中共軍事現代化及網路作為
China's Military Modernization And Cyber Activities

譯者簡介

鄧炘傑備役少校，管院專9期、國防大學政治作戰學院英文正規班、中原大學企管研究所碩士；曾任排長、連長、地區補給庫分庫長、教準部編譯官，現任特約翻譯、華語／英語專業領隊／導遊。

As a member of the US-China Economic and Security Review Commission, I will present some of the commission's findings on China's military modernization, US- China security relations, and China's cyber activities from the 2013 Annual Report to Congress.The views I present today, however, are my own. I want to acknowledge the fine work of our staff in preparing the annual report and especially the excellent research of our foreign policy and security staff in helping to prepare this testimony.

作為美中經濟暨安全檢討委員會的一員，我會將2013年度報告中有關中共軍事現代化、美中安全關係，以及中共網路行動等研究結果呈報給國會。不過今天的報告，純屬個人觀點。同時也藉此對撰擬年度報告及負責外交與國安研究同仁致謝。

China's Military Modernization
中共的軍事現代化

China's military, the People's Liberation Army (PLA), is undergoing an extensive modernization program that presents significant challenges to US security interests in Asia. This modernization includes creating a surveillance and strike architecture that supports operations at longer distances away from China's coast. It makes the PLA a more formidable force in all the dimensions of war: air, space, land, sea, and in the electromagnetic spectrum. The PLA has new, multi-mission-capable combat ships, aircraft, submarines, and new

generations of missiles.

中共人民解放軍(PLA) 正在進行中的全面現代化計畫，已經對美國在亞洲的安全利益形成重大挑戰。這些現代化，包括能遠離海岸支援其作戰的監視與打擊能力，讓共軍在空中、太空、陸地、海洋、電磁等所有作戰空間，都成為一支令人生畏的武力。共軍擁有新型多功能水面戰艦、戰機、潛艦，以及新一代的飛彈。

First and foremost, major elements of this program-such as the DF-21D antiship ballistic missile and increasing numbers of advanced submarines armed with antiship cruise missiles-are designed to restrict US freedom of action throughout the Western Pacific. The PLA is rapidly expanding and diversifying its ability to conduct conventional strikes against US and allied bases, ships, and aircraft throughout the region, including those that it previously could not reach with conventional weapons, such as US military facilities on Guam. As the PLA's anti-access/area-denial capabilities mature, the costs and risks to the United States for intervention in a potential regional conflict involving China will increase.The Chinese military, of course, sensitive to nineteenth and twentieth century history, thinks of these actions as counter-intervention strategies designed to prevent foreign militaries from intervening in China's sovereign affairs or territory.

首先，這些方案中的要項－例如東風21D彈道反艦飛彈，以及數量日增配備了巡弋反艦飛彈的先進潛艦－無不為拘束美國在西太平洋的行動自由而設計。解放軍全面打擊美國及其盟邦的基地、船艦、飛機的戰力快速膨脹與多樣化，以往無法以其傳統武器觸及的設施，如關島，亦難以倖免。一旦中共反介入／區域阻絕能力成熟，美國要干預、牽涉中共的區域衝突，其風險與代價都將升高。當然，有鑑於對19、20世紀歷史外力介入中國主權與領土的敏感歷史，中共認為反干預戰略等諸般行動，無非只在為此作準備。

Furthermore, the PLA's rapidly advancing regional power projection capabilities enhance Beijing's ability to use force against Taiwan, Japan, and rival claimants in the South China Sea. More seriously, because China's military doctrine emphasizes preemptive attacks, it raises the stakes in any crisis. Many potential security scenarios could require the US military to defend US regional allies and partners as well as maintain open and secure access to the air and maritime commons in the Western Pacific.

此外，共軍快速增長區域武力投射能力，以加強北京對於臺灣、日本，以及南中國海的敵對勢力、使用武力的本錢。更麻煩的是，中共的軍事準則強調先下手為強，在任何衝突中都很容易擦槍走火。在西太平洋地區，許多衝突想定都必須由美國出面防衛地區盟邦，並確保空中、海上公共領域的開放與安全。

At the same time, rising unease over both China's expanding capabilities and increasing assertiveness is driving US allies and partners in Asia to improve their own military forces and

strengthen their security relationships with each other. These trends could support US interests in Asia by lightening Washington's operational responsibilities in the region.

在此同時，中共擴張軍力和與日俱增的自信，促使美國的亞太盟友積極強化軍力，並強化彼此的安全結盟關係。這種趨勢減輕了華府在亞洲地區的作戰責任，符合美國利益。

On the other hand, if China's neighbors pursue military capabilities that could be used offensively or preemptively due to the perception that the United States will be unable to follow through on its commitment to the rebalance to Asia, this could undermine US interests in the region.

另一方面，如果中國鄰邦，認為美國無法信守亞洲再平衡的承諾，軍力方面朝向能採取攻勢或先制作戰的方向擴充，則不利於美國在此一地區的利益。

In the commission's 2013 annual report we discuss the following main developments in China's military modernization:

在本委員會2013年度報告中，我們對中共軍事現代化的重大發展，討論如下：

Navy
海軍

Aircraft Carriers. Since commissioning its first aircraft carrier, the Liaoning, in September 2012, China continues to develop a fixed-wing carrier aviation capability, which is necessary for the carrier to carry out air defense and offensive strike missions. The Liaoning is a former Russian aircraft carrier purchased from the Ukraine. It was refitted and modernized in China. The PLA Navy conducted its first successful carrier-based takeoff and landing with the Jian-15 (J-15) in November 2012, certified its first group of aircraft carrier pilots and landing signal officers on the carrier's first operational deployment from June to July 2013, and verified the flight deck operations process in September 2013.The Liaoning will continue to conduct short deployments and shipboard aviation training until 2015 to 2016, when China's first J-15 regiment is expected to become operational. The J-15 is a Chinese copy of the Russian Su-33. China likely intends to follow the Liaoning with at least two domestically produced hulls. The first of these appears to be under construction and could become operational before 2020.

航空母艦：在第一艘航母遼寧號於2012年9月正式服役以來，中共一直持續發展定翼艦載機戰力，俾能遂行防空及打擊任務。遼寧號是中共從烏克蘭買來的前俄羅斯航母，在中共進行艤裝與現代化。2012年11月，殲-15首次在遼寧號成功完成起降；2013年6～7月，第一批艦載飛行員及著陸信號官通過驗證；2013年9月，完成飛行甲板作業程序驗證。2015～2016年，遼寧號將持續進行短期程的部署並實施艦載機飛行訓練，一直到其第一個殲-15殲擊團完成戰備。殲-15戰機是中共仿俄製蘇愷-33所研發出來。中共繼遼寧號之後，或將至少自行打造2艘航母艦體；第一艘判已在建造中，應可在2020年之前

投入戰備。

Submarine-Launched Ballistic Missiles. China's Julang-2 (JL-2) submarine- launched ballistic missile is expected to reach initial operational capability very soon.The missile has been under development for a number of years, which shows that Chinese military industries still have some problems in developing and fielding new systems. The JL-2, when mated with the PLA Navy's Jin-class nuclear ballistic missile submarine (SSBN), will give China its first credible sea-based nuclear deterrent. The Jin SSBN/JL-2 weapon system will have a range of approximately 4,000 nautical miles, allowing the PLA Navy to target the continental United States from China's littoral waters.China has deployed three Jin SSBNs and probably will field two additional units by 2020.

潛射彈道飛彈：中共的巨浪-2型(JL-2)潛射彈道飛彈預料即將到達初期作戰階段。該型飛彈歷經多年研發，顯示中共軍事工業在新系統的發展與服役過程中，尚有若干問題。一旦巨浪-2型飛彈搭配晉級核動力潛艦(SSBN)，將讓中共首度擁有可靠的核子嚇阻能力。晉級核動力潛艦搭載巨浪-2型飛彈，射程約4,000浬，使中共海軍可以從沿海直接瞄準美國本土目標。中共現有3艘晉級潛艦，2020年前可望再部署兩艘。

Sea-Based Land Attack Capability. China currently does not have the ability to strike land targets with sea-based cruise missiles. However, the PLA Navy is developing a land attack capability, likely for its Type-095 guided-missile attack submarine and Luyang III guided-missile destroyer. Modern submarines and surface combatants armed with land attack cruise missiles (LACM) will complement the PLA's growing inventory of air-and ground-based LACMs and ballistic missiles, enhancing Beijing's flexibility for attacking land targets throughout the Western Pacific, including US facilities in Guam.

海基攻陸能力：中共目前並無從海上發射巡弋飛彈，攻擊陸上目標的能力。然而，其海軍正透過095型導彈攻擊潛艦，和旅洋3型導彈驅逐艦發展這種能力。現代化潛艦及水面戰艦，只要配備攻陸巡弋飛彈(LACM)，可以增強當前數量日增的陸基及空基巡弋飛彈與導彈，讓北京可以肆意攻擊西太平洋，包含關島在內的所有陸上目標。

Shipbuilding. The PLA Navy continues to steadily increase its inventory of modern submarines and surface combatants. China is known to be building seven classes of ships simultaneously but may be constructing additional classes.Trends in China's defense spending, research and development, and shipbuilding suggest the PLA Navy will continue to modernize. By 2020, China could have approximately 60 submarines that are able to employ submarine-launched intercontinental ballistic missiles, torpedoes, mines, or antiship cruise missiles. China's surface combat force also has modernized and expanded with approximately 75 surface combatants that are able to conduct multiple missions or that have been extensively upgraded since 1992.The combat fleets are supported by a combat logistics force that can

conduct underway replenishment and limited repairs. All of these ships will be equipped to take advantage of a networked, redundant command, control, communications, computer, intelligence, surveillance, and reconnaissance system (C^4ISR) fielded by the PLA.

造艦：共軍海軍之現代化潛艦與水面戰艦的數量，一直穩定成長。中共正同步建造7個不同級別的艦艇，甚至不只這些。從中共的國防預算、研發、造艦的趨勢看，其海軍將持續邁向現代化。預判2020年，中共將有60艘配備潛射洲際彈道飛彈、魚雷、水雷，和反艦巡弋飛彈的先進潛艦。水面戰力方面，其數量與現代化程度亦將持續提升。1992年迄今，約有75艘水面戰鬥艦經過性能提升，並能執行多項任務。後勤兵力可以為艦隊進行海上補給及部分維修作業。所有艦艇均將具備網路化的備份指揮、管制、通信、信息、情報、監視、偵察(C^4ISR)系統。

Attack Submarines. China has a formidable force of 63 diesel-electric and nuclear attack submarines.They are equipped with nuclear and conventional torpedoes and mines as well as antiship cruise missiles.In 2012, China began building four "improved variants" of its Shangclass nuclear attack submarine. China also continues production of the Yuan-class diesel-electric submarine-some of which will include an air-independent propulsion system that allows for extended duration operations- and the Jin-class SSBN. Furthermore, China is developing two new classes of nuclear submarines and may jointly design and build four advanced diesel-electric submarines with Russia.China's growing submarine inventory will significantly enhance China's ability to strike opposing surface ships throughout the Western Pacific and to protect future nuclear deterrent patrols and aircraft carrier task groups.

攻擊潛艦：中共目前擁有63艘柴電或核動力攻擊潛艦。配備核子及傳統魚雷、水雷，以及反艦巡弋飛彈。2012年，中共開始建造4艘「改良版」商級核動力攻擊潛艦。元級柴電動力潛艦也在建造中，其中有些還採用了絕氣推進系統，可提供潛艦更長的作戰時間；晉級核子彈道導彈潛艦，則已全面採用這項技術。此外，除了正在建造的2艘新型核動力潛艦，中共還跟俄羅斯合作設計、建造4艘先進的柴電動力潛艦。數量持續成長的潛艦，讓中共有能力攻擊出現在西太平洋的敵方船艦，並保護未來成軍的核子嚇阻巡邏及航母戰鬥群。

Air Force
空軍

Fighter Aircraft. China also is developing two next-generation fighters, the J-20 and the J-31, which could feature low observability and active electronically scanned array radar.The PLA Air Force conducted the first test flights of the J-20 and J-31 in January 2011 and October 2012, respectively.These aircraft will strengthen China's ability to project power and gain and maintain air superiority in a regional conflict.

戰鬥機：中共目前正在發展兩型下一世代戰機，殲-20和殲-31。這兩型戰機都屬於低能見度(low observability)，且配備了主動電子掃瞄相列雷達。共軍空軍殲-20和殲-31分

別在2011年1月和2012年10月，進行首次試飛。這些新型戰機，將有助於中共強化武力投射能力，以及在區域衝突中取得並保持空優。

Cargo Transport Aircraft. In January 2013, China conducted the first test flight of its indigenously developed cargo transport aircraft, the Yun-20 (Y-20). China previously was unable to build heavy transport aircraft, so it has relied on a small number of Russian Ilyushin-76 (IL-76) aircraft for strategic airlift since the 1990s. Aircraft specifications provided by official Chinese media indicate the Y-20 can carry about twice the cargo load of the IL-76 and about three times the cargo load of the US C-130.The Y-20 will enhance the PLA's ability to respond to internal security crises and border contingencies, support military international peacekeeping and humanitarian assistance operations, and project power in a regional conflict. The larger aircraft and expanded fleet will enhance the PLA's capability to employ the 15th Airborne Army, part of the PLA Air Force.

運輸機：2013年1月，中共對自製的運-20運輸機實施首次試飛。1990年代迄今，中共因為無法自製重型運輸機，所以依靠少數俄製伊留申-76型運輸機來擔任戰略運輸任務。依據中共官方媒體透露，運-20可以搭載的貨物為伊留申-76之兩倍，約為美製C-130運輸機3倍。運-20運輸機可以強化共軍針對境內衝突或邊境緊急事件的反應能力、有效支援國際維和及人道救援行動，並在區域衝突中執行武力投射。更大型飛機和擴建的機隊，也有助於共軍更有效運用隸屬空軍的空降兵第15軍。

LACM-Capable Bomber Aircraft. In June 2013, the PLA Air Force began to receive new Hongzha-6K (H-6K) bomber aircraft. The H-6K, an improved variant of the H-6 (originally adapted from a late-1950s Soviet design), has extended range of around 2,400 to 3,100 miles and can carry China's new long-range LACM, the CJ-10. The CJ-10 has a range of around 900 to 1,200 miles.The bomber/LACM weapon system provides the PLA Air Force with the ability to conduct conventional strikes against regional targets throughout the Western Pacific, including US facilities in Guam.Although the H-6K airframe could be modified to carry a nuclear-tipped air-launched LACM, and China's LACMs likely have the ability to carry a nuclear warhead, there is no evidence to confirm China is deploying nuclear warheads on any of its air-launched LACMs.The H-6K also may be able to carry supersonic antiship cruise missiles.

可搭載攻陸巡弋飛彈的轟炸機：2013年7月，共軍空軍開始接收轟-6K轟炸機。轟-6K是轟-6的改良版(轟-6原型是依蘇聯1950年代設計改良而成的)，作戰半徑從2,400哩，延伸到3,100哩，而且可以搭載新式的長劍-10攻陸巡弋飛彈；長劍-10的攻擊半徑大約900～1,200哩。轟炸機與巡弋飛彈的搭配，讓其空軍有能力在西太平洋對區域性目標進行傳統的打擊，包含美國在關島的軍事設施在內。雖然轟-6K的機身結構經過修改，可以攜帶配備核子彈頭的空射攻陸巡弋飛彈，而中共的巡弋飛彈，據信也有能力配備核子彈頭；但目前並沒有證據確定，中共在空射攻陸巡弋飛彈上，配置了核子彈頭。轟-6K

應該可以搭載超音速反艦巡弋飛彈。

Space and Counter-space
太空與反太空

In May 2013, China fired a rocket into nearly geosynchronous Earth orbit, marking the highest known suborbital launch since the US Gravity Probe A in 1976 and China's highest known suborbital launch to date. Although Beijing claims the launch was part of a high-altitude scientific experiment, available data suggest China was testing the launch vehicle component of a new high-altitude anti-satellite (ASAT) capability.If true, such a test would signal China's intent to develop an ASAT capability to target satellites in an altitude range that includes the US global positioning system (GPS) and many US military and intelligence satellites. In a potential conflict, this capability could allow China to threaten the US military's ability to detect foreign missiles and provide secure communications, navigation, and precision missile guidance.

2013年5月，中共發射了1枚火箭進入地球同步軌道；這是繼美國在1976年執行「重力探測A」計畫之後，中共最為世人所知的次軌道探索行動。雖然北京對外宣稱這是高空科學實驗的一部分，但從已知數據可以推斷，中共正藉此測試其高空反衛星能力。若然，這種測試，就表示中共有意發展反衛星戰力，其高度包括美國全球衛星定位系統，跟其他軍事及偵察衛星為標的。潛在衝突中，中共如果具備了這種能力，將可以威脅到美國偵察外國飛彈、提供加密通訊、導航和飛彈精密導引等任務遂行。

Furthermore, in September 2013, China launched a satellite into space from the Jiuquan Satellite Launch Center in western China. Our annual report cites commentary from Gregory Kulacki of the Union of Concerned Scientists, who believes that this launch may represent a capacity to launch new satellites in the event China suffers losses in space from space combat.

此外，2013年9月，中共從西部的酒泉衛星發射中心，發射了一枚衛星進入太空。我們的年度報告中引述了「科學家關懷聯會」庫拉克基(Gregory Kulacki)的評論，他表示這次發射行動，代表了中共就算在太空戰爭中遭受損失，還是有能力發射新的衛星進入太空。

China also has improved its ballistic missile defense capabilities by fielding the Russian-made SA-20B surface-to-air missile (SAM) system. In some cases, China's domestically produced CSA-9 SAM system should also be capable of intercepting ballistic missiles.

中共還藉著部署俄製SA-20B地對空飛彈系統，來強化其彈道飛彈防禦能力。某些情況下，中共自製的CSA-9地對空飛彈，也有攔截來襲的彈道飛彈之能力。

On 27 December 2012, China announced its Beidou regional satellite navigation system is fully operational and available for commercial use. Using 16 satellites and a network of ground stations, Beidou provides subscribers in Asia with 24-hour precision navigation and timing

services.China plans to expand Beidou into a global satellite navigation system by 2020.Beidou is a critical part of China's stated goal to prepare for fighting wars under "informationized conditions," which includes a heavy emphasis on developing the PLA's C^4ISR and electronic warfare capabilities. The PLA is integrating Beidou into its systems to improve its command and control and long-range precision strike capabilities and reduce the PLA's reliance on foreign precision navigation and timing services such as GPS.

2012年12月27日，中共宣布其北斗區域性衛星導航系統可充分運作，並供商業運用。使用了16顆衛星，及一整套由電腦網路連線的地面站台組成，可提供亞洲用戶全天候的精確導航與對時服務。中共計畫在2020年前，將北斗擴大成全球衛星導航系統。北斗是中共設定「在信息條件下」作戰的目標中，很重要的部分；這個目標特別強調發展共軍的C^4ISR及電子作戰能力。共軍正在將北斗這套系統加以整合，以提升指揮、管制及長程精準打擊能力，並且降低共軍對類似全球衛星定位系統(GPS)這些外國精準導航及對時服務系統的依賴。

Strategic Intercontinental Ballistic Missiles
戰略洲際彈道飛彈

China is enhancing its nuclear deterrent capability by modernizing its nuclear force. It is taking measures such as developing a new road-mobile intercontinental ballistic missile (ICBM), the DF-41. This missile could be equipped with a multiple independently targetable reentry vehicle (MIRV), allowing it to carry as many as 10 nuclear warheads.In addition to MIRVs, China could also equip its ballistic missiles with penetration aids and may be developing the capability to transport ICBMs by train.Furthermore, according to the DoD's 2011 report to Congress on China's military, the PLA "has developed and utilized [underground facilities] since deploying its oldest liquid-fueled missile systems and continues to utilize them to protect and conceal their newest and most modern solid-fueled mobile missiles."

中共正藉核子武力現代化，以強化其核子威懾能力；所採行的措施，包括發展新的道路機動式洲際彈道飛彈(ICBM) ── 東風-41型。這套飛彈系統配備了多目標重返大氣層載具(MIRV，譯註：又稱分導式多彈頭，是多彈頭發展的另外一個型態，也可以算是多彈頭重返大氣層載具的功能強化版)，可攜帶多達10枚核子彈頭。除了MIRV之外，中共也將這型彈道飛彈配置了彈頭穿透輔助(penetration aids)功能，也可能發展鐵道運送。此外，根據國防部2011年呈給國會的中共軍事報告，共軍「正在發展並利用其地下設施，來部署老式的液體燃料導彈系統，並保護及隱藏其最新、最現代化的固體燃料導彈」。

Defense Spending
國防支出

To support its military modernization, China continued to increase defense spending in 2013. In March, China announced its official defense budget for 2013 rose 10.7 percent in

nominal terms to $117.39 billion, signaling the new leadership's support for the PLA's ongoing modernization efforts. This figure represents 5.3 percent of total government outlays and approximately 1.3 percent of estimated gross domestic product (GDP).China's official annual defense budget now has increased for 22 consecutive years and more than doubled since 2006. Most Western analysts agree Beijing likely will retain the ability-even with slower growth rates of its GDP and government revenue-to fund its ongoing military modernization.

為了支持其國防現代化，中共在2013年持續增加國防支出。3月份，中共公布其2013年官方版國防預算增加了10.7%，達到1,173億9千萬元；顯示新的領導階層，支持共軍持續現代化的方向。該數據占了政府總預算的5.3%，國內生產毛額(GDP)的1.3%。官方的國防預算已連續22年增加，2006年來更是倍增。大部分西方分析家都同意，即使國內生產毛額成長趨緩，政府稅收不如預期，北京還是要持續挹注其國防現代化。

It is difficult to estimate China's actual defense spending due to the uncertainty involved in determining how China's purchasing power parity affects the cost of China's foreign military purchases and domestic goods and services, as well as Beijing's omission of major defense-related expenditures. Some purchases of advanced weapons, research and development programs, domestic security spending, and local government support to the PLA are not included in China's official figures on defense spending. The Institute of International Strategic Studies assesses China's actual defense spending is 40 to 50 percent higher than the official figure.The US Department of Defense estimated China's actual defense spending in 2012 fell between $135 and $215 billion, or approximately 20 to 90 percent higher than its announced defense budget.

正確估算中共真正的國防支出並不容易，因為很難確知購買力平價指數對國外軍火採購、國內軍品及服務的成本影響，猶如其刻意隱瞞的重大國防支出。若干先進武器採購、研發計畫、內安支出，及地方政府支付額度等，都不包括在官方國防預算中。「國際關係研究所」評估，中共實際國防支出較官方數字高出40～50%。美國國防部判斷中共2012年國防支出，約在1,350～2,150億之間，較其公開數字高出約20～90%。

US-China Security Relations
美中安全關係

US-China military-to-military relations deepened and expanded in 2013 after several years of setbacks. From 2012 to 2013, the number of US-China military-to-military contacts more than doubled from approximately 20 to 40.In particular, contact between the US Navy and the PLA Navy increased significantly during this time frame. Key military-to-military contacts in 2013 included the first port visit by a US Navy ship to China since 2009, the first port visit by a Chinese ship to the United States since 2006, and the second ever US-China counter-piracy exercise. Additionally, China in March 2013 accepted the invitation, first extended by then Secretary of Defense Leon Panetta in September 2012, to participate in the US-led multilateral

Rim of the Pacific Exercise near Hawaii in 2014.

美國與中共的軍事關係，在2013年經過多年的停滯之後，有更深入與更廣泛的交流。從2012～2013年，美中之間的軍事接觸次數，從原本大約20增加到40次，攀升了不只一倍。尤其是美國海軍與共軍海軍之間的往來，在這段期間更是明顯頻繁。2013年重大的軍事接觸，包括2009年以來，第一次美軍船艦造訪中共，以及2006年來第一次共軍船隻訪問美國；還有就是美中兩國有史以來第二度的反海盜演習。此外，中共在2013年3月正式接受2012年9月由當時美國國防部長里昂・潘內達(Leon Panetta)的邀請，參加2014年由美國主導，在夏威夷附近舉行的多國環太平洋演習。

The DoD contends that a strong military-to-military relationship develops familiarity at the operational level. The department argues that this reduces the risk of conflict through accidents and miscalculations, builds lines of communication at the strategic level that could be important during a crisis, contributes to better overall bilateral relations, and creates opportunities to obtain greater contributions from China to international security. US Pacific Command commander ADM Samuel Locklear in July 2013 said, "The progress that we're making between our two militaries is quite commendable ……because we are able to have very good dialogue on areas where we converge, and there are a lot of places where we converge as two nations, and we're also able to directly address in a matter-of-fact way where we diverge."

國防部認為，加強軍事交流，有助於雙方在作戰階層的相互瞭解，降低因為意外及錯估形勢造成衝突的機率。在危機時刻於戰略階層建立溝通管道，促進雙方友好關係，並進而創造契機使中共與國際安全關係更加穩固。美國太平洋總部司令洛克利爾(Samuel Locklear)海軍上將2013年7月表示：「兩軍之間的關係進展成效斐然……正因為雙方有良好的對話基礎，所形成的共識就可以擴展到兩個國家；即使在某些可能看法會有分歧的地方，也能在實質的基礎上直接對話」。

There have been eight rounds of strategic dialogue between China and the United States, currently managed by the Pacific Forum-CSIS. This is a Track 1.5 dialogue that involves some representatives from the US government in attendance, but virtually all Chinese participants are from some part of their government. The past several rounds of the dialogue have dealt with some of the most important strategic issues facing China and the United States, including nuclear strategic stability; the relationship between cyber attacks, space warfare, and nuclear stability; ballistic missile defense; and strategic early warning. Officers from China's strategic missile forces have been in attendance at the dialogue. I see this as one of the most productive dialogues taking place with China. The PLA is an active participant. Ideally such discussions should be direct, government-to-government talks, but it is encouraging that the PLA and the Chinese Foreign Ministry are engaged on these matters.

在戰略與國際研究中心(CSIS) 主辦的太平洋論壇中，中共與美國之間已經有過八度的戰略層級對談。這是一項1.5軌的會談，美方代表有些是政府官員，但中方的出席者，

沒有例外都來自政府各部門。過去幾個回合，討論內容都是中共跟美國將會面臨到最重要的戰略議題，包含核子戰略穩定、網路攻擊、太空作戰、網路攻擊、彈道飛彈防禦，及戰略早期預警等。中共戰略飛彈部隊出身的軍官，也出席了會談。個人認為這是與中方所有會談中，最具有建設性的。共軍方面確實積極參與。這種會議如果是直接由雙方政府對口，固然很理想；令人高興的是共軍和中共外交部也參與其中。

In another positive development, in mid-November, the US Army and the PLA ground forces conducted their first ever field exercise together. The exercise was focused on disaster relief and took place in Hawaii.

另一個正向的發展，是11月中旬雙方地面部隊，舉行了雙方有史以來第一次實兵聯合演習。演習地點在夏威夷，重點放在災害救助。

My own experience in direct military-to-military contacts with China leads me to advise caution in what we do with the PLA and what we show them. In my opinion, the wise limitations placed by Congress on military exchanges with China in the National Defense Authorization Act (NDAA) of 2000 should not be lifted. The commission's annual report also reflects this sentiment. Military-to-military contacts with China require careful oversight to ensure that the United States does not improve China's capability against our own forces, Taiwan, or our friends and allies in the Asia-Pacific region.

以我個人經驗來說，這種和中共軍方對軍方的直接往來，比較要注意的是：和共軍演練什麼，以及我們拿出來的是什麼。我認為，國會於2000年通過的國防授權法(NDAA)不可取消，本委員會的年度報告，也反映了此一看法。雙方的軍事接觸，必須仔細監督，以免讓共軍增強了對付美國、臺灣，或是其他亞太盟邦的能力。

Enhanced military-to-military contacts between China and the United States in 2013 took place in the context of China's efforts to rebrand the bilateral relationship as a "new type of major-country relationship." This concept, promoted heavily in 2013 by Chinese President Xi Jinping and other high-level Chinese officials, posits the United States and China should, as two major powers, seek to cooperate on a range of bilateral and global issues while avoiding the kind of harmful competition that often characterizes relationships between dominant powers and rising ones.

2013年間與美國軍方頻繁的軍事接觸，再次顯示中共有意讓世界各國瞭解，這是它與美國之間「新型大國關係」。中共國家主席習近平和其他高階官員，於2013年提出這種概念之後不遺餘力地大聲鼓吹，認為世人應該把中共和美國等量齊觀，在雙邊關係和全球議題上相互合作之餘，並避免傳統大國和新興強權之間的惡性競爭。

Cooperation is a good thing, but US military leaders cannot lose sight of the PLA's record on human rights. This dictates practical limitations on what we do with China's armed forces.

The principal mission of China's military is to keep the Chinese Communist Party (CCP) in power, as we saw in the way that the PLA was used during the 4 June 1989 Tiananmen Massacre and in Tibet.

相互合作是件好事，但是美國軍方高層不可忽視共軍過往的人權紀錄。這表示美國與中共解放軍的作為，還是要設定一個底線。共軍的主要任務，是要維護中國共產黨的權力；他們採用的方式，就像1989年6月4日天安門的大屠殺，以及西藏的鎮壓行動。

China's Cyber Activities
中共的網路作為

While China continues to develop its navy, air force, missile forces, and space and counter-space capabilities, in Chinese military writings, cyberspace is an increasingly important component of China's comprehensive national power and a critical element of its strategic competition with the United States.Beijing seems to recognize that the United States' current advantages in cyberspace are allowing Washington to collect intelligence, exercise command and control of military forces, and support military operations. At the same time, China's leaders fear that the United States may use the open Internet and cyber operations to threaten the CCP's legitimacy.

當中共持續發展其海、空軍、飛彈部隊，及太空與反太空戰力時，軍事相關文件中，已經將網路空間視為中共整體國力與美國戰略競逐要項的重要一環。北京似乎已經認定，就是因為握有網路優勢，美軍才能在情報蒐集、指揮管制和軍事行動上無往不利。同時，中共領導階層也很忌憚美國以開放的網際空間和網路，威脅到共產黨統治的正當性。

Since the commission's 2012 Annual Report to Congress, strong evidence has emerged that the Chinese government is directing and executing a large-scale cyber espionage campaign against the United States. China to date has compromised a range of US networks, including those of DoD and private enterprises. These activities are designed to achieve a number of broad security, political, and economic objectives.

本委員會2012年度向國會提呈的報告中，已經有明顯證據顯示，中共政府正主導、執行對美大規模的網路諜報活動，迄今已危及美國許多網路，包括國防部和私人企業；這些作為旨在達到其安全、政治、經濟等目的。

There are no indications the public exposure of Chinese cyber espionage in technical detail throughout 2013 has led China to change its attitude toward the use of cyber espionage to steal intellectual property and proprietary information. The report by Mandiant, a US private cyber-security firm, about the cyber espionage activities of PLA Unit 61398 merely led the unit to make changes to its cyber "tools and infrastructure" to make future intrusions harder to detect and attribute.There are about 16 technical reconnaissance (signals intelligence) units

and bureaus in the PLA and at least seven electronic warfare and electronic countermeasures units.Each of China's seven military regions is supported by an electronic countermeasures regiment, and it looks like the PLA Second Artillery Force has its own supporting unit.These organizations focus on cyber penetrations, cyber espionage, and electronic warfare.

目前沒有跡象顯示2013年間，中共的網路諜報活動，在技術層面上已經轉向偷竊智慧財產跟專利權資訊。美國一家民營網路安全公司「曼迪安特」(Mandiant)發表針對共軍61398部隊的報告，不過只讓該部隊更加精進其「工具與基礎設施」，使爾後的入侵更難偵測。共軍大約有16個(信號情報)技術偵察單位和局處，和至少7個電子作戰／電子反制單位。中共七大軍區，都各自編配了一個電子反制團；二砲部隊，應該也有其電子支援單位。這些組織的任務，就是進行網路滲透、網路諜報及電子作戰。

When confronted with public accusations from the United States about its cyber espionage, Beijing usually attempts to refute evidence by pointing to the anonymity of cyberspace and the lack of verifiable technical forensic data. It also shifts the media focus by portraying itself as the victim of Washington's cyber activities and calling for greater international cooperation on cyber security.In a press conference on the day after Mandiant released its report in February 2013, a spokesperson for China's Ministry of Foreign Affairs said, "Groundless speculation and accusations regarding hacker attacks, for various purposes, is both unprofessional and irresponsible and it is not helpful for solving the problem." He also emphasized cyber attacks are a serious problem for China.

當面對美國公開指控進行網路諜報活動時，北京經常以網路空間的匿名特性，以及缺乏確切的證據加以反駁；還反過來把自己形容成華盛頓網路行動的受害者，並呼籲在網路安全方面更緊密的國際合作，試圖轉移媒體焦點。在2013年2月曼迪安特公司召開記者會公布報告後次日，中共外交部一位發言人就說：「關於我國進行駭客攻擊，是沒有事實根據的推測和指控，背後隱藏了多種目的；這不只是不專業、不負責任的做法，對於解決問題也毫無幫助」。他特別強調，中共也同樣面臨嚴重的駭客攻擊問題。

However, a number of public US government reports, admissions by private companies that they have been the target of cyber espionage, investigations by cyber-security firms, and US press reporting contradict Beijing's long-standing denials. While attribution is difficult and takes great skill, trend analysis is allowing cyber-security professionals to develop a more comprehensive understanding of Chinese cyber actors, tools, tactics, techniques, and procedures.

然而，許多曾因網路諜報活動受害的公司，和網路安全機構調查結果，以及媒體等呈報給美國政府的公開報告，都反駁北京方面的一再否認。雖然查證困難而且也極費工夫，但是趨勢分析家透過網路安全專業，已經能對中共網路行動的參與單位、工具、策略、技術和程序，有更全面的瞭解。

Threats to US National Security
對美國國家安全的威脅

China's cyber espionage against the US government and defense industrial base poses a major threat to US military operations, the security and well-being of US military personnel, the effectiveness of equipment, and readiness. China apparently uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on US strategies and plans, enable future military operations, shorten research and development (R&D) timelines for military technologies, and identify vulnerabilities in US systems and develop countermeasures.

中共針對美國政府和國防工業設施進行的網路間諜活動，對美國的軍事行動、美軍人員的安全福祉、裝備效能與作戰整備等，都已經形成威脅。很明顯的，中共用這種方法補救其研究計畫不足之處、設定未來目標、蒐集美國的戰略和計畫情報，以強化未來軍事作戰能力、縮短軍事科技研發時程，並找出美國的弱點，來發展反制手段。

Military doctrine in China also calls for attacks on the critical infrastructure of an opponent's homeland in case of conflict. In July 2013, a threat researcher at Trend Micro, a private Japanese cyber-security firm, claimed he had detected a Chinese cyber intrusion, commencing in December 2012, of a honeypot.He had created the honeypot to resemble the industrial control system of a water plant in the United States. The researcher attributed the intrusion to Unit 61398, based on forensic analysis.If true, this suggests Unit 61398 is collecting intelligence on critical infrastructure in addition to other targets. Such activities are consistent with PLA doctrine, which explains that one function of wartime computer network operations is to "disrupt and damage the networks of [an adversary's] infrastructure facilities, such as power systems, telecommunications systems, and educational systems."

中共的軍事準則，也強調如果發生衝突，應該對敵方國境內重要設施發動攻擊。2013年7月，日本民營網路安全公司「趨勢科技」(Trend Micro)的一位威脅研究員宣稱，透過他偽裝成美國一家自來水工廠的工業控制系統，設下稱為「蜜罐」的陷阱，發現從2012年12月起，中共進行的網路入侵。根據該研究員分析，入侵的單位就是61398部隊。如果此情屬實，表示61398部隊正對美國的重要設施及其他目標蒐集情報。這些行動與共軍準則記載相吻合，也可以解釋準則中所述：作戰時期電腦網路作戰的功用之一，在於「干擾並破壞敵方設施網絡，諸如電力、通訊及教育系統等」。

A number of instances of Chinese cyber espionage targeting US national security programs have been identified in recent years. In May 2013, the Washington Post described a classified report by the Defense Science Board, which lists more than 24 US weapon system designs the board determined were accessed by cyber intruders. The Washington Post reported, "Senior military and industry officials with knowledge of the breaches said the vast majority

were part of a widening Chinese campaign of espionage against U.S. defense contractors and government agencies." The list includes the Patriot missile system, Aegis ballistic missile defense system, the F/A-18 fighter, the V-22 Osprey multirole combat aircraft, and the Littoral Combat Ship.

近年來，已經有不少證據顯示，中共網路間諜確實以美國的國家安全計畫作為攻擊目標。2013年5月，華盛頓郵報引述一份來自國防科學局的機密報告指出，24項以上由該局認可的美製武器系統，都遭受到網路駭客入侵。華盛頓郵報說：「對網路破壞有深刻瞭解的軍事、工業資深官員表示，大部分他們所掌握的中共網路間諜行動所針對的目標，都是美國國防合約商，跟政府機構」。表列中包含愛國者飛彈、神盾飛彈防禦系統、F/A-18大黃蜂戰機、V-22魚鷹多功能戰機，以及淺海戰鬥艦等。

Information gained from intrusions into the networks of US military contractors likely improves China's insight into US weapon systems, enables China's development of countermeasures, and shortens China's research and development timelines for military technologies.In addition, the same intrusions Chinese cyber actors use for espionage also could be used to prepare for offensive cyber operations. Chinese cyber actors could place latent capabilities in US software code or hardware components that might be employed in a potential conflict between the United States and China.

透過這種網路入侵方式，從美國軍火合約商那裡獲得的資訊，有助於更加瞭解美國的武器系統、使中共得以發展出反制策略，並且縮短軍事科技的研發時程。此外，中共網路駭客使用的諜報及入侵手段，同樣可以用在網路攻勢作戰之準備。中共駭客可能在美國軟體代碼或硬體元件上，預先植入潛伏性病毒，當美國與中共之間發生潛在衝突時，就可以加以利用。

There has been concern in recent years about security risks to the DoD's supply chain. In a meeting in May 2013, commissioners and DoD officials discussed the department's interpretation of US law regarding procurement sources. DoD officials indicated a stricter procurement evaluation standard that includes sourcing concerns could be applied only to items on the United States Munitions List. Items outside this list are judged by a different standard, which some officials believe might preclude concerns about the origin of products. For example, items procured for C^4ISR maintenance facilities are not subject to stricter scrutiny. Commissioners raised concerns that this interpretation of the law was limiting the department's ability to address potential risks arising from certain procurement sources. Commissioners urged the DoD to expand the purview of the stricter standard to items beyond the munitions list.

近年來國防補給體系的安全問題，業已引發關注。2013年5月，本委員會委員與國防部官員共同召集一場會議，旨在探討國防部對採購來源相關法令的詮釋。會議中，國防部代表指出，評鑑彈藥相關品項採購來源的標準較嚴格，而彈藥以外，如C^4ISR的保

修設備，則另有標準。若干官員認為，如此就可能忽視了這些品項的來源。與會委員也認為國防部的詮釋，確實限縮了因應某些採購品項，因其來源產生風險的能力，因而呼籲國防部應將較嚴格的標準，一體適用於彈藥以外的採購品項。

The DoD is currently moving in this direction. Section 806 of the NDAA for Fiscal Year 2011 (Public Law 111-383), is intended to address the problem, but it has yet to be fully implemented. Section 806 authorizes the secretary of defense and the secretaries of the Army, Navy, and Air Force to reject procurement sources for information technology on grounds of protecting supply chain security if they receive a recommendation to do so from the DoD.The department is in the process of implementing Section 806, having conducted tabletop exercises and written the Defense Federal Acquisition Regulation Supplement Rule implementing Section 806. As of May the rule was undergoing interagency coordination.These changes to DoD procurement ultimately may provide officials with the flexibility they need to protect all DoD systems. However, progress has been slow and the problem the commissioners highlighted will remain until the new policy is implemented, potentially posing a threat to national security. Therefore, in the 2013 Annual Report the commission recommends Congress urge the administration to expedite progress in its implementation of Section 806 of the NDAA for Fiscal Year 2011.

國防部目前正朝此方向前進。2011會計年度國防授權法案(公法111-383)第806款，就是打算要解決這個問題，但尚未竟其功。806款授權國防部長和陸、海、空三軍部長，為了保護補給體系安全，當接獲國防部的建議，將可依法否決某些資訊科技設備的採購決議。國防部正在推動806條款的運作，不但進行沙盤推演，同時擬訂推動806條款相關的「聯邦國防採購補充規則」，5月份進入跨部會協調階段。這些改變讓國防部系統防護官員擁有更大彈性。但整個過程緩慢，除非新規定付諸實施，委員所重視的問題仍對國安形成威脅。因此，在2013年年度報告中，委員會就建議國會督促行政部門加速推動，2011會計年度提出的國防授權法案第806條款。

Developments in cloud computing in China may present cyber-security risks for US users and providers of cloud computing services and may also have implications for US national security. Based on the findings of a report by Defense Group Inc. for the commission, the relationship between the Ministry of State Security (MSS) and the Chongqing Special Cloud Computing Zone represents a potential espionage threat to foreign companies that might use cloud computing services pr ovided from the zone or base operations there.In addition, the plan to link 21Vianet's data centers in China and Microsoft's data centers in other countries suggests the Chinese government one day may be able to access data centers outside China through Chinese data centers.With concerns about espionage in mind, in the 2013 Annual Report, the commission recommends Congress direct the administration to prepare an inventory of existing federal use of cloud computing platforms and services and determine where the data storage

and computing services are geographically located. Such inventory should be prepared annually and reported to the appropriate committees of jurisdiction.

中共的雲端運算發展，對美國的使用者、雲端運算服務供應商，甚至國家安全都有影響。根據防衛集團公司(Defense Group Inc.)為美中經濟暨安全檢討委員會所提供的報告顯示，中共國家安全部(MMS)和重慶特殊雲端運算區之間的關係，代表中共很有可能透過該區或者其他基地可操控的雲端伺服器，針對外國公司進行網路諜報滲透。此外，中共21世紀互聯網資料中心，和其他國家微軟公司連線的計畫，讓中共政府他日就可透過資料交換進入其他國家資料中心。基於對中共網路滲透的疑慮，2013年度報告中就建議國會應該要求行政部門備妥聯邦現行使用的雲端平台完整清單，並決定資料儲存和伺服器將來要設立何處。此一清單應每年修正一次，並呈報法定委員會。

Cloud computing also could improve the PLA's C^4ISR capabilities. DGI writes that cloud computing "could enable more effective and flexible development and deployment of military equipment, while at the same time improving the survivability of the PLA's information systems by endowing them with greater redundancy (allowing a system's capabilities to survive the disabling or destruction of any individual node)."

雲端運算也能強化共軍C^4ISR的能力。防衛集團公司表示，雲端科技「可以讓軍事裝備的發展和部署更具效率與彈性，同時讓體系在個別節點失能或受損時，其能力得以存活」。

Threats to US Industry
對美國企業的威脅

China's cyber espionage against US commercial firms poses a significant threat to US business interests and competiveness in key industries. This cyber espionage complements traditional human espionage. Through these efforts, the PLA and China's defense industries are able to leapfrog ahead in technologies and systems and fill in gaps in their own research and development capabilities at a considerable savings in time and money. Gen Keith Alexander, commander of US Cyber Command, assessed the cost to US companies of intellectual property theft is about $250 billion a year, although not all the losses are due to Chinese activity. Chinese entities engaging in cyber and other forms of economic espionage likely conclude that stealing intellectual property and proprietary information is much more cost-effective than investing in lengthy R&D programs.These thefts support national science and technology development plans that are centrally managed and directed by the PRC government.

中共對美國公司進行的網路滲透，已經對美國的商業利益和重要企業的競爭力，造成重大威脅。網路滲透與傳統諜報人員的刺探行動可以相輔相成。透過這些手段，共軍與中共國防工業不但在技術上突飛猛進，在研發方面可藉此填補技術落差，更可節省相當可觀的研究時間與經費。美國網路指揮部指揮官亞歷山大(Keith Alexander)將軍評估，包括中共網軍所造成的損害在內，美國公司每年在智慧財產權上面的損失，大約是2,500億美元。中共透過網路諜報偷竊智慧財產和所有權資訊所獲得的進展，比耗費時間自行

研發，算起來要划算得多。這種對國家科技發展大有幫助的偷竊計畫，其實是由中國共產黨政府部門集中管理與主導的。

The Chinese government, primarily through the PLA and the Ministry of State Security, supports these activities by providing state-owned enterprises information and data extracted through cyber espionage to improve their competitive edge, cut R&D timetables, and reduce costs. The strong correlation between compromised US companies and those industries designated by Beijing as "strategic" industries further indicates a degree of state sponsorship, and likely even support, direction, and execution of Chinese economic espionage.Such governmental support for Chinese companies enables them to out-compete US companies, which do not have the advantage of leveraging government intelligence data for commercial gain.

中共政府最主要是透過共軍和國家安全部，以網路間諜的方式進行資料蒐集，提供給國營機構，藉此增加競爭優勢，縮短研發時程，並降低成本。某些原本與美國合作關係密切的公司與企業，及北京指定的，甚至某種程度受國家資助的「戰略性」工業，均可能協助支援、指導、執行中共商業間諜的任務。受中共政府支援的公司，因為還能獲得官方商業情報資料加以利用，在競爭力方面明顯優於美國公司。

It is difficult to quantify the benefits Chinese firms gain from cyber espionage. We do not know everything about the kinds of information that is targeted and taken, nor do we always know which Chinese actor stole the information. Some thefts may take place that are never detected. In terms of business intelligence, some targets of cyber theft likely include information related to negotiations, investments, and corporate strategies including executive e-mails, long-term business plans, and contracts.

很難計算這些公司從網路間諜活動中，到底獲得了多少利益；因為我們無法界定哪一類的資訊會被鎖定、盜取，更不知道哪些公司在從事這些勾當。許多行之有年的商業竊取行為，至今仍沒有被發現。就商業情報的範疇來說，網路間諜會有興趣竊取的標的，包括協商內容、投資標的、合作策略、長期計畫與合約等。

In addition to cyber theft, Chinese companies almost certainly are acquiring information through traditional espionage activities, which limits our ability to identify the impact of cyber espionage in particular. Nevertheless, it is clear that China not only is the global leader in using cyber methods to steal intellectual property, but also accounts for the majority of global intellectual property theft.Chinese actors have on several occasions in recent years leveraged cyber activities to gain sensitive or proprietary information from US enterprises:

除了網路之外，幾乎所有中國公司當然也沿用傳統的諜報行為，使得我們無法正確估算，網路竊取的衝擊範圍到底有多大。不過有一點很確定：中共不但是使用網路方式

竊取智慧財產權之首，而且大部分智慧財產權剽竊事件，都跟中共有關。近幾年中共利用網路，從美國企業獲取機密或私有資訊的案例如下：

● In the report by Mandiant mentioned earlier, there is evidence that since 2006 PLA Unit 61398 has penetrated the networks of at least 141 organizations, including companies, international organizations, and foreign governments. These organizations are either located or have headquarters in 15 countries and represent 20 major sectors, from information technology to financial services. Of those organizations penetrated, 81 percent were either located in the United States or had US-based headquarters. According to Mandiant, Unit 61398, gained access to a wide variety of intellectual property and proprietary information through these intrusions. Unit 61398 is the Second Bureau of the PLA's technical reconnaissance department, based in Shanghai.

●根據前述曼迪安特公司透露，證據顯示2006年開始，共軍61398部隊，已經對至少141個包括公司、國際機構，與外國政府組織進行滲透。這些組織或其總部分別位於15個國家，涵蓋包括資訊科技與金融服務在內的20個領域。這些被滲透的組織，81%位於美國，或將總部設於美國。根據該公司的瞭解，61398部隊已經透過入侵，為盜取各種智慧財產和私人資訊建立了管道。61398部隊隸屬共軍技術偵察部第二處，基地設在上海。

● In another high-profile example of a Chinese company allegedly targeting a US company's intellectual property through cyber espionage, the Department of Justice (DoJ) in June 2013 filed charges against Sinovel Wind Group, a Chinese energy firm, alleging Sinovel stole intellectual property from Massachusetts-based company American Superconductor (AMSC).Once Sinovel was able to reproduce AMSC's technology after stealing its proprietary source code, the Chinese firm broke the partnership, cancelled existing orders, and devastated AMSC's revenue. AMSC has sought compensation from Sinovel through lawsuits in China, an effort which is ongoing and has resulted in legal fees for AMSC exceeding $6 million.While these lawsuits continue to move slowly through the Chinese legal system, adding to AMSC's legal fees, Sinovel is reaping the profits of stolen technology.

●另一個傳得沸沸揚揚有關中共鎖定美國公司竊取智慧財產的案例，跟美國司法部有關。司法部2013年6月起訴一家中共能源公司 ── 華銳風電集團(Sinovel Wind Group)，偷取美國麻州的美國超導體公司(American Superconductor，AMSC)之智慧財產權。華銳風電集團竊取了專利的原始碼，複製AMSC的技術以後，就取消合夥關係，取消訂單，嚴重損害AMSC的營收。AMSC已經透過中共法院對華銳提出賠償訴訟；目前進行中的法律程序，該公司必須支付600餘萬美金的訴訟費用。當中共法院系統進入冗長費時的訴訟程序時，華銳集團已經用偷來的技術獲利。

Deterring Chinese Cyber Theft
遏阻中共的網路偷竊

It is clear that attempting to name the perpetrators in China in an attempt to shame the Chinese government is not sufficient to deter Chinese entities from conducting cyber espionage against US companies. Mitigating the problem will require a well- coordinated approach across the US government and with industry. Many potential actions are being discussed by Congress, the Obama administration, and outside experts. These actions include linking economic cyber espionage to trade restrictions, prohibiting Chinese firms using stolen US intellectual property from accessing US banks, and banning US travel for Chinese organizations that are involved with cyber espionage. The US-China Economic and Security Review Commission recommends Congress take the following actions:

很明顯，想靠著指名道姓揭露中共的網路犯罪者，讓中共政府因自慚形穢而停止這些對付美國公司的間諜行為，看來是行不通的。要解決這個問題，有賴美國政府和企業界暢通的協調。國會、歐巴馬政府，和相關專家學者已經在討論可能的反制措施，包括將經濟型的網路間諜活動，與貿易限制結合起來，不准中方企業從美方偷來的智慧財產進出銀行體系，並禁止參與網路間諜活動的中共機構進出或通行美國。「美中經濟暨安全檢討委員會」建議國會採取以下措施。

● Adopt legislation clarifying the actions companies are permitted to take regarding tracking intellectual property stolen through cyber intrusions.

●立法允許智慧財產被竊的公司，可以網路入侵方式追蹤盜竊源頭。

● Amend the Economic Espionage Act (18 U.S.C. § 1831-1839) to permit a private right of action when trade secrets are stolen.

●修改經濟間諜法案，當商業機密被盜時，允許採取適當行為，維護私有權利。

● Support the administration's efforts to achieve a high standard of protection of intellectual property rights in the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (TTIP).

●支持行政部門的作為，在「泛太平洋夥伴關係」 (TPP)及「泛大西洋貿易與投資夥伴協定」(TTIP)中，完成對智慧財產權的高標準保護。

● Encourage the administration to partner with other countries to establish an international list of individuals, groups, and organizations engaged in commercial cyber espionage. The administration and partner governments should develop a process for the list's validation, adjudication, and shared access.

●鼓勵行政部門與他國合作，建立涉及商業網路間諜的個人、群體及組織清單。行政部門及合作國政府應將清單之驗證、司法管轄及分享方式，研擬一套程序。

● Urge the administration to continue to enhance its sharing of information about cyber threats with the private sector, particularly small- and medium-sized companies.
●呼籲行政部門加強與民間，特別是中、小型公司，分享網路威脅資訊。

My personal view is that the president already has the authority to place sanctions on Chinese persons, government industries, and companies through the International Emergency Economic Powers Act.If the magnitude of the damage to the US economy is as great as that cited by General Alexander, the president should exercise that authority.
我個人的看法是，總統早就可以依據「國際緊急經濟權力法」，對中共不法的個人、國營企業和公司實施制裁。如果對美國經濟的危害程度，確如亞歷山大將軍之前所引述，總統就應該依法執行這個權力。

Sustaining the US Military's "Rebalance" to Asia
維持美國在亞洲地區的軍力「再平衡」

In January 2012, DoD's Defense Strategic Guidance declared the US military will "of necessity rebalance toward the Asia Pacific" by emphasizing existing alliances, expanding its networks of cooperation with "emerging" partners, and investing in military capabilities to ensure access to and freedom to maneuver within the region.US Chief of Naval Operations ADM Jonathan Greenert explained the US Navy's role in the rebalance: "As directed by the 2012 Defense Strategic Guidance ……the [US] Navy formulated and implemented a plan to rebalance our forces, their homeports, our capabilities, and our intellectual capital and partnerships toward the Asia Pacific."Specifically, the US Navy aims to increase its presence in the Asia Pacific from about 50 ships in 2013 to 60 ships by 2020 and "rebalance homeports to 60 percent" in the region by 2020.
2012年1月，國防部的國防戰略指導，宣布美國軍方將有「維持亞太地區的再平衡之必要」，包括強化現行聯盟關係，擴張與新夥伴的合作網絡，投資軍事力量，以確保進出該地區的自由。美國海軍軍令部長格林爾特(Jonathan Greenert)將軍，解釋美國海軍在所謂「再平衡」的角色：「根據2012年國防戰略指導，……美國海軍執行的一套計畫，透過包括我方軍力、對方母港，以及我方情報總部與夥伴關係等各種整備工作，共同促使亞太地區兵力再平衡」。比較特別的是，美國海軍設法在亞太地區增加曝光率，從2013年的大約50艘軍艦，到2020年時會有60艘；屆時，美國海軍會有60%的船艦，以亞太地區的港口作為母港，也是其再平衡戰略的一個措施。

However, the commission's annual report notes that US Defense Secretary Chuck Hagel

in July 2013 said Washington would have to choose between a smaller, modern military and a larger, older one if sequester level funding continues.[71] Admiral Greenert has warned constraints in the current budget environment could delay or prevent the US Navy from achieving its objectives in the rebalance.[72] There is growing concern in the United States and among US allies and partners that the DoD will be unable to follow through on its commitment to the rebalance due to declining defense budgets and emerging crises elsewhere in the world. This could lead some regional countries to increasingly accommodate China or pursue military capabilities that could be used offensively or preemptively. Either scenario could undermine US interests in the region.

然而，委員會的年度報告也提到，美國國防部長查克・海格2013年7月曾說，如果華盛頓方面維持預算緊縮政策，美國軍力就必須在小而現代化，以及大而過時這兩者之間選擇其一。[71]美國內部以及各盟邦、夥伴都越來越擔心，國防預算降低，以及其他地方的新危機，會不會讓國防部無法維持在亞太地區再平衡的承諾。[72]這可能會讓該地區某些國家向中共靠攏，或是設法增強足以採取攻勢作為或先發制人的軍事力量。以上情況都可能會傷害美國在亞太地區的利益。

I urge you to keep in mind that by 2020, China could have a navy and air force in Asia that outnumbers and almost matches the technical capability of our own forces. If our military force shrinks because of our own budget problems, we may have 60 percent of our forces in the Asia-Pacific region, but 60 percent of 200 ships is far less than 60 percent of a 300-ship navy. That may not be sufficient to deter China or to reassure our friends and allies in the region.

請記住，2020年時，共軍可能就會擁有數量傲視亞洲，技術能力與我們不相上下的海軍及空軍。如果因為預算問題導致美國軍事力量下滑，屆時即使我們還是能部署60%的軍力在亞太地區，但是120艘軍艦的海軍實力，畢竟比180艘的差很遠。這種實力並不足以嚇阻共軍，也無法讓亞太地區的夥伴與盟邦，對我們有足夠的信心。

文章出處：戰略研究季刊，2014年第一季
作者簡介：Wortzel M. Wortzel博士，美國陸軍退役上校，畢業於軍事參謀學院及美國陸軍戰爭學院，夏威夷大學政治經濟碩士及博士學位。32年軍旅生涯中，大多服務於亞太地區。1988~1990之間，擔任美國陸軍駐中共助理武官，1995~1997升任陸軍武官。2001年開始，在美中經濟暨安全檢討委員會任職兩屆。著有《龍飛九天 ── 解放軍實力擴展到全球》一書，2013年出版。