟軍事事務革新甚或帶來一場軍事革命，這種觀點為人普遍接受。[1] 至於在這種觀點下將形成長期性攻勢或短期性守勢的軍事主流，為一個懸而未決的問題。攻勢主導意味著不只是進攻而已，在戰鬥時仍需更多資源做防禦，至於防禦主導則可以扭轉這種問題。富國才有本錢在競賽場上投資錯誤的方向，但美國可能已不再有這種本錢，尤其在一場對抗實力匹敵者的競爭中，錯誤的投資方向將導致戰略失利。事實上，上述問題的答案要能引導兵力的發展與部署，同時也必須納入國家安全議題的討論範圍。

To examine this question, this article provides a couple of historical examples of the shift between offense and defense dominance at the tactical level. It then examines how the offense-defense balance is shifting in each of six warfighting (land, sea, air, space, cyber, and electromagnetic) domains. Next, it examines how interactions between the domains could further reinforce the defense and finally what the shift to defense dominance means for the Nation.

為了檢視這個問題，本文先列舉一些在戰術層級上攻擊主導與防禦主導間轉變的歷史案例，接著在六大作戰領域(陸、海、空、太空、網路、電磁頻譜)檢視攻守易位的制衡，之後在這些領域中說明攻擊與防禦應如何交互運用，才能進一步強化防衛，最後結論提出轉向防禦主導對國家之意涵。

The Shifting Balance in History
歷史上攻守易位的制衡

History records a constantly shifting balance between offense and defense, driven by a combination of social, economic, and political changes. Despite Americans' love for technology, it alone cannot drive major shifts. For instance, defense was dominant during much of the medieval period because of the cost and difficulty of reducing a castle. This was based not only on the technology of building a castle but also the political, social, and economic structures necessary to do so. Offense was not restored until a wide range of social, political, technological, and military changes necessary for the development of military establishments

capable of rapidly reducing the castles occurred. While cannons provided a key technology, the society first had to develop the political, social, and economic systems to produce and sustain them.

觀諸歷史，攻守易位的制衡不斷受到社會、經濟和政治變化的影響。儘管美國對科技情有獨鍾，但單單只有科技並無法推動重大變革。例如，在中世紀大部分期間，由於城堡具易守難攻特性，防禦蔚為主流，這項風氣盛行除了城堡的建築技術外，也包含政治、社會和經濟等必要因素。攻勢作為的復甦也與廣大的社會、政治、科技及軍事等變化息息相關，因為這些因素對於軍事單位發展迅速攻克城堡的能力不可或缺。當火砲成為一項關鍵技術時，社會必須先發展政治、社會及經濟體系，才能夠從事後續相關生產與維護工作。

A much later major shift of advantage to the defense was driven by the development of rifled muskets and the cannon, the mass production of these weapons, the tactical adaptation of field fortifications, mobilization of mass manpower, economies that could pay for them, and governments that could marshal those resources. The combination of these factors led to defense dominating the tactical battlefield from the late U.S. Civil War until near the end of World War I. Governments could field and arm forces that combined the tactics and technology, which meant any unit moving above ground could be quickly observed and taken under fire. The opposing armies were forced to go to ground in massive trench systems that could be held even against numerically superior attacking forces. Failure of military leaders to recognize these changes-despite the lessons of Crimea, the Boer War, and the Russo-Japanese war-led to repeated, bloody, futile attempts to cross World War I's "no-man's-lands."

在更久之後，防禦優勢的重大更迭乃受到線膛步槍與火砲的造用、這些武器的大規模生產、野戰工事的戰術運用、大量的人力與經濟動員，以及政府能居中統整各項資源等因素所導致。在上述各項因素加總下才促成戰術戰場上的防禦主流作為，這段時間從美國內戰直至接近第一次世界大戰結束為止。各國政府運用戰術與科技結合的方法來部署軍隊，這意味著任何軍隊只要在地面上移動，都會被迅速發現並遭受攻擊。敵軍被迫之下只能走地面下的壕溝網絡，另外壕溝也被拿來作為對抗數量優勢之敵。有克里米亞戰爭(1853～1856年)、波耳戰爭(第一次1880～1881年、第二次1899～1902年)、日俄戰爭(1904～1905年)等殷鑑不遠，若軍事領導者仍未能認知這些改變因素，那麼如同第一次世界大戰時，不斷將士兵送入敵我雙方壕溝陣地間的「無人區」一樣，徒增傷

亡。

It was not until the Germans applied new concepts and tactics to technology emerging from the second industrial revolution-first lightweight machine guns and mortars, then armor and aircraft-that movement was restored to the battlefield. The transition was not completed before the end of World War I. During the interwar period, political, social, and economic systems had to evolve in parallel to produce the skilled engineers and operators, the financial backbone, and the will to conduct the global mechanized warfare of World War II. Since then, the offense has generally dominated tactically in conventional conflicts.

德國的新構想與戰術歸功於第二次工業革命所帶來的新興科技，首次使用輕機槍與迫擊砲，接著是裝甲車與飛機，之前的攻勢亦再度成為戰場重點。這種轉變在一戰結束前仍在持續進行，在戰間期(一戰結束至二戰爆發)，政治、社會及經濟體系也不斷演化，促成專門技術工程師與操作員的出現、奠定財政基礎，以及形成發動二戰全球機械化戰爭的意志。從那時起，攻勢通常是傳統衝突中的戰術主流。

Today, convergence of 21st-century technologies is dramatically changing the battlefield environment. Commercial satellite networks tied to artificial intelligence (AI) processing tools mean that we are approaching a period of constant surveillance of the planet with visual, infrared, and electromagnetic sensors, as well as synthetic aperture radar. At the same time, nations are developing AI-assisted command and control systems that will allow them to absorb, understand, and act promptly on the resulting intelligence. This will enable them to coordinate attacks across all domains, including long-range precision attacks and swarms of autonomous hunters, informed by many sources and sensors, that will seek out their prey.

今日在21世紀各項科技進展的融合，戰場環境發生巨大的改變。商業衛星網路與人工智慧程序處理器相結合，這意味著我們以視覺感測器、紅外線感測器、電磁感測器及合成孔徑雷達從事幾近不間斷的全球監偵。於此同時，各國不斷發展人工智慧輔助的指管系統，這讓各國能吸收、理解所產製的情資並據此快速行動，還能統合所有領域的攻擊，如長程精準攻擊與自主式群集武器在多種來源和感測器的資訊協助下，成為高效能的戰場狩獵者。

These co-evolving concepts, tactics, and commercial and military technologies are once

again creating a battlespace in which movement becomes extremely dangerous. If a unit moves, it will create a signal and can be attacked at much greater ranges than in the past. At the same time, cyber, space, and electromagnetic domains will provide both reinforcement for and increasingly powerful alternatives to kinetic attacks.

這些共同演進的構想、戰術，以及商業和軍事科技又重新形塑戰場空間，這讓部隊移動變得極度危險，一個單位移動所產生的信跡，將遭受比過去更大範圍的攻擊面。於此同時，網路、太空及電磁領域將進一步強化動能攻擊方式並增加攻擊選項。

Whether this convergence leads to offense or defense dominance is a complex question. In fact, the sheer complexity of interaction among the six domains requires that we consider the impact on each domain before we try to understand the overall impact on the character of war. (I have assigned electromagnetic spectrum as a domain. Although it is not yet considered one in U.S. doctrine, both China and Russia are dedicating great resources to dominating this domain.) This article focuses on major power conflict. Conflicts between states and nonstate actors play out in fundamentally different ways than state conflicts, and this article does not attempt to address the impact of the interrelated societal and technological changes on those conflicts.

各項科技進展的融合將形成攻勢或守勢軍事主流，這是一個複雜的問題。事實上，在我們試圖理解戰爭特徵的整體影響之前，須先思考各作戰領域的影響，才能找出在六大作戰領域的複雜互動情形(儘管美軍當前準則尚未將電磁頻譜視為作戰領域，但本文將之列入作戰領域之一，因為中共與俄羅斯為企圖主導該領域，已不斷投入大量資源)。本文置重點於主要國家衝突，須理解的是國家與非國家行為者之間的衝突，在根本上不同於國家與國家之間的衝突，至於衝突中的社會與科技變化之影響，則非本文討論重點。

It is essential to understand the difference between offense domination and a temporary advantage gained by offensive action. Offense domination provides the aggressor a major advantage that can be pursued throughout the conflict. Thus, it is inherently escalatory because the side that attacks first is perceived to have a war-winning advantage. Attacking first has historically provided the advantage of selecting the time and place of the battle. But it has also often provided only a temporary advantage because the attack did not prove sustainable for several reasons. These can best be expressed by the attack reaching its culminating point

before it attained its strategic goals. This has been particularly true when concepts, tactics, and technology combined to increase the inherent advantages of the defense.

重要的是，理解攻勢主導與攻勢行動所獲取短暫優勢之間的不同。攻勢主導可以讓入侵者獲致重大優勢，是故在整個衝突中，入侵者將致力於追求攻勢作為，衝突升級在所難免，原因是認知到率先攻擊的一方將獲得戰爭勝利的優勢，這種認知在戰史上也得到證實，率先攻擊可獲得特定時空的作戰優勢；然而，在一些條件限制下，攻擊並無法持續進行，往往只能提供短暫優勢，較合適的解釋應是攻擊在達成其戰略目標前，就已經達到戰力轉換點。至於結合構想、戰術及科技來強化既有的防禦優勢，向來也是不變的真理。

It is essential to note that temporary advantage in one domain may also allow a much more powerful attack from another domain. An obvious example is a temporary advantage in the electromagnetic domain that neutralizes air defense, thus allowing a much more destructive attack from the air domain into other domains. It is also essential that leaders understand the balance between offense and defense. Failure to do so has often led leaders to start a war they are confident will be short, only to be bogged down in a long, brutal conflict. As noted by Cathal Nolan in The Allure of Battle, the confidence is too often an illusion based on false assumptions. The U.S. Civil War and World War I are examples of this hazard.

值得注意的是，某領域的短暫優勢可能招致另一領域的強勢攻擊，明顯案例是電磁領域的短暫優勢雖然可以癱瘓防空，但勢必遭受來自空中等其他領域的毀滅性攻擊。同樣值得注意的是，領導者須理解攻守易位的制衡，若未能理解箇中之道，即使自信滿滿發起戰爭，後面等著他們的是一場長期殘酷的衝突泥沼。一如《作戰誘惑》乙書「卡塔爾・諾蘭」所述，自信太常是因為建立在錯誤假設上的錯覺，美國內戰與第一次世界大戰正是這種危險案例。

Land
陸上作戰領域

The impact of the fourth industrial revolution on this oldest domain of war has already been dramatic. As noted, the balance between offense and defense in land combat has shifted through the ages. Since the last year of World War I, the offense has dominated

conventional ground combat. (Irregular warfare has followed its own pattern.) However, emerging technologies are shifting the balance in conventional warfare back to the defense.

第四次工業革命對最古老的陸上作戰領域之影響一直為人關注。地面作戰的攻守易位已經隨著時間變化，自一戰最後一年以來，攻擊已成為傳統地面作戰的主流(非正規作戰則遵循自身模式)。不過，新興科技正在使傳統戰爭形態易位至防禦。

Since new systems allow units to remain passive and yet see the battlefield clearly, the defense will have a distinct advantage. Electro-optical and electronic warfare sensors can provide a great deal of information that, combined with external sensors such as satellites and drones, can allow the defenders to visualize the battlefield without revealing their own positions. The defenders will not have to emit signals until they choose to fire. And they will have the advantage of fighting from prepared positions. While most current systems must be manned to operate, autonomous and remote-control systems are being developed worldwide. As these systems mature, defenders can be located at a distance from their weapons and thus not be at risk even after firing. Recent events have shown ground forces will be subject to attack by the emerging families of swarming drones.[2] Inexpensive autonomous drones are flying now and can be mass produced using advanced manufacturing techniques. It is not unreasonable to expect a defender to be able to launch hundreds or even thousands of loitering munitions against each brigade-size attack.

新武器系統雖然強化單位的戰況覺知，但由於仍是處於被動態勢，便凸顯防禦作為的顯著優勢。電子光學與用於電子戰的感測器可以提供大量情資，再加上如衛星和無人機等外部感測器，使防禦者能在不暴露自己位置下洞悉全般戰場環境，也使之只有在選擇開火時才會暴露自己信跡，因此防禦者在陣地內備戰時具有作戰優勢。儘管自主式與遙控武器系統在全球普遍發展，但當前武器系統大多仍須人為操作。隨著這些自主式與遙控武器系統發展漸趨成熟，防禦者便能與其武器系統保持一定距離，即使在開火後也不會產生風險。近期事件顯示，新興群集無人機可對地面部隊產生威脅，[2] 成本不高的自主式無人機已上線飛行，還能以先進製造技術做大規模生產。可以想見，防禦者能發

2 Shaan Shaikh and Wes Rumbaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic and International Studies, December 8, 2020, available at <https://www.csis.org/analysis/air-and-missile-war-nagornokarabakh-lessons-future-strike-and-defense>.

射數以百計或數以千計的滯空彈藥來回應敵旅級規模的攻擊。

In contrast, attackers will have to move if they intend to execute anything but strike missions against the defender. The very act of moving will create a signature. While attackers will retain the traditional advantage of selecting the time and place of attack, the advantage of physically massing either offensive or defensive forces is declining as weapons ranges increase dramatically. Mass can be achieved by assembling long-range fires rather than massing forces. This favors the defender since attackers may well be forced to pass through restrictive chokepoints, while defenders can disperse to the maximum effective range of their weapons. However, as the Azerbaijanis demonstrated against the Armenians, the offense can remain dominant if the attacker adopts modern concepts and weapons while the defender relies on 20th-century weapons and concepts.

相對地，攻擊者若企圖對防禦者執行打擊任務，部隊勢必會進行轉移，然在移動過程就會產生信跡。在武器射程日益增加下，不論是攻擊或防禦的大規模兵力集結優勢都將在其影響下大打折扣，惟攻擊者仍保有特定時空攻擊的傳統優勢。戰力集中已可透過整合長程火力系統去形成優勢，而非採用傳統上集結大規模兵力來達成。攻擊者在被迫穿越受限制的咽喉點之際，防禦者此時將位居有利位置，因為防禦者能預先部署可達最有效射程的武器位置。然而，誠如亞塞拜然與亞美尼亞的戰事所示，只要攻擊者採取的是現代化武器與構想，防禦者靠的是上一世紀的武器與構想，就仍然可採攻擊為主。

Sea
海上作戰領域

Today, land-based anti-ship systems are dominating the surface of the sea out to ever increasing ranges. These land-and air-launched ballistic and cruise missile systems, vertical takeoff and landing drones, and attack aircraft cued by ubiquitous surveillance systems have the enormous advantage of hiding in the cluttered land environment. Their surface ship targets must operate in much more open environments. Land-based systems also have the advantage of both range and magazine depth. And if emerging laser and microwave systems prove effective, land-based forces will have an enormous advantage in power generation capacity. The adage, attributed to Admiral Horatio Nelson, "A ship's a fool to fight a fort," remains true-but now

extends to ever greater ranges from shore.

今日，陸基反艦武器系統正在主宰海平面並逐漸擴大其範圍。這些陸射與空射型的彈道與巡弋飛彈、垂直起降無人機及攻擊機等(由無處不在的監視系統提供定位資訊)在陸地形形色色的環境下，具有隱蔽與掩蔽的巨大優勢，而這些武器的水面艦目標位於全開放海域的不利地位。陸基武器系統還兼具射程與深彈艙(彈藥補給充足)的優勢。至於新興雷射與微波武器系統若能驗證成功，則地面部隊在發電量上也將具有巨大優勢。誠如霍雷肖．納爾遜將軍的格言，「只有一艘笨船才會去攻打一個堡壘」，至今仍然適用，只是現在從海面至岸上的打擊距離又更遠而已。

Geography as well as oceanography can enhance the power of land-based systems. The sea has chokepoints that have been major factors in conflicts between major powers since the Peloponnesian War. Even today, control of straits such as Hormuz or Malacca can allow a power to determine what resources flow to an opponent. In these confined waters, land-based defenses can gain an even greater advantage by employing many less expensive, shorter range anti-ship systems and smart sea mines (essentially tethered torpedoes).

運用地理和海洋地理也能強化陸基武器系統的威力。自伯羅奔尼撒戰爭以來，海洋咽喉點一直是主要強權國家間衝突中的重要因素，時至今日，一國只要能控制如荷莫茲海峽或麻六甲海峽之類的海洋咽喉點，就得以控制敵人的資源通路。在這些狹窄海域中，陸基防禦藉由部署眾多成本不高、較短程反艦武器系統，以及智慧水雷(主要是繫留魚雷)等來獲致更大的優勢。

Extended range land- and airlaunched cruise missiles mean many naval fights will include land-based participants. As Captain Wayne Hughes, USN, demonstrated in his work, the first fleet to conduct successful pulse attacks against an opposing fleet gains a major advantage. Land-based systems can provide more missiles at less cost for each pulse attack.[3] However, as fights move further from shore, the number of land-based systems that can range the fight decreases. At some point, the tactical advantage will shift back to the offense.

增程型陸射與空射巡弋飛彈意味著陸基武器系統將成為許多海戰的一部分。誠如

3 Wayne Hughes and Robert Gurrier, Fleet Tactics and Naval Operations, 3rd ed. (Annapolis, MD: Naval Institute Press, 2018).

美海軍(USN)上校韋恩・休斯在其著作中所述，首批艦隊若能對敵艦隊進行成功的強勁攻擊，就能奪取重大優勢。陸基武器系統能為各波強勁攻擊提供更多飛彈(成本較低)火力支援。[3] 然而，隨著戰事逐漸遠離海岸，陸基武器系統可以支援海上的數量就愈來愈少。在某些情況下，戰術優勢會轉回攻擊作為。

The subsurface fight will continue to favor offense in the deep ocean but the defense in the vicinity of chokepoints. Emerging technologies are making shallow water more transparent than ever. And fixed-sensor arrays can cover key passages between open seas. Rapid advances in autonomous submarine drones will thicken the sensor nets in restricted waters as well as enable swarms of weapons to be launched against infiltrating submarines. In short, emerging technologies are making waters both more transparent and more congested.

在深海的水下作戰將持續以攻擊為主，但在海洋咽喉點周遭則是以防禦為主，至於在新興科技的協助下，透視淺水海域下的情況變得比以往更為容易。固定式陣列型感測器的偵測範圍可以涵蓋開放海域中的海上通道。自動無人潛艦的迅速發展將使得限制海域中的感測網絡更綿密，甚至這種群集武器也能用來對付滲透的敵潛艦。簡言之，新興科技讓海域的透明度增加，也讓海域更為擁擠。

Mining of enemy ports may well be the most effective and viable offensive naval action simply because autonomous drones with small signatures will be able to penetrate enemy defenses to lay mines. Smart mines can be programmed to attack specific classes of ships, thus giving the miner an ability to select targets for best effect without having to maintain forces in the vicinity of the port.

在敵港口佈雷或許是最有效率且可行的海軍攻擊行動，原因在於自主式無人機的信跡小，能穿越敵空防執行佈雷任務而不被發現。智慧水雷可以用來專門執行特定船艦的攻擊任務，因此讓水雷有能力選定目標是最有效的方式，如此一來就無須在港口周邊部署兵力。

Air
空中作戰領域

With missile weapons outranging most manned aircraft, winning in the air will really be about the ability to sustain the fight logistically. The current generation of manned aircraft

needs major operating facilities. Even the F-35B requires significant, easily identified, and targetable maintenance facilities. Nor is the threat limited to in-theater airbases. The advent of containerized long-range cruise missiles and drones deployed on a wide variety of shipping means that bases almost anywhere in the world can be struck. Thus, a key question is whether the joint force can defend its base facilities against swarms of missiles and drones. The United States is betting heavily on directed energy-lasers and microwave (electromagnetic pulse [EMP])-weapons to defeat swarm attacks. While these systems still face numerous challenges, they have promise.

當飛彈武器射程超越大多數的有人駕駛飛機時，贏得空戰的關鍵將是戰時後勤的持續力。當前世代有人駕駛飛機需要各種大型空勤設施的支持，甚至連F-35B這種新世代戰機同樣也需要大型、易辨認及目標顯著的修護設施。敵威脅不會只限於戰區內的空軍基地，因為在長程巡弋飛彈的箱型化酬載和以各式船運部署無人機的進展下，這意味著位於世界各地的任何基地都可能遭受攻擊，因此重要的是美軍應如何防禦其基地設施，以避免飛彈和無人機的群集式攻擊。美國不斷挹注大量資金於導能武器，如雷射與微波(電磁脈衝[EMP])武器，以利反制群集式攻擊，雖然這類系統仍面臨諸多挑戰，但美國已經勢在必行。

While directed energy weapons could protect air bases from drones and missiles, they also can certainly engage manned aircraft. When they are deployed, these weapons will provide significant advantage to the defense for two reasons. First, they require large power systems to operate. Attackers must bring those power systems with them and thus the power available is limited by the ability to lift it by land, sea, or air. In contrast, the defenders can either tap directly into the national power grid for virtually unlimited power or use as many generators as they need. Second, the defender has the enormous advantage of blending into the cluttered ground environment. The actual systems are relatively small and can thus be camouflaged as air conditioning units on tops of buildings or small sheds in the countryside. Again, the attacker must move toward the defended area and thus will generate signals, while the defenders need not generate a signal until they choose to engage. As directed energy weapons become operational, they will increase the advantage the defense holds over the offense in the air domain.

既然導能武器可以防護空軍基地免受無人機與飛彈的攻擊，當然也可以接戰有人駕駛飛機。當這類武器完成部署時將能提供重大的防禦優勢，理由有下列兩點：第一，它們在操作時需要大型電力系統，攻擊者若要操作這類武器，就必須攜帶電力系統，然在

攜行過程中又受到陸、海、空運輸能力之限制。相對地，防禦者幾乎可以無限制的直接使用國家電網，或是視其所需而使用各式發電機。第二，防禦者的巨大優勢是因為能融入各種形形色色的地貌之中。導能武器系統相對較小，所以能在頂樓偽裝成空調設備，或是偽裝成鄉村間的工棚。再者，攻擊者在往防禦區域移動時會產生信跡，反觀防禦者並不會產生信跡，除非其選擇目標接戰後才會暴露。隨著導能武器逐漸達成作戰能力，防禦者將在空中領域比攻擊者更具優勢。

Space
太空作戰領域

Conventional wisdom has stated for years that war in space will be offense dominated because antisatellite systems are cheaper than satellites. An attacker could quickly destroy an enemy's key satellites, and it would take months, if not years, to replace these large, very expensive assets. Given the heavy dependence of U.S. forces on space services, this is a truly alarming situation.

多年來大多數人普遍認為太空戰爭將是攻擊主導，原因在於建置反衛星武器系統的成本要比衛星來得低。攻擊者可以迅速摧毀敵人的重要衛星，然重建這些既大型又昂貴的設備須耗時數月，甚至數年之久。鑒於美軍極為依賴太空服務，這是一個令人擔憂的警訊。

However, rapid developments in space launch and satellite miniaturization are changing that situation. The exponential increase in the number of satellites in orbit, the disaggregation of functions into many platforms, and the increasing ability to rapidly replace satellites in orbit mean that defense may now have the advantage. Disaggregating functions such as gathering intelligence and providing communications links mean that the attacker must engage many more targets to degrade space systems. In addition, vastly improved space awareness, the difficulty of acquiring these small targets, and their ability to maneuver to prevent interception increase the advantages accruing to the defense.

然而，在火箭發射升空與衛星小型化的迅速發展之下，情勢正不斷改變。在太空軌道的衛星數量正呈現指數型增長，具有各種不同功能的衛星平台，愈是分散，且能迅速取代軌道中的衛星，就愈能在防禦上取得優勢。蒐集情資和通信鏈路由不同功能的衛星所提供，這意味著攻擊者必須摧毀更多的衛星，才能有效損壞太空系統。此外，大幅提

升太空覺知能力，以及增加偵獲小目標衛星的困難度並強化其在軌道的移動能力，進而避免遭受反衛星武器的攔截攻擊，這些都能增進防禦的優勢。

Part of successful defense will be restoring space functions damaged by an attack. In addition to the U.S. Space Force's Space Rapid Capabilities Office, private firms are developing high-altitude drones as potential replacements.[4]

成功的防禦作為之一是經攻擊後太空功能的再生能力，在這方面，美國太空軍太空迅速能力辦公室和民間公司都在不斷發展高空無人機，希冀作為未來可能的替代方案。[4]

However, a major vulnerability remains the PNT (positioning-navigating-timing) information provided by the GPS constellation. Timing has become central to the functioning of a wide range of critical civilian systems-banking, communications, retail sales, and uncounted other applications all rely on precision timing. Systematic attacks on the GPS network will cause massive disruption of the U.S. economy as well as society in general. The key question is whether these critical functions can be quickly replaced by other systems in the event of an attack. Fortunately, both civilian and governmental organizations are developing alternatives to the GPS functions. However, until the United States can quickly replace this critical function, offensive action can provide a window of opportunity to an attacker. Yet, as noted, the benefits of such an attack are likely to be fleeting and will almost certainly trigger a reply in kind. In short, space will become an arena of ongoing conflict with the advantage to the defense.

然而，重大弱點還是在於由全球衛星定位系統(GPS)衛星群所提供的定位、導航和定時資訊(PNT)。定時已經成為民間重要機構運作的要素，如銀行業、電信業、零售商，以及在其他方面的眾多運用上都須要精準的定時功能。全球衛星定位系統網絡一旦遭受系統性攻擊，將造成美國經濟大規模中斷，甚至連社會一般層面也連帶受影響。然重要的是，這些關鍵的運作功能一旦遭受攻擊後，能否迅速以其他系統作為替代方案。所幸美國政府部門與民間機構都不斷在發展得以替代全球衛星定位系統的方案。然而，除非美國能做到在短時間內替換損壞的關鍵系統，否則對攻擊者而言，採取攻擊行動仍可以取得有利的機會之窗。不過，攻擊所帶來的優勢將是短暫的，因為受攻擊者同樣也

4 See "Space Rapid Capabilities Office," n.d., available at <https://www.kirtland.af.mil/Units/Space-Rapid-Capabilities-Office/>.

會發動反擊。簡言之，太空的衝突場域仍是以防禦位居上風。

Cyber
網路作戰領域

In 2019, then-Secretary of Defense Mark Esper noted that winning in cyberspace requires offense. This continued the theme established in 2012 when then-Secretary Leon Panetta warned of a "cyber Pearl Harbor."[5] Yet there is a growing pushback against the idea that cyber is inherently offense dominated.

2019年時任美國國防部長「馬克・艾思博」指出，攻擊是網路空間的致勝關鍵，該立論依據是建立在2012年同樣時任國防部長「里昂・潘內達」所提醒的「網路珍珠港事件」警言。[5] 不過，對於網路先天是攻勢主導的說法逐漸出現一些不同見解。

In their 2018 book, Brandon Valeriano, Benjamin Jensen, and Ryan Maness noted that cyber-offensive operations consist of espionage, disruption (temporarily reducing the capacity of an opponent's system), and degradation (damaging of elements of the system).[6] But in contrast to the two secretaries, these authors do not see offense as dominant. Other scholars, including former cyber operators, agree with them. They see offense dominance as being overstated. The cost of "breaking into a particular network may be cheap after the tools and infrastructure are in place," but "building and maintaining the infrastructure for a program of sustained operations requires targeting, research, hardware engineering, software development, and training. This is not cheap."[7]

「布蘭登・瓦列里諾亞」、「班傑明・贊臣」、「萊恩・曼尼斯」三人在2018年合著的《網路戰略》乙書中指出，網路攻勢作戰由諜報、中斷(暫時降低對手系統的能力)、損壞(破壞系統的要素)三種手段所組成。[6] 與前述兩位部長不同之處是三位作者並

5 Elisabeth Bumiller and Thomas Shanker, "Panetta Warns of Possible 'Cyber-Pearl Harbor,'" New York Times, October 12, 2012.

6 Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, Cyber Strategy: The Evolving Character of Power and Coercion (Oxford, UK: Oxford University Press, 2018), 11-13.

7 Charles Smythe, "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance," Yale Journal of International Affairs, June 10, 2020, available at <https://www.yalejournal.org/publications/cult-of-the-cyber-offensive-misperceptions-ofthe-cyber-offensedefense-balance>.

不認為網路是攻勢主導，還有一些曾經是網路操作者的學者也有相同看法。他們認為網路攻勢主導的重要性被過度膨脹。「雖然在各項工具與設施到位後，侵入特定網路的成本是低的，但建立並維持某專案設施的持續性運作則需要設定目標、從事研究、硬體工程、軟體開發及訓練等，這些都所費不貲。」[7]

In short, we have well-informed experts with contradictory views on the value of cyber as an offensive weapon. This is consistent with the historical pattern of new technologies. Advocates did not really know the impact of emerging technologies until they were employed in open conflict. Thus, despite advocating defending persistently forward (which is essentially offensive), the U.S. Cyber Command Vision states, "Cyberspace is an active and contested operational space in which superiority is always at risk."[8]

簡言之，我們被各個專家灌輸網路是攻勢武器這種矛盾的價值觀，這種觀念雖然符合新科技的發展史軌跡，但仍須等到這些新興科技運用於公開衝突之中，贊同網路為攻勢武器的人士才能真正理解新興科技的影響。儘管美軍提倡持續性向前防禦，但其本質仍屬攻勢，誠如〈美國網路司令部願景〉文件指出，「網路空間是一個主動競爭的作戰領域，但其中爭取優勢總會面臨巨大的風險。」[8]

So how should we evaluate cyber as a weapon? Clearly, cyber espionage/theft works. It has allowed China, Iran, North Korea, Russia, and numerous criminal organizations to steal personal information, intellectual property, and money on a scale not seen before.

所以我們要如何視網路為一項武器呢？明顯的案例是網路諜報與竊取，這讓中共、伊朗、北韓、俄羅斯及許多犯罪組織得以竊取個人資料、智慧財產權及金錢，這種規模是前所未見的。

Cyber disruption also has a record of limited success as indicated by repeated attacks from the Love Bug virus to NotPetya malware. A significant number of these attacks have disrupted the targeted systems for a period ranging from hours to weeks. NotPetya also caused significant damage to numerous organizations that were not the target of its attack but were simply

8 Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command (Fort George G. Meade, MD: U.S. Cyber Command, 2018), 6, available at <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.

collateral damage. These incidents indicate that cyber disruption attacks can assist an offense but are inherently difficult to coordinate with real-time attacks-and to date have not reliably produced the desired effects.

網路中斷也曾達成有限的成功紀錄，如愛蟲病毒到NotPetya惡意軟體等一連串的網路攻擊事件。這種大量的攻擊次數能讓電腦目標系統中斷，時間從數小時至數週之久。NotPetya惡意軟體也造成許多組織的大量損失，雖然這些組織非該惡意軟體的攻擊目標，但光是連帶損失就很可觀了。這些事件指出，網路中斷攻擊雖然可以協助攻擊作為，但在本質上是難以配合即時攻擊的，因為迄今尚未有產生所望效應的案例可供參考。

Destructive attacks have also had limited success, the most famous being the Stuxnet attack on the Iranian centrifuges attributed to the United States and Israel. This attack reportedly damaged about 20 percent of the centrifuges, yet the International Atomic Energy Agency reported that Iranian production increased during the period-perhaps in response to the attack.[9] Increasing the uncertainty about the offense-defense balance in cyber, there have been other operations, such as SolarWinds/Holiday Bear, that have achieved widespread penetration of computer networks but whose objective remains unclear.[10]

摧毀式攻擊過去成功的例子為數不多，最有名的案例是攻擊伊朗離心機的震網病毒，背後的策劃者為美國與以色列。據報導，該攻擊雖然造成離心機二成功能受損，但國際原子能署指出，伊朗反而在那段期間增加產量，研判應是作為攻擊的回應。[9] 網路攻守平衡也逐漸增加不確定性，因為還有一些如SolarWinds公司供應鏈遭駭與Holiday Bear駭客攻擊等事件，都已造成電腦網路被大量入侵，但其目的為何尚不得而知。[10]

There are two other major options, however, that have not been used to date in cyber attacks that require much deeper study-kinetic weapons and EMP. Kinetic attacks can damage the well-mapped networks of fiber optic cables, switches, downlink stations, and processing centers essential to an information network. The increasing availability of long-range,

9 John Glaser, "Cyberwar on Iran Won't Work. Here's Why," CATO Institute, August 21, 2017, available at <https://www.cato.org/commentary/cyberwar-iran-wont-work-hereswhy>.

10 "Examining the SolarWinds/Holiday Bear Hack: SIPA Experts Consider the Shifting Standards of Cyberespionage," Columbia University School of International and Public Affairs, available at <https://www.sipa.columbia.edu/news/examining-solarwindsholiday-bearhack>.

autonomous, precision weapons means cross-domain attacks from land, sea, and air platforms will be an integral part of counter-cyber operations. The potential to hit hundreds of key nodes either in theater or even in the United States is growing.

然而，尚有動能武器與電磁脈衝這兩個重要選項，迄今仍未用於網路攻擊，這是需要做更深入研究的地方。動能攻擊可以摧毀鋪設於各地的光纖電纜、轉換器、下載鏈路站，以及與資訊網路相關的資料處理中心等。長程、自主、精準武器的逐步發展與部署，意味著來自陸、海、空武器平台的跨領域攻擊，將成為反制網路作戰的整體作為之一，而且不管是戰區內，甚或是美國本土的數百個關鍵節點，遭攻擊的可能性也因而提升。

The fact that the Internet was initially designed to work even when under major attack will mitigate the impact of kinetic attacks, but the attacks will still cause significant disruptions. Fortunately, the Internet is a complex adaptive system and thus will show remarkable resilience when under attack. EMP attacks will be dealt with in the following section on electromagnetic domain.

網路的設計初衷是用來維持運作，當其遭受重大攻擊時，將使動能攻擊的力量減弱，同時也會造成重大的運作中斷情形。所幸網路是一個具適應力的複合系統，同時也能在遭受攻擊時展現出無比的韌性。接下來，將在電磁頻譜部分說明電磁脈衝攻擊的問題。

Electromagnetic Spectrum
電磁頻譜作戰領域

In January 2021, General John Hyten, Vice Chairman of the Joint Chiefs of Staff, stated, "We have to be able to effectively fight and win the electromagnetic spectrum fight right from the beginning-that is, electronic warfare in every domain."[11] Given the increasing reliance on communications networks, highlighted by the Pentagon's efforts to create the Joint All-Domain Command and Control system, the ability to use the electromagnetic spectrum or deny

11 Theresa Hitchens, "'Spectrum Superiority' Key to All Domain Operations: Gen. Hyten," Breaking Defense, January 7, 2021, available at <https://breakingdefense.com/2021/01/spectrum-superiority-key-to-all-domainoperations-gen-hyten/>.

an opponent its use will be critical to success. Although it has not been officially designated a domain by the Pentagon, the electromagnetic spectrum requires the same level of thought and effort as the five named domains.

2021年1月，時任美國參謀首長聯席會議副主席「約翰・海登」上將指出，「美軍從一開始就必須有效作戰並贏得電磁頻譜領域的勝利，意即要從各作戰領域的電子戰著手。」[11] 鑒於五角大廈所建立的聯合全域指管體系，未來必將愈來愈依賴通信網絡，因此運用電磁頻譜能力或讓敵無法使用該能力，便成為作戰成功的關鍵要素。美國國防部雖然尚未將電磁頻譜列為作戰領域之一，但吾人仍需有與其他五個作戰領域相同的思維與作為。

Once again, land-based defenders may well have an advantage in this domain; they can use fiber optic communications systems to avoid the electromagnetic domain. In addition, they have access to the national power grid to provide effectively unlimited power for jammers.

陸基的防禦者同樣在該領域具有優勢，因為其能使用光纖通信系統，以避免電磁頻譜領域的攻擊，此外還能使用國家電網系統，以有效維持干擾器的電力穩定。

A potential gamechanger in the electromagnetic spectrum is an EMP weapon. These weapons represent a major threat from the tactical to the strategic levels. At the tactical level, the United States has demonstrated a drone that can create an EMP directed at specific targets. Since it is delivered by a drone, this type of attack is really a cross-domain attack but, like kinetic attacks, must be considered as part of any cyber offense-defense balance.

電磁頻譜領域中可能的戰局扭轉者應是電磁脈衝武器，其對戰術乃至戰略層級構成重大威脅。在戰術層級，美國已驗證無人機可以對特定目標發起電磁脈衝攻擊，既然電磁脈衝是由無人機所發動，這類攻擊就是真正的跨領域攻擊，雖然也像是動能攻擊，但必須將之納入網路攻守易位制衡的思維內。

A defending unit can do more to harden its electronics against this kind of attack than an attacker can. However, EMP weapons can overturn the defender's advantage if the defender has not exploited the inherent advantage of the defense. We know these attacks can cause major damage to unprotected electronics, and even the most basic systems today have embedded electronics. The attacker has one major advantage: he can attempt to employ his

EMP weapon before any of his own systems are within range of the pulse. Yet if they cannot prevent a response in kind, the attacker loses the advantage when a retaliatory strike hits his forces.

防守方單位可以做比攻擊者還多這類防範攻擊的強化電子措施；然而，若防禦者不去利用這種防禦的先天優勢，電磁脈衝武器就會反轉防禦者的優勢。我們知道這類攻擊能對未防護的電子設備造成損壞，況且今日大多數的基礎系統都內建電子儀器。攻擊者有一個重大優勢，其在自身電子設備進入防守方電磁脈衝武器的範圍之前，同樣可以試著部署電磁脈衝武器，不過攻擊者也須備妥因應之道，否則其部隊在面臨報復攻擊時將喪失優勢。

For both offense and defense, building resilient, redundant systems can reduce the damage done by tactical EMP weapons but will be costly and require massive retrofits for existing weapons. Of course, the miniaturization necessary for offensive systems will make them significantly more expensive.

不管是對攻擊方或防守方而言，建立具韌性的備用系統，可以降低受戰術電磁脈衝武器所造成的損壞，但其所費不貲，因為將需要大規模更新現有武器系統。至於攻擊武器系統的小型化也是必要作為，且將付出更高的成本。

At the strategic level, a nuclear-generated high-altitude EMP could seriously damage the national infrastructure for a period of months. The fact that this type of attack currently requires a nuclear device to be detonated over the target area means that it must be discussed as part of nuclear deterrence/warfare. At the same time, the cost of protecting civilian systems from large-scale EMP weapons will be extraordinarily high. Large-scale EMP weapons are truly weapons of mass destruction and thus should be treated as part of a nuclear deterrence program. Since all major powers can deploy large-scale EMP weapons, perhaps the best that can be hoped for is the stability inherent in mutually assured destruction.

在戰略層級，高空核子驅動電磁脈衝將嚴重破壞國家基礎設施，足以癱瘓運作長達數個月之久。當前這類攻擊需要在目標區上方引爆核裝置，這意味著該作為須納入核嚇阻與核戰的作戰計畫之中。於此同時，防護民間系統免於大規模電磁脈衝攻擊的成本將極為龐大。大規模的電磁脈衝是真正的大規模毀滅性武器，因此應視為核嚇阻計畫之一部分。既然各主要強權國都有能力部署大規模電磁脈衝武器，或許追求穩定的最佳之道可能要寄望在「相互保證毀滅」的作法了。

A Caution
注意事項

As always, perception is reality. Unfortunately, the perception that cyber and space are offense dominated is inherently escalatory. If political leaders believe they can achieve decisive dominance in these domains only by attacking first, crisis management becomes much more difficult. Therefore, it is critical to counter the idea that going first in cyber, space, or the electromagnetic spectrum provides unrecoverable advantages. This is not only necessary to prevent aggression but also to prevent escalation on the friendly side.

認知到最後總是成為事實，不幸的是，將網路與太空視為攻勢主導的認知正在逐漸攀升。一旦政治領導人相信只要在這些作戰領域優先運用攻勢作為，就得以達到決定性主導優勢，則危機管理將變得更為困難，因此導正在網路、太空或電磁頻譜領域中攻勢優先的想法至關重要，否則將喪失作戰先機，重要的是不僅要避免我方躁進的行動，同時也要避免友軍陣營的躁動情形。

Interaction Between Domains
作戰領域間的互相影響

Understanding the relative strengths of the offense and defense in the various domains is essential to the joint warfighter. For instance, while degradation or destruction has proved to be a difficult challenge within the cyber domain, the use of precision weapons delivered from land, sea, air, or space can have a devastating effect on the cyber capabilities of an opponent. Unclassified sources provide maps of critical nodes and links (downlinks, fiber optics, and terrestrial switches) of many commercial networks that could allow massive attacks across the networks.[12]

理解在各作戰領域中攻擊與防禦的相對力量對聯合作戰的戰士的確至關重要。例如，要使網路領域全面損壞或摧毀，並不是一件簡單的任務，但只要使用來自陸、海、

12 Matthew Cole, "A Dissertation So Good It Might Be Classified," Wired, January 1, 2004, available at <https://www.wired.com/2004/01/a-dissertation-so-good-itmight-be-classified/>; "Finding Fiber in Your Area May Be Easier Than You Think," GEOTEL, available at <https://www.geo-tel.com/finding-fiber-in-your-area-may-be-easierthan-you-think/>.

空或太空的精準武器攻擊敵資訊設施，就能對敵網路能力造成極大的破壞力。由於透過公開來源資訊能找到許多商業網路的關鍵節點與鏈路(如下行鏈路、光纖線路、地面轉換器)分布圖，這也讓大規模網路攻擊成為可能。[12]

The increasing range and number of autonomous precision-attack systems are steadily improving the ability of the land, sea, and air domains to conduct effective cross-domain attacks. Ground-based forces have the advantages of operating in complex terrain (whether rural or urban) and access to deep magazines and national power grids. The increasing ranges of ground force weapons will allow defenses to reach out much farther to target land, sea, and air forces as well as critical infrastructure for space and cyber forces.

自主式精準攻擊武器系統的射程與數量日益增加，正不斷改變陸、海、空作戰領域的能力，進而遂行更有效的跨領域攻擊。地面部隊在複雜多變的地形中(不管是鄉村或都市)具有地利優勢，因為不僅彈藥補給充足，而且也能使用國家電網的電力系統。地面部隊武器的射程日益增加，將使防守方能進一步延伸鎖定敵陸、海、空軍部隊的距離，甚至是及於太空與網路部隊所使用的關鍵基礎設施。

All-domain offensive operations are incredibly complex, not least because each domain operates on different execution timelines. Major land and naval operations take from weeks to years to execute. It can take weeks to position the forces for air operations, but they can be executed in hours with campaigns lasting days to weeks. Cyber, space, and electronic warfare operations can also take weeks to years to put forces in place but can measure execution in microseconds to days. Thus, coordinating the offensive operations of the separate domains is particularly challenging-yet cross-domain attacks may be the most effective. Space Development Agency Director Derek Tournear has stated that cyber is a greater threat to satellites than missiles.[13] Air forces have stated for years that the most effective way to defeat an air force is to destroy its bases and its aircraft on the ground. Today, ground-based forces can do this from beyond the range of most aircraft delivered weapons. Naval forces have historically been able to appear suddenly out of the vast expanses of the oceans but

13 Sandra Erwin, "DOD Space Agency: Cyber Attacks, Not Missiles, Are the Most Worrisome Threat to Satellites," Space News, April 14, 2021, available at <https://spacenews.com/dod-space-agency-cyber-attacks-notmissiles-are-the-most-worrisome-threat-tosatellites/>.

increasingly are being closely tracked by space assets. In short, cross-domain attacks will become more powerful but will be an order of magnitude more difficult than coordinating a defense.

全領域的攻勢行動極為複雜，尤其是因為各領域有其各自的作戰期程。重大的陸上與海上作戰執行時間須耗時數週至數年不等，在為時數日至數週的戰役中，空中作戰陳兵佈陣數週，但也許在數小時就執行完畢。網路、太空和電子戰行動也是一樣，耗費數週至數年來部署兵力，執行時間可以從微秒至數天不等。因此，雖然各個作戰領域在攻勢作戰合作上極富挑戰性，但跨領域的攻擊應是最具作戰效能，誠如美國太空發展署署長「德瑞克・圖爾尼爾」指出，網路對衛星的威脅更勝於飛彈。[13] 空軍部隊數年來咸認，最有效打擊空軍的方式是摧毀其基地與地面上的飛機，如今地面部隊可以做到在大部分飛機的武器射程外發動打擊。海軍部隊在過往歷史上都能突然現身於廣闊的外海，但如今其一舉一動已在太空設備的嚴密追蹤下。簡言之，跨領域攻擊雖然較具威力，但將比防禦的合作要更困難十倍。

What Does It Mean for the United States?
對美國之意涵

If the United States leads the shift to defense dominance in land, air, and sea domains while maintaining the ability to contest the space, cyber, and electromagnetic domains, it gains major strategic advantages. Perhaps the greatest advantage will lie in deterring aggression. MIT political scientist Stephen Van Evera argued that war is more likely to occur when the tactical offense dominates the battlefield because conquest is perceived to be easy. He listed 10 reasons leaders were more likely to take their nations to war under these conditions than during periods when the defense dominates tactically. During periods of defense dominance, then, aggression becomes less likely simply because the probability the attacker succeeds decreases greatly.[14] Fortunately, in the two current Great Power competitions, the United States is essentially on the tactical defensive. To achieve regional hegemony, both China and Russia will have to cross borders and seize territory; the United States and its allies only have todefend.

美國若能主導陸、海、空作戰領域的防禦主流，再加上維持在太空、網路及電磁領域的競爭力，就能取得重大戰略優勢，或許最大成效在於嚇阻進犯行為。美國麻省理工

14 Stephen Van Evera, Causes of War: Power and the Roots of Conflict (Ithaca, NY: Cornell University Press, 1999).

學院(MIT)政治學者「史蒂芬・范・埃佛拉」認為當戰術攻勢主導戰場時，會認定攻克對方是容易的，導致戰爭更有可能發生。他列舉十個理由指出，為何領導人在攻勢主導期會比在戰術防禦主導期，更有可能將其國家帶往戰爭。在防禦主導期，進犯行為較不可能發生是因為攻擊方成功的機率大為降低。[14] 所幸當前美國在與「中」、俄兩大國的競爭中，美國基本上是採取戰術防禦。為了成為區域霸權國，「中」、俄兩國都必須跨越邊界並奪取領土，美國及其同盟只要做好防禦準備即可。

In Asia, China has worked hard to develop antiaccess/area-denial (A2/AD) capabilities for the region. Fortunately for the allies, A2/AD works both ways. As defense becomes dominant, the United States can cooperate with its allies and friends to take advantage of the fact that they are separated by water from China. They can create an A2/AD based on the First Island Chain. A family of smart and relatively inexpensive weapons on the First Island Chain can both deny China commercial use of the East and South China seas and prevent either China's navy or merchant ships from reaching the Pacific Ocean. Already existing cruise missiles, drones, and smart sea mines can create a defense in depth. Japan, Australia, South Korea, and Singapore all have the capability to produce these systems. By applying advanced manufacturing techniques, they can produce them in large numbers. The United States can cooperate with them to co-produce these weapons and then train together to employ them in concert with existing land-, sea-, and air-based platforms. This strategy reinforces deterrence because it directly addresses three of China's strategists' greatest fears: being cut off from global trade (the Malacca Dilemma), the desire for certainty in military planning, and the impact of a long war on domestic stability.

在亞洲，中共致力於發展區域內「反介入與區域拒止」(A2/AD)能力。所幸對美國盟邦而言，「反介入與區域拒止」有相互的運作面向(一面是中共運作，另一面是美國及其盟邦運作)。只要防禦成為主流，美國可以與其盟邦和盟友合作，善用它們各自被中共海域所隔開的地理環境，意即在第一島鏈的基礎下，建立一道「反介入與區域拒止」防線。在第一島鏈運用一系列智能與成本不高的武器，不僅能阻斷中共在東海與南海的商業通道，而且也能避免中共海軍與商船進入太平洋。既有的巡弋飛彈、無人機、智慧水雷能開創防禦縱深，而日本、澳洲、南韓、新加坡各國都有生產這些武器系統的能力，同時在先進製造技術的協助下，就能以大規模數量生產。美國可以與這些國家合作共同生產這類武器，並共同訓練如何部署於陸基、海基及空基平台。這種戰略能強化嚇阻，因為其直接命中中共戰略家最擔憂的要害：切斷全球貿易通路(如同麻六甲困

境)、軍事計畫作為需要確定性、長期戰爭對國內穩定的衝擊。

While the tactical situation is dramatically different in Europe, the North Atlantic Treaty Organization (NATO) can also exploit the rising dominance of defense to deter and, if necessary, deny Russian incursions into Eastern Europe. The combination of inexpensive short-range drones, loitering munitions, cruise missiles, mines, and improvised explosive devices (which could easily include 50,000 pounds of explosives in a 20-foot container full of fertilizer) could immediately create responsive, thick belts for a defense in depth. This approach solves NATO's number one problem in defending Eastern Europe-the inability to deploy sufficient forces before Russia can mobilize its own forces for an invasion. While a Russian invasion is both highly unlikely and not in keeping with Russian doctrine, NATO planners have focused on the intractable problem of reinforcing Eastern European states.

然而在歐洲的戰術情況截然不同，北約組織(NATO)也可以利用興起中的防禦主流趨勢進行嚇阻，必要時遏制俄羅斯入侵東歐。結合運用成本不高的短程無人機、滯空彈藥、巡弋飛彈、水雷及即製爆裂物(5萬磅炸藥可以輕易藏在一個裝滿肥料的20呎貨櫃內)等，就可以立即開創一個供防禦縱深使用的既靈活又堅固的陣地帶。這種方法解決北約在防禦東歐時的最大問題：無法有效在俄羅斯動員部隊發動入侵前完成軍隊部署。雖然俄羅斯不太可能入侵東歐，俄羅斯準則也沒有入侵的設計；鑒此，北約計畫人員應先將重點置於解決東歐各國間錯綜複雜的問題。

Unfortunately, these plans are often conceived in terms of heavy armor units deploying from home stations to the battle front. The Alliance lacks the funding, the will, and the infrastructure to forward deploy the number of heavy armor units, aviation, and logistics support necessary to execute such a defense before the Russians can mobilize.[15] By adopting

15 See Max Bergmann and Siena Cicarelli, "NATO's Financing Gap: Why NATO Should Create Its Own Bank," Center for American Progress, January 13, 2021, available at <https://www.americanprogress.org/issues/security/reports/2021/01/13/494605/natosfinancing-gap/>; "WIN/Gallup International's Global Survey Shows Three in Five Willing to Fight for Their Country," Gallup International, May 7, 2015, available at <https://www.gallup-international.bg/en/33483/win-gallupinternationals-global-survey-shows-three-infive-willing-to-fight-for-their-country/>; Kevin Blanchford, "Can NATO and the EU Really Defend the Baltic States Against Russia?" The National Interest, February 7, 2020, available at <https://nationalinterest.org/blog/buzz/cannato-and-eu-really-defend-baltic-states-againstrussia-121711>.

a defense that reinforces selected existing systems with small, smart, and numerous systems, NATO can create an affordable force that can mobilize faster than the current Russian forces.

不幸的是，這些計畫的構思往往是讓重裝甲單位從駐地部署至前線，並未思索北約同盟缺乏資金、意志、供前進部署重裝甲和航空單位使用的基礎設施，以及在俄羅斯動員前執行防禦所需的必要後勤支援等問題。[15] 北約藉由採取防禦態勢可以強化既有的特定武器系統，如小型、智能型和其他眾多系統等，也應建立一支財政可負擔且比俄軍動員速度更快的軍隊。

Today, the United States faces flat (effectively decreasing after inflation) defense budgets as well the need to modernize its nuclear triad while facing major maintenance backlogs in its air and naval inventories. Fortunately, the rising dominance of defense provides an opportunity to shift from the previous generation of few but exquisite weapons systems such as the F-35 and Gerald R. Ford-class carriers to the new generation of smart, small, and much less expensive systems that take advantage of the shift to defense.[16] This approach meets America's need to support its allies and efficiently deter its enemies, even as its effective defense budget decreases.

今日，美國面臨國防預算編列持平(在通貨膨脹後實質減少)，以及在推動核武鐵三角現代化的同時，又面臨海、空軍武器庫也需要維持費的壓力。所幸防禦主流趨勢逐漸興起提供一個契機，讓當前世代如F-35戰機與福特號航空母艦等某些少量精密的武器載台，得以轉型成新一代的小型化、智能化及更節省成本的武器系統，這些都是回歸「防禦至上」所能獲得的好處。[16] 即使在美國實質國防預算減少的情況下，這種方式可以滿足美國須支援其盟國並有效嚇阻敵人之需求。

(111年4月18日收件，111年8月16日接受)

16 See T.X. Hammes, Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons, Policy Analysis No. 786 (Washington, DC: The Cato Institute, 2016), available at <https://www.cato.org/policy-analysis/technologies-converge-powerdiffuses-evolution-small-smart-cheap-weapons>.