DOI: 10.6915/PMSS.202503_(26).0007
軍事社會科學專刊，第 26 期，頁 163-226 (2025 年 3 月)

Maintaining U.S. Information Advantage from Crisis into Conflict

維持美國從危機到衝突的資訊優勢

涂拉克博士(美國陸軍退役上校) Dr. Arthur N. Tulak, COL, USA, Ret.*

王允昱 Yun-Yu, Wang (翻譯)**

王鵬程 Peng-Cheng, Wang (譯審)***

As the international security situation continues to deteriorate, with wars expanding in Europe and the Middle East, the U.S. must maintain sufficient military forces in these regions to contain those conflicts, while concurrently presenting a credible deterrent to the leaders of Russia, Communist China, and Communist North Korea. America's adversaries are continually calculating the correlation of forces and means, as well as comparisons of comprehensive national power, which could lead to another conflict, as the U.S. and her allies are forced to deter and defend across multiple theaters. In the Indo-Pacific region, the current commitment of forces to other regions could lead to miscalculation by Xi Jinping and Kim Jong Un, as they look for the right opportunity to achieve their clearly intended goals of conquest and subjugation of their ethnically-kin democratic populations in the democratic Republic of China (Taiwan) and the Republic of Korea (ROK). It is imperative that we progress our capabilities to maintain information advantage in the next crisis, as our adversaries continue to plan and prepare to deny such advantage to the U.S. and her Allies and Partners.

隨著國際安全形勢不斷惡化，以及戰爭在歐洲和中東地區蔓延，美國必須在這些地區維持足夠的軍事力量，以有效遏制衝突，同時向俄羅斯、中共和北韓的領導人展示明確且可信的威懾能力。美國的對手持續進行力量與手段相關性的評估，同時比較各方的綜合國力，這種動態分析可能引發新的衝突，因為美國及其盟友被迫在多個戰場上同時進行威懾和防禦。在印太地區，將軍事力量轉移至其他戰場的現況，可能導致習近平與金正恩的誤判，因為他們或將抓住時機，試圖實現其明確的

* 美國陸軍退役上校、美南加州大學教育學博士(Dr. Arthur N. Tulak, COL, USA, Ret)；通訊作者 E-mail：arthur.n.tulak.ctr@us.navy.mil

** 翻譯/王允昱中校：國防大學軍事共同教學中心研究教官

*** 譯審/王鵬程上校：美國陸軍指揮參謀學院 2010 年班、國立中正大學戰略暨國際事務研究所碩士、國防大學戰爭學院教官

目標：征服並控制其血緣相近的民主國家，包括中華民國(臺灣)和南韓的人民。我們必須優先提升自身能力，確保在未來的危機中維持資訊優勢，因為我們的對手正在積極策劃，並準備削弱美國及其盟友與夥伴的此項戰略優勢。

The purpose of achieving information advantage is to gain a decision-making advantage over the adversary, to be able to take decisive action, and to hold onto the offensive in order to be able to dictate the operational terms to an opponent. In crisis and conflict, this advantage will result in cascading effects for the side that cannot anticipate and counter the moves of the adversary. As the Communist People's Republic of China (PRC) is officially the pacing threat for the U.S. military, it is critical for us to understand how the U.S. might contest for information advantage during the crisis phase preceding a major conflict against that specific threat(Cameron Carlson, et al, 2024).

實現資訊優勢的目標，是在決策層面取得對敵方的壓倒性優勢，使美方能夠果斷採取行動，並始終保持攻勢，從而主導敵方的作戰條件。在危機與衝突中，這一優勢將對無法預測並反制敵方行動的一方產生連鎖的毀滅性影響。由於中共已被正式認定為美國軍方的主要威脅，我們必須深入研究如何在面臨此特定威脅的重大衝突前的危機階段，爭奪並維持資訊優勢。

The most significant military threat posed by the PRC is the military invasion of Taiwan. The probability of this invasion has increased dramatically over the last ten years, and many U.S. military leaders have expressed concern that the People's Liberation Army's (PLA) invasion of Taiwan is imminent, and might prove inevitable if the wars in Europe and the Middle East continue and possibly expand to a wider conflict, inviting adventurism from America's adversaries. The Commission on the National Defense Strategy (NDS), in its final report delivered to Congress on July 29, 2024, found that the U.S. was not prepared to meet the security threats facing the U.S., and that the 2022 NDS force construct did not "sufficiently account for global competition *or the very real threat of simultaneous conflict in more than one theater*" based on the increasing political and military cooperation of America's peer or near-peer adversaries, that pose real threats to the U.S. system of alliances and partnerships(Chris Gordon, 2024; Jane Harman, et al, 2024). The commissioners proposed a "multiple theater force construct" that is more reflective of our posture during the Cold War against the Soviet Union, which required a

force-sizing strategy to fight a world war on a global scale(Troxell, 1997).

中共帶來的最重大軍事威脅是對臺灣的軍事入侵。在過去十年間，這種入侵的可能性大幅增加，許多美國軍事領導人表達對解放軍(PLA)即將入侵臺灣的擔憂。他們認為，如果歐洲和中東戰爭持續，並可能擴大為更廣泛的衝突，這將進一步助長美國對手的冒險主義行為，從而使入侵成為不可避免。2024 年 7 月 29 日《國防戰略委員會(NDS)》提交國會的最終報告中指出，美國尚未做好應對當前安全威脅的準備，並且 2022 年《國防戰略委員會》的部隊架構未能「充分考慮全球競爭或多戰場同時衝突的現實威脅」，這些威脅源於美國對手或潛在對手，在政治和軍事上的日益合作，對美國盟友與夥伴體系構成真實威脅。委員會建議採用一種「多戰區部隊建設」(Multiple Theater Force Construct)，這更能反映冷戰時期對抗蘇聯的戰略態勢，當時需要一種針對全球範圍內全面戰爭的部隊規模化戰略。

Xi Jinping and Vladimir Putin believe their nations are already actively engaged in conflicts with the United States(GEN Gary M. Brito, 2024). The Chinese Communist Party, the government of Communist China, declared a People's War against the U.S. in 2019(Bloomberg News, 2019), while the Russian Foreign Ministry claimed this year that the U.S. is already at war with Russia(Times of India, 2024). Kim Jon Un, General Secretary of the Workers' Party of North Korea and Chairman of the Central Military Commission of the Workers' Party of North Korea has ended all efforts at reconciliation with the democratic ROK, declared it to be his nation's "principal enemy," and stated that he "has no intention of avoiding war"(Lee Jeong-Ho, 2024) . Kim had previously declared that reunification with South Korea is no longer a policy goal nor is it possible to achieve(Dan Leaf, 2024). Kim also threatened to "thoroughly annihilate" the United States and South Korea if provoked(CBS News, 2024). In 2024, Kim has provided artillery rounds, ballistic missiles, and anti-tank rockets to Russia, and recently provided 1,500 of his special forces troops to Russia for training at local military bases, with a likely deployment to the western front to carry out combat operations against Ukraine(Nick Koutsobinas, Katherine Donlevy, 2024). The U.S. and Communist North Korea are still technically in a "state of war" following the armistice to stop fighting on July 27, 1953(United States Department of State, Bureau of Arms Control, 1953). Iran, which has no diplomatic relations with the U.S., has killed over 1,000 Americans via its

proxy wars, since the 1979 revolution(Richard Kemp, et al, 2015). More recently, the Office of the Director reported that “Iran has enabled scores of militia rocket, missile, and UAV attacks against U.S. forces in Iraq and Syria”(ODNI, 2024). Iran’s ‘Supreme Leader’ Ayatollah Ali Khamenei has explained that the ‘Death To America’ chants from its people and government are “not just a slogan, it is a policy”(Channel 1, Iran, 2023). Russian President Vladimir Putin and Iranian President Masoud Pezeshkian announced closer ties during a meeting on October 11, 2024, which Putin said will help to establish “new world order”(Deirdre Bardolf, 2023). Iranian relations with the PRC have already benefited Iran by undermining the efficacy of U.S. sanctions against it, helping Iran to become the dominant power in the Middle East(Reuel Marc Gerecht and Ray Takeyh, 2024). In the event of a conflict over Taiwan, Iran might decide to create additional problems for the U.S. to aid the Communist Chinese. GEN, Ret, Jack Keane commented that Russia, China, Iran and North Korea are all 'collaborating and cooperating together [to oppose] a mutual enemy – the United States and like-minded democracies”(Fox News, 2024).

習近平和普丁認為，他們的國家已經積極參與和美國的衝突。中共政府於2019年宣布對美國展開「人民戰爭」，而俄羅斯外交部則在今年聲稱，美國已經與俄羅斯處於戰爭狀態。北韓勞動黨總書記兼中央軍事委員會主席金正恩已終止與南韓的所有和解努力，並宣稱南韓是北韓的「主要敵人」，且表示他「無意避免戰爭」。金正恩此前曾聲明，與南韓的統一不再是政策目標，也無法實現。金正恩還威脅，如果遭到挑釁，他將「徹底消滅」美國和南韓。2024年，金正恩向俄羅斯提供砲彈、彈道飛彈和反戰車火箭，最近又派出1,500名特種部隊士兵到俄羅斯的軍事基地接受訓練，可能部署至西線，參與對烏克蘭的作戰行動。美國與北韓技術上仍處於「戰爭狀態」，儘管雙方在1953年7月27日簽署停戰協議停止戰鬥。自1979年革命以來，伊朗通過代理戰爭已經殺害超過1,000名美國人，而伊朗與美國並無外交關係。最近，美國情報部門報告指出：「伊朗已促成多起針對美國駐伊拉克和敘利亞部隊的火箭、飛彈以及無人機襲擊。」伊朗最高領袖哈米尼(Ayatollah Ali Khamenei)解釋道，其人民和政府的「打倒美國」口號「不僅僅是一個口號，而是一項政策」。俄羅斯總統普丁和伊朗總統裴澤斯基安(Masoud Pezeshkian)，在2024年10月11日的會議上宣布加強聯繫，普丁表示這將有助於建立「新的世界秩序」。伊朗與中共的關

係已幫助伊朗削弱美國制裁的效力，使其成為中東地區的主導力量。如果發生有關臺灣的衝突，伊朗可能決定為美國製造額外的問題，以支援中共。退役上將傑克·基恩(GEN, Ret, Jack Keane)評論道，俄羅斯、中共、伊朗和北韓都在「協同合作對抗共同的敵人—美國及志同道合的民主國家」。

Period Of Concern for The Indo-Pacific

Xi Jinping, General Secretary of the Chinese Communist Party (CCP) and Chairman of the Central Military Commission (CMC) is believed to have set a deadline of 2027 for the PLA to be ready to undertake the invasion(Michael Martina and David Brunnstrom, 2023). At a summit with President Biden in Woodside California on November 15, 2023, Xi warned the U.S. President during that Beijing will 'reunify' Taiwan with China(Kristen Welker, et al, 2023). Xi' has made the issue of annexing Taiwan a national priority stating in his New Year's address on December 31, 2023, that "'reunification' with Taiwan is inevitable"(Reuters, 2023). Since 1937, the CCP's policy has been to "liberate Taiwan," which was at that time under Japanese occupation (Xinhau, 2022). This phrase was still applied after the Nationalists retreated to Taiwan to maintain the internationally-recognized government of the Republic of China(Jade Guan, 2022; Simona A. Grano & Helena Y.W. Wu, 2021). The CCP previously announced in January 2019 that the PRC would not rule out the use of military force and would use "all necessary measures" to achieve this so-called 'liberation'(Xinhau, 2022). Finally, Xi made clear that he believes he has the necessary forces and capabilities to accomplish it when he stated "reunification cannot be stopped by any force, or anyone"(Matt Pottinger, 2024).

印太地區關注時期

中共總書記兼中央軍事委員會主席習近平，被多數專家學者認為已設定 2027 年為期限，要求解放軍做好發動入侵準備。2023 年 11 月 15 日在加利福尼亞州伍德賽德舉行的峰會上，習近平警告美國總統拜登，北京將實現臺灣與中國的「統一」。習近平將併吞臺灣的問題列為國家優先事項，並在 2023 年 12 月 31 日的新年致辭中表示，「與臺灣的統一是不可避免的」。自 1937 年以來，中共的政策一

直是「解放臺灣」，當時臺灣處於日本的佔領之下。在國民黨撤退到臺灣並維持國際公認的中華民國政府後，這一說法仍被中共使用。中共曾於 2019 年 1 月宣布不排除動用軍事力量，並將採取「一切必要措施」來實現所謂的「解放」。最後，習近平明確表示，他相信自己擁有完成統一所需的力量和能力，他曾說過：「統一無法被任何力量或任何人阻止。」

A review of the forecasts made by senior U.S. and ally/partner military leaders on the timing of a PLA invasion will provide us with a sense of how proximate this war is now. In 2021, U.S. Army General Paul E. Funk II, Commanding General of the U.S. Army's Training and Doctrine Command (TRADOC), assessed that Communist China and Russia would pose a significant challenge to the U.S. and her Allies in the 2025-2028 time frame(LTG Paul Funk, 2021). In the case of Russia, the threat to America's allies in Europe materialized two years early, as the Russo-Ukrainian War expanded dramatically on 24 February 2022, and is almost certain to continue well into 2025. Taiwan's Defense Minister Chiu Kuo-cheng assessed in 2021 that the PRC would be able to mount a full-scale invasion by 2025(The Guardian). Former Chairman of the U.S. Joint Chiefs of Staff (CJCS) GEN Mark Milley in his testimony to Senate Appropriations Committee stated that Communist China was working to ensure it had the capability to take Taiwan by military force by 2027(Sam Lagrone, 2021). Former Commander of U.S. Indo-Pacific Command (INDOPACOM), ADM, USN, Ret. Phil Davidson, stated in testimony to Congress in June 2021 that Communist China could try to take control of Taiwan in 'the next six years, which would run through 2027(Mallory Shelbourne, 2021), a position reinforced by ADM John Aquilino who succeeded ADM Davidson in command and who assessed that the PLA would be fully ready to invade by 2027(Michael Katz, 2024). On the question of whether or not Communist China would resort to a military option. RADM Michael Studeman, former Intelligence Director of INDOPACOM commented "It's only a matter of time, not a matter of 'if'" (Bill Gertz, 2021). Regarding the "when" question, GEN, Ret. Jack Keane opined that "…the clock may be moving closer to aggressive military action against Taiwan, as opposed to being later"(Fox News 2022), an opinion shared by Secretary of State, Antony Blinken, who said that Communist China wanted to take-over Taiwan on a "much faster timeline" than the U.S. leadership had expected(Noah

Robertson, 2024). Finally, U.S. Air Force Lt. Gen. Mike Minihan, former Director of Operations J3, Chief of Staff, and Deputy Commander of INDOPACOM, predicted that the U.S. may find itself at war with Communist China as early as 2025(Air and Space Forces Magazine, 2023). With these forecasts from very experienced senior U.S. military leaders, there is concern that the U.S. is running out of time to take the necessary actions and make the required investments to ensure that we can maintain an information advantage at the opening of a conflict with Communist China(Tom Rogan, 2024).

對美國及盟友(夥伴)高層軍事領導人，就解放軍入侵時機的預測進行回顧，將幫助我們瞭解這場戰爭的迫近程度。2021年美國陸軍教育與準則訓練司令部(TRADOC)司令保羅·E·芬克二世上將(Army General Paul E. Funk II)評估，中共與俄羅斯將在2025至2028年間，對美國及其盟友構成重大挑戰。就俄羅斯而言，其對美國歐洲盟友的威脅將提前兩年實現，因俄烏戰爭於2022年2月24日劇烈升級，且幾乎確定將持續至2025年。時任中華民國國防部長邱國正於2021年評估，中共將能在2025年前發動全面入侵。美國參謀長聯席會議前主席馬克·米利上將(ADM Mark Milley)在《參議院撥款委員會》作證時表示，中共正致力於確保在2027年前，具備以武力奪取臺灣的能力。美國印太司令部前指揮官菲爾·戴維森海軍上將(ADM Phil Davidson)於2021年6月在國會作證時表示，中共可能會在「未來六年內，也就是到2027年」試圖控制臺灣。這一觀點得到了接任戴維森上將的約翰·阿基利諾上將(ADM John Christopher Aquilino)的支持，他評估解放軍將在2027年前完全具備入侵的準備。關於中共是否會訴諸軍事選項的問題，印太司令部前情報總監邁克爾·斯圖德曼少將(RADM Michael Studeman)評論道：「這只是時間問題，而不是『是否』的問題。」至於「何時」的問題，退役上將傑克·基恩(GEN, Ret. Jack Keane)認為，「……針對臺灣的侵略性軍事行動可能比預期更早」，美國國務卿安東尼·布林肯(Antony John Blinken)也持相同看法，他指出中共希望在比美國高層預期「更快的時間表」內接管臺灣。最後，美國空軍中將、前印太司令部作戰部主任兼副指揮官邁克·米尼漢(Mike Minihan)預測，美國可能最早在2025年與中共開戰。根據這些經驗豐富的美國高層軍事領導人的預測，有理由擔憂美國已經沒有足夠的時間採取必要行動，並進行所需要的投資，以確保在與中共的衝突初期能夠維持資訊優勢。

PRC Preparations for, and Actions During The Crisis Phase

U.S. President Joe Biden has stated publicly to the press on four occasions that the U.S. has a commitment to come to the defense of Taiwan if Communist China were to attempt an invasion(NBC News, 2022). Accordingly, Communist China is preparing to achieve information advantage in the crisis phase, to introduce friction into U.S. decision-making with the aim of slowing down the U.S. commitment of military forces into the theater. U.S. Marine Corps' Information Operations Doctrine explains that the U.S. should expect adversaries to use their "technologies to destroy their enemy's ability to function, *or to make decisions*"(Marine Corps Doctrinal Publication 8). In the case of a war over Taiwan, the U.S. should also expect the CCP to use all possible methods to disrupt U.S. Strategic level decision-making on how to respond to Communist Chinese military aggression. Their goal would be to achieve information advantage, particularly *decision advantage*, over the next U.S. President taking office in the period of danger that starts in 2025. The most significant decision to be made, *War or no War*, is one that is mainly political in nature, as it is to be made by politicians in the political process. This fact creates opportunities for hostile influence operations aimed at the political process and its decision-making. The U.S. and her allies are in a period of peacetime competition, and the effort to generate friction in the U.S. command, control, communications and computer networks on-demand, and to introduce doubt into the U.S. decision-making process is already underway via Communist China's peacetime influence operations, cyber warfare, and network warfare, which would all shift to more aggressive forms in the crisis phase. The most immediate threat against the U.S. mainland population and her critical infrastructure is the information operations and cyber warfare threat posed by the PRC.

中共危機階段的準備與行動

美國總統拜登曾四次公開向媒體表示，若中共試圖入侵臺灣，美國承諾將對臺灣進行防衛。因此，中共正在準備在危機階段實現資訊優勢，以在美國決策過程中製造摩擦，目的是拖慢美國向戰區投入軍事力量的進程。根據美國海軍陸戰隊的《資訊作戰條令》，美國應預期對手將「利用技術摧毀其敵人的運行或決策能力」。

在臺灣戰爭的情況下，美國應預期中共會使用一切可能的方法，干擾美國在戰略層面上對中共軍事侵略的應對決策。他們的目標是實現資訊優勢，特別是決策優勢，以對2025年開始的危險期內上任的下一任美國總統施加影響。最重要的決策「是否開戰」，本質上主要是政治性的，因為這一決策將由政治過程中的政界人士做出決定。這一事實為針對政治過程及其決策的敵對影響行動創造機會。美國及其盟友正處於和平時期的競爭階段，而通過中共的和平時期影響行動、網路戰及資訊戰，對美國指揮、控制、通信及電腦網路製造摩擦，並向其決策過程中引入懷疑的努力，已經在進行中，這些行動將在危機階段轉變為更具侵略性的形式。對美國本土居民及其關鍵基礎設施的最直接威脅，是中共構成的資訊作戰及網路戰威脅。

Communist China's shift from peacetime influence operations in competition to the crisis phase would build on the currently successful implementation of elements of PRC's "Unrestricted Warfare" (UW), published by the PLA in February 1999 by PLA Colonels Qiao Liang and Wang Xiangsui(Qiao Liang and Wang Xiangsui, 1999). The ten elements of UW are: 1) Trade warfare; 2) Financial warfare; 3) Psychological warfare; 4) Smuggling warfare; 5) Drug Smuggling warfare; 6) Network warfare; 7) Resources warfare; 8) Economic Aid warfare; 9) International law warfare (a.k.a. "Lawfare"), and; 10) Cultural warfare(Qiao Liang and Wang Xiangsui, 1999). Most of these 'warfares' are already being carried out against the U.S. and her allies, with the aim of achieving favorable conditions for victory in the event of military conflict. Of note, the fifth, Drug Smuggling warfare, is having lethal results on the American citizenry, with over 200 Americans dying daily, and more than 75,000 Americans dying each year from overdoses of fentanyl manufactured in and shipped from Communist China(The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, 2024). Communist China's Network Warfare and Lawfare against the U.S. and her Allies and partners are well known, and are making media headlines continually(FORUM Staff, 2024; Jordan Foley, 2024).

中共從和平時期的影響行動轉變為危機階段，將基於其目前成功實施的部分「超限戰」(UW)策略，該策略由解放軍喬良和王湘穗上校於1999年2月發表。超限戰的十個元素包括：1、貿易戰；2、金融戰；3、心理戰；4、走私戰；5、毒品走私戰；6、網路戰；7、資源戰；8、經濟援助戰；9、國際法律戰(又稱「法律戰」)；以及

10、文化戰。這些「戰爭」中的大部分已針對美國及其盟友展開，目的是在可能的軍事衝突中創造有利的勝利條件。值得注意的是，第五項「毒品走私戰」正在對美國公民造成致命影響，每天有超過200名美國人，因服用過量的由中共製造並運輸的芬太尼(毒品，一種止痛藥)而死亡，每年死亡人數超過75,000人。中共針對美國及其盟友和夥伴的網路戰和法律戰廣為人知，並不斷登上媒體頭條。

While Unrestricted Warfare is not claimed as an official doctrine by the PLA, three of these warfare approaches were adopted in the PLA's "Three Warfares Strategy," namely Psychological warfare, Legal warfare, and the War of Public Opinion which is connected with cultural infiltration and media propaganda. The overall objective of the Three Warfares Strategy is "to control the narrative and influence perceptions in ways that advance China's objectives while thwarting its competitors' ability to respond"(Marine Corps Doctrinal Publication 8, 2022). PLA Unrestricted Warfare provides a theory of warfare and methods that span peacetime competition into high-end kinetic warfighting. Unrestricted Warfare also provides an additional venue for achieving decision advantage by creating multiple dilemmas affecting forward deployed and deploying forces, as well as the domestic populations of the U.S. and her allies and partners. Unrestricted Warfare creates the possibility of warfare with critical infrastructure attacks that cause few casualties, and can be seen on the whole as a non-lethal pre-emptive action that accompanies the application of military power against one of America's allies and partners. The purpose of all of these UW attacks would be to disrupt the speed of U.S. responses(Ross Baggage, 2023). The Network warfare component of UW, is the peacetime application of the PLA warfighting doctrine of "System Destruction Warfare," which describes the PLA's abilities and concepts of operations to conduct "systems destruction attacks" to take down information systems, and networks(Jeffrey Engstrom, 2018). Chinese military writings suggest that the PLA seeks "to reconnoiter a potential adversary's computer systems in peacetime, influence opponent decision-makers by threatening those same systems in times of crisis, and disrupt or destroy information networks and systems by cyber and electronic warfare (EW) means in the event of conflict"(Heritage Foundation, 2024).

雖然「超限戰」並未被解放軍正式承認為其官方教條，但其中三種作戰方式已

被納入解放軍的「三戰策略」，即心理戰、法律戰和輿論戰，這些作戰方式與文化滲透及媒體宣傳密切相關。三戰策略的總體目標是「通過控制敘事和影響認知，推進中國的目標，同時削弱競爭對手的應對能力」。解放軍的「超限戰」提供一套從和平時期競爭，到高端實體戰鬥的戰爭理論與方法。超限戰還通過製造多重困境，影響美國及其盟友和夥伴的前線部署部隊和國內民眾，為實現決策優勢提供額外的手段。超限戰可能涉及對關鍵基礎設施的攻擊，這些攻擊雖然傷亡較少，但整體上可被視為配合對美國盟友或夥伴，使用軍事力量的非致命性先發制人行動。所有這些超限戰攻擊的目標是破壞美國的反應速度。超限戰中的網路戰部分，是解放軍「體系破壞戰」作戰理論在和平時期的應用，該理論描述解放軍摧毀資訊系統和網路的能力及作戰概念。中共軍事著作指出，解放軍的目標是在和平時期對潛在對手的電腦系統進行偵察，在危機時期通過威脅同樣的系統來影響對手決策者，並在衝突中通過網路戰和電子戰手段，干擾或摧毀資訊網絡和系統。

Dr. Ross Babbage, an expert on Chinese and Russian political warfare campaigns, explains that in a conflict with the PRC, the U.S. should expect a major disruption of military and government command and control (C2) networks, public communications networks, financial and banking networks, local and state government networks, power and water distribution networks, wastewater treatment plants, and the list goes on(Ross Babbage, 2023). The PLA understands the connectivity of military forces networks to "local and national governments, infrastructure, and institutions" and "[t]hose networks are therefore essential targets for the PLA and the broader Chinese network warfare community" (Dean Cheng, 2022). The PRC has built peer- or near-peer-level capabilities in space and cyberspace, which it would likely use to try to deter and prevent the United States from engaging in a conflict by disrupting U.S. critical infrastructure, including computer networks, satellites, and other enabling functions(Harman, et al, 2024). The TRADOC G2 reports that "China, Russia, and other adversaries are investing heavily in hybrid and irregular capabilities, such as information and cyber operations, to attack soft targets and systems within the territory of the United States and its allies"(GEN Gary M. Brito, 2024). Increasingly, the PLA considers cyber capabilities a critical component in its overall integrated strategic deterrence posture, alongside space and nuclear deterrence. PLA studies discuss using warning or demonstration strikes—strikes against select

military, political, and economic targets with clear “awing effects”—as part of deterrence(Office of the Secretary of Defense, 2023).

中國與俄羅斯政治戰爭專家羅斯·巴貝奇博士(Dr. Ross Babbage)指出，在與中共的衝突中，美國應預期其軍事與政府指揮與控制(C2)網絡、公共通信網絡、金融與銀行網絡、地方與州政府網絡、電力與水資源分配網絡，以及廢水處理廠等將遭遇重大干擾，且影響不止於此。解放軍瞭解軍事力量網絡與「地方及國家政府、基礎設施與機構」的連接性，因此這些網絡成為解放軍及更廣泛的中共網路戰社群的重要攻擊目標。中共已在太空與網路空間構建出對等或接近對等的能力，可能利用這些能力干擾美國的關鍵基礎設施，包括電腦網路、衛星及其他支援功能，從而試圖威懾並阻止美國介入衝突。根據美國陸軍教育與準則司令部(TRADOC)G2的報告，「中共、俄羅斯及其他對手正大量投資於混合與非正規能力，如資訊與網路作戰，以攻擊美國及其盟友領土內的軟目標及系統。」解放軍越來越將網路能力視為其整體綜合戰略威懾態勢中的關鍵組成部分，與太空與核威懾並列。解放軍的研究討論使用警告性或示範性打擊—針對特定的軍事、政治及經濟目標進行打擊，並產生明確的「震懾效果」，做為威懾的一部分。

America’s many adversaries are also seeking information advantage by conducting influence operations during competition to condition target audiences to be more responsive to their policies. A purpose of such efforts is to achieve disunity in the U.S. population that could be exploited in the opening stages of a war. The U.S. and her allies and partners are the targets of influence campaigns designed to divide the domestic populace to make it difficult to rally the nation in a crisis. The technique of exploiting fissures among adversary populations has been demonstrated over many election cycles in the United States, Taiwan, and other nations(Global News, 2024; Courtney Kube and Carol E. Lee, 2024; Nicole Wells, 2024; Newsmax, 2024), and could also be employed to generate disunity in the decision to employ military forces. These efforts are the 'softening up' of the resolve, amity, and resilience of the adversary population, with the aim of making nigh impossible for the U.S. population to unite rapidly, as it did at the outset of both World Wars and the Global War on Terror. Xi Jinping, the General Secretary of the Chinese Communist Party (CCP) and Chairman of the Central Military Commission (CMC), considers America's weakness to be the fragility of consensus of the

U.S. domestic population at the opening of a conflict(Ross Babbage, 2023). The Office of the Director of National Intelligence assesses that Communist China increasingly seeks to “exploit perceived U.S. societal divisions” as part of its peacetime competition influence shaping operations(Office of the Director of National Intelligence, 2023). As our adversaries' main goals are to keep the U.S. out of regional conflicts to maintain freedom of action and maneuver, they will invest heavily in inform and influence actions during peacetime competition to drive public opinion to a state favorable to the adversary at the opening of conflict.

美國眾多對手也通過競爭期間進行影響行動，尋求資訊優勢，以使目標受眾對其政策更加順從。這類行動的目的是在美國國內製造分裂，並在戰爭初期加以利用。美國及其盟友和夥伴是影響行動的目標，這些行動旨在分化國內民眾，使其在危機中難以團結起來。利用敵方之間的罅隙，而這些方式已在美國、臺灣及其他國家的多次選舉中得到展示，並可能被用於在動用軍事力量的決策上製造分歧。這些努力旨在削弱敵方人口的決心、友好關係和韌性，其目的是讓美國民眾幾乎不可能像在兩次世界大戰和全球反恐戰爭初期那樣迅速團結起來。中共總書記兼中央軍事委員會主席習近平認為，美國的弱點在於其國內人口，在衝突初期缺乏共識的脆弱性。美國國家情報總監辦公室評估指出，中共越來越傾向於利用「美國社會分裂的表象」，將其做為和平時期競爭中影響塑造行動的一部分。由於敵方的主要目標是讓美國遠離地區衝突以保持行動與機動的自由，他們將在和平時期的競爭中投入大量資源於資訊與影響行動，以在衝突初期將輿論引導至對敵方有利的狀態。

In the competition phase, Three Warfares coupled with Chinese Communist Party United Front Work operating in the U.S. and in the homelands of her allies and partners would be busy fomenting dissension and opposition against government policies supporting the Taiwan military and the defense of Taiwan. The PLA understands that success in the cognitive domain in crisis relies on advantages created during peacetime competition in the homelands of adversaries, and the minds of their populations(Edmund Burk, et al. 2020). To consider how that might manifest itself, one need only look at recent demonstrations and riots carried out by college students in U.S. cities and college campuses that quite simply reinforce Hamas and Hezbollah propaganda, and which are enabled by financial support and encouragement from both the government of Iran, and

their aligned U.S.-based organizations(Shia Kapos, 2024; David Klepper, 2024). These protests and riots are being compared to the protests against U.S. policy on the war against communism in Vietnam, as both are credited with having some influence over U.S. domestic opinion on the issue of military support to a U.S. ally, with the aim of pressuring U.S. political leaders to stop providing such support(Andrea Shalal and Bianca Flowers, 2024). Israel was designated as a major non-NATO ally by the U.S. under President Ronald Reagan during the Cold War in 1987. This status did not appear to afford it any protection in the current U.S. domestic political environment. Taiwan is in this same alliance category, as the U.S. Congress required that Taiwan be treated as though it were designated a major non-NATO ally when it enacted the Foreign Relations Authorization Act for FY 2003 on September 30, 2002(Public Law 107–228, 2002). The U.S. should expect similar efforts from the United Front Work apparatus in the U.S. during the crisis phase to generate domestic political opposition to standing by our declared allies and partners as part of their efforts to achieve information superiority, an important doctrinal concept for the PLA.

在競爭階段，三戰策略結合中國共產黨在美國及其盟友和夥伴本土的統一戰線工作，將積極挑起針對支持臺灣軍事及防衛政策的分裂和反對行動。解放軍明白，在危機中的認知領域取得成功，依賴於和平時期競爭期間在敵方本土和其人民心理中創造的優勢。要考慮這種情況可能如何展現，只需觀察近期美國城市及大學校園內由大學生發起的示威和騷亂，這些活動直接強化哈馬斯和真主黨的宣傳，並受到伊朗政府及其美國本土相關組織的財政支持與鼓勵。這些抗議和騷亂被比作針對美國反共戰爭政策的越戰抗議活動，因為兩者都被認為對美國國內關於對盟友軍事支持問題的輿論產生一定影響，其目的是向美國政治領導人施壓，要求其停止提供這種支持。以色列於1987年冷戰期間被美國總統羅納德·雷根(Ronald Wilson Reagan)指定為主要非北約盟友，但這一地位在當前美國國內政治環境中，似乎未能為其提供任何保護。臺灣屬於同一類別，因為美國國會於2002年9月30日通過2003財年《外交關係授權法案》時，要求將臺灣視為主要非北約盟友對待。美國應預期在危機階段，共產黨統一戰線工作部將發起類似行動，旨在引發國內政治反對，反對支持我們已宣示的盟友與夥伴，這是解放軍實現資訊優勢的一項重要理論概念。

In both competition and crisis, it should be expected that Communist China would benefit from its increasing cooperation with Russia, North Korea and Iran. The various bilateral military security and cooperation agreements made among these countries create a system of overlapping alliances, and are eerily similar to the pacts signed among the nations of the Triple Entente and Central Powers, leading up to the First World War, and perhaps also the Molotov-Ribbentrop Pact between Germany and Soviet Russia, which included secret protocols for the division of Poland. The 1961 treaty between the communist nations of China and North Korea, which stipulates that China is obliged to intervene against unprovoked aggression, was renewed on the 60th anniversary of its signing on July 2021 for another twenty years(Khang Vu, 2021). Communist China signed a 25-year "strategic agreement" with Iran in 2021(The Economist, 2023). Russia and Iran announced a new type of bilateral military relationship on January 24, 2024, which was preceded by several arms shipments from Iran to Russia to support its war in Ukraine(Emil Avdaliani, 2024). Communist China and Russia established a "no limits" partnership in February 2022, and re-committed to that partnership May 16, 2024, marking the 75th year anniversary of formal China-Russia diplomatic relations(Anushka Saxena, 2024), Russia and North Korea signed a mutual defense commitment on June 19, 2024, that provides mutual security guarantees and military-technical cooperation(Kelsey Davenport, 2024).

在競爭和危機中，可預期中共將從與俄羅斯、北韓和伊朗日益增強的合作中受益。這些國家之間簽署的各種雙邊軍事安全與合作協議，構建一個重疊的同盟體系，與第一次世界大戰前三國協約和同盟國簽署的協定，以及德國與蘇聯之間簽署的《莫洛托夫-里賓特洛甫條約》(互不侵犯條約)驚人相似，後者包括秘密協議以瓜分波蘭。1961年中共與北韓共產主義國家之間的條約規定，中共有義務對未經挑釁的侵略行動進行干預，該條約於2021年7月簽署60周年時續簽，延長了20年。中共於2021年與伊朗簽署一份為期25年的「戰略協議」。俄羅斯與伊朗於2024年1月24日宣布建立一種新的雙邊軍事關係，這之前伊朗曾多次向俄羅斯運送武器，以支持其在烏克蘭的戰爭。中共與俄羅斯於2022年2月建立「無上限」夥伴關係，並於2024年5月16日重申這一夥伴關係，以紀念中俄正式建交75周年。俄羅斯與北韓於2024年6月19日簽署一項互助防衛承諾，提供相互安全保證及軍事技術合作。

These agreements appear to support the coordination of peacetime competition influence operations, as the overlapping relationships are reflected in bilateral agreements on economic cooperation and assistance, the provision of combat systems and technology, facilitating the evasion of international sanctions, as well as mutually reinforcing foreign policy and strategic messaging in opposition to the U.S. and the West(Bruce W. Bennett, 2023; Andrea Kendall-Taylor and Richard Fontaine, 2024; Tom O'Connor, 2021; The Center for National Interest, 2024; Bruce Klinger, 2024). Iran, the newest member of this group, is presently conducting a cyber-enabled influence campaign targeting the U.S. regarding U.S. policy on its proxy war against Israel carried out by the Hamas and Hezbollah terrorist organizations(Daniella Jiménez, 2024). The Iranians are actively conducting these influence operations to shape U.S. public opinion in their favor. In the event of a military crisis over Taiwan, Iran could decide to help its like-minded autocratic partner, Communist China, to reinforce PLA influence operations against the U.S.

這些協議似乎支持和平時期競爭中的影響行動協調，因為雙邊協議中體現了重疊的關係，包括經濟合作和援助、提供作戰系統與技術、協助規避國際制裁，以及共同加強反對美國和西方的外交政策和戰略傳訊。伊朗做為該組織中最新的成員，目前正在針對美國展開網絡驅動的影響行動，目標是美國針對哈馬斯和真主黨恐怖組織代理戰爭的政策。伊朗積極實施這些影響行動，目的是將美國輿論導向對其有利的方向。若臺灣爆發軍事危機，伊朗可能決定幫助其志同道合的威權夥伴中共，以加強解放軍對美國的影響行動。

Information Advantage in the Crisis Phase through Resilient Networks and Systems

In the crisis phase, the worst case scenario would be if the military cooperation outlined in the preceding paragraph resulted in a combined cyber and non-kinetic attacks against the U.S. and her allies. In his 2021 article published by War on the Rocks, Chris Dougherty explains that information systems have become the single biggest vulnerability in any conflict with Communist China or Russia, as both adversaries have been developing strategies and capabilities to quickly achieve their operational objectives by attacking U.S. Information systems(Chris Dougherty, 2021). The Chinese Communist

PLA believes that the dominant mode of warfare is "the confrontation between information-based systems-of-systems"(Edmund Burke, et al, 2020). This is carried out through network warfare, degrading/destroying the adversary's networks to achieve "network warfare superiority" (Edmund Burke, et al, 2020). John Costello and Joe McReynolds of the U.S. National Defense University explain that the PLA's Strategic Support Force (SSF) will employ both "psychological warfare and electronic warfare in the pre-crisis period to raise the political and military risks associated with aggression"(John Costello and Joe McReynolds, 2019). In any case, the U.S. should expect such attacks from the PRC, reflecting the PLA's "system destruction warfare" with a focus on destroying, degrading, disabling, or paralyzing our many networks, both military and civilian, that enable the country to function. Increasingly, the PLA considers cyber capabilities a critical component in its overall integrated strategic deterrence posture, alongside space and nuclear deterrence. In a decision-superiority attack under the system destruction warfare approach, the U.S. should also expect the prompt employment of two of the UW methods, namely financial warfare combined with network warfare, which could achieve crippling effects against U.S. financial, networks to include everyday use of banking and credit services. The goal from such attacks would be to create panic and anxiety in the U.S. civilian population resulting from loss of access to funds. Restoring banking and credit services following attacks will be a significant challenge, according Lea Cure, Cyber Threat Intelligence Manager for Citizens Bank, who summed up the magnitude of the challenge thusly: "The technologies we use and the technologies we use to move money are critical. If those go down, what will we do?"(Sam Langrock, 2024) Compounding this would be the simultaneous attacks on communications, distribution systems networks (including power, water, sewage, oil, gas, electricity) that would create multiple dilemmas for the U.S. as it responds to the military threat. Considering how its adversaries are employing network warfare during peacetime competition, the U.S. can expect that they have planned how to transition to crisis, and leverage their penetration into U.S. networks to go on the offense to achieve the highest possible levels of disruption effects against the networks needed for society to function, and potentially create multiple and metastasizing

challenges that will compete for resources and attention. The U.S. Army assesses that the PLA will conduct "cognitive domain operations to gain dominance in the information and human dimensions to have outsized impact on both public opinion and military morale."(GEN Gary M. Brito, 2024)

透過強韌的網路與系統實現危機階段的資訊優勢

在危機階段，最壞的情況是前段提到的軍事合作，導致美國及其盟友遭受聯合網路攻擊和非物理攻擊。克里斯·道格蒂(Chris Dougherty)在2021年發表於《戰爭之石(War on the Rocks)》的一篇文章中指出，資訊系統已成為與中共或俄羅斯衝突中的最大單一漏洞，因為這兩個對手一直在開發策略和能力，以通過攻擊美國資訊系統迅速實現其作戰目標。中共解放軍認為，戰爭的主要模式是「基於資訊的系統與系統的對抗」。這是通過網路戰來實現的，通過削弱或摧毀敵方網路以實現「網路戰優勢」。美國國防大學的約翰·科斯特洛和喬(John Costello)·麥克雷諾茲(Joe McReynolds)解釋說，解放軍的戰略支援部隊(SSF，該部隊已於2024年4月19日解散，分別組建為解放軍信息支援部隊、軍事航天部隊及網絡空間部隊)，將在危機前階段使用「心理戰和電子戰」，以提高與侵略行為相關的政治和軍事風險。無論如何，美國應預期來自中共的此類攻擊，反映了解放軍的「體系破壞戰」，重點是摧毀、削弱、癱瘓或破壞包括軍用和民用在內的多種網絡，這些網絡支撐國家的運行。解放軍越來越將網路能力視為其整體綜合戰略威懾態勢中的關鍵組成部分，與太空和核威懾並列。在體系破壞戰中的決策優勢攻擊中，美國應預期解放軍迅速採用兩種「超限戰」方法，即「金融戰」和「網路戰」相結合，這可能對包括日常銀行和信貸服務在內的美國金融網絡產生癱瘓性影響。這類攻擊目標是由於無法獲得資金而在美國平民中引發恐慌和焦慮。在攻擊後恢復銀行和信貸服務將是一個重大挑戰。此外，同時對通信和分配系統網絡(包括電力、水、污水、石油、天然氣和電力)的攻擊，將使美國在應對軍事威脅時面臨多重困境。美國可以預期，敵方已計畫如何過渡到危機階段，並利用其對美國網路發動滲透及攻勢，以對社會運行所需的網路實現最大程度的破壞效果。美國陸軍評估指出，解放軍將進行「認知領域作戰(認知戰)」，以在資訊和人類層面上獲得主導地位，從而對公共輿論和軍事士氣產生超乎尋常的影響。

Communist China, Russia, Iran, and North Korea have all steadily established

footholds inside our domestic critical networks so as to be in a position to conduct attacks in the crisis phase. The U.S. Army points out that these include “hardened government systems, private industry, and social media to … disrupt our critical functions, and delay our ability to project force.” (GEN Gary M. Brito, 2024) In his remarks at the TechNet Cyber Conference in June 2024, General Timothy Haugh, Commander of U.S. Cyber Command and Director of the National Security Agency, explained that Communist China’s current efforts to “gain critical infrastructure footholds and disrupt supply chains pose significant risks to the Department of Defense’s (DoD’s) ability to defend the nation.”(Carley Welch, 2024) Speaking at the same event, Lt Gen Robert Skinner, Director of the U.S. Defense Information Systems Agency reinforced those remarks saying that Communist China is “…focused on disrupting our critical infrastructure [and] targeting our critical infrastructure.” (Carley Welch, 2024)

中共、俄羅斯、伊朗和北韓已在美國的國內關鍵網絡中穩步建立據點，以便在危機階段發動攻擊。美國陸軍指出，這些據點包括「強化的政府系統、私人產業和社交媒體……以破壞我們的關鍵能力，並延遲我們部署軍事力量的能力。」在2024年6月的TechNet網路大會上，美國網路司令部指揮官兼國家安全局局長提摩西·霍夫(General Timothy Haugh)將軍表示，中共目前試圖「在關鍵基礎設施中建立據點，並破壞供應鏈，這對國防部的國防能力構成重大風險。」在同一活動中，美國國防資訊系統局局長羅伯特·斯金納中將(Lt Gen Robert Skinner)進一步強調，中共「……專注於破壞我們的關鍵基礎設施，並且針對我們的關鍵基礎設施發動攻擊。」

What is the level of penetration of U.S. infrastructure networks that we are facing?

The Hon. Christopher Wray, Director of the Federal Bureau of Investigation (FBI), reported to Congress in January 2024 that Communist China "… made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try to induce panic and break America’s will to resist."(FBI News, 2024) Mr. Wray also later reported to Congress in April 2024 that the Communist Chinese government had gained illicit access to networks within America’s “critical telecommunications, energy, water, and other infrastructure sectors.”(Didi Tang, and Eric Tucker, 2024) The Chinese

Communist Party's domestic laws impose information sharing requirements on PRC-based companies to share information on their contracts abroad with Ministry of State Security, and so as PRC companies continue to capture much of the worldwide market for setting up and maintaining 5G networks, the PRC "will challenge the security and resiliency of other countries' networks."(Yasmin Tadjdeh, 2021)

我們面臨的美國基礎設施被網路滲透程度？

美國聯邦調查局(FBI)局長克里斯托弗·雷(Christopher Wray)於2024年1月向國會報告指出，中共「…明確表示，任何支撐美國社會運行的部門都是其在世界舞台上追求主導地位的目標，並計畫通過打擊民用基礎設施來引發恐慌，破壞美國的抗拒意志。」克里斯托弗·雷於2024年4月再次向國會報告，中共政府已非法侵入美國「關鍵的電信、能源、水資源及其他基礎設施部門的網絡」。中共的國內法律要求中國企業向國家安全部共享其海外合同的資訊。因此，隨著中國企業繼續佔領大量全球5G網路建設和維護市場，中共「將挑戰其他國家網絡的安全性和韌性」。

In her testimony before Congress in January 2024, Ms. Jen Easterly, the Director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, listed the targets of such an attack as including disruption of energy pipelines (natural gas, petroleum), telecommunications, water systems, transportation nodes, "…all to ensure that they can incite societal panic and chaos" and in so doing deny or disrupt the ability for the U.S. government to mount an organized and adequate response(Didi Tang, and Eric Tucker, 2024). The chaos and panic will be felt at the local city level, "especially those cities and municipalities that share infrastructure with nearby Army bases."(LTG Susan S. Lawrence, 2024) Writing on the threat of network attacks, George Seffers observed that "current frameworks are inadequate to meet the growing threat to urban communities."(George I. Seffers, 2024) Recalling recent events, we have seen many examples of such disruption attacks, in the U.S. and across the globe. Looking at cyber attacks as one example, the "Volt Typhoon" hacks carried out by Communist China that targeted U.S. critical infrastructure, disrupting communications, education, utilities and government sectors in Guam and elsewhere. "Attacks [like the Volt Typhoon incidents] on critical infrastructure – food and water delivery, health care

services, defense contracting, and more – could jeopardize U.S. military response across the world as well as a sense of stateside calm."(Colin Demarest, 2024) Another recent example is the unintentional shutdown of computer networks across the globe known as the "Crowdstrike incident" on July 19, 2024. The effects of that botched software update provide a great example of the chaos and panic that results from the shut-down of computer networks across government and industry systems. Disruption of computer access impacted airlines and airports, banks, hotels, hospitals, manufacturing, stock markets, broadcasting, gas stations, retail stores, and governmental services, such as emergency services. Microsoft estimated that Microsoft reported that an estimated 8.5 million Windows devices had been impacted by the outage(CIO staff, 2024). The incident was labelled largest outage in the history of information technology(Dan Milmo, et al, 2024).

美國國土安全部網絡安全和基礎設施安全局局長珍·伊斯特利(Jen Easterly)，在2024年1月向國會作證時列舉此類攻擊的目標，包括破壞能源管道(天然氣、石油)、電信、水資源系統和交通樞紐，「…所有這些都是為了確保他們能引發社會恐慌和混亂」，從而否定或破壞美國政府組織有效應對的能力。這種混亂和恐慌將在地方城市層面顯現，「特別是那些與附近陸軍基地共享基礎設施的城市和市鎮」。關於網路攻擊的威脅，喬治·塞弗斯(George Seffers)指出，「當前框架不足以應對日益增長的對城市社區的威脅。」回顧近期事件，我們看到許多此類破壞性攻擊的例子，既有發生在美國本土，也有遍及全球。例如，中共實施的「伏特颱風(Volt Typhoon)」網路攻擊(駭客組織)，針對美國關鍵基礎設施，破壞關島及其他地區的通信、教育、公用事業和政府部門。「針對關鍵基礎設施的攻擊，例如：食品和水的配送、醫療服務、國防承包等，可能危及美國在全球的軍事反應能力，也可能破壞國內的平靜氛圍。」另一個近期的例子是2024年7月19日被稱為「大規模藍白事件(Crowdstrike)」的全球電腦網路意外停運。這次失敗的軟件更新造成的影響是一個典型案例，展示了政府和產業系統的電腦網路停止運作，所引發的混亂和恐慌。電腦網路的中斷影響航空公司和機場、銀行、酒店、醫院、製造業、股票市場、廣播、加油站、零售商店以及政府服務(如緊急服務)。微軟報告估計約850萬台Windows設備受到此次停運的影響，此次事件被稱為資訊技術歷史上最大的停運事故。

Cyber Ransom Attacks at a National Scale?

It is conceivable that Communist China could essentially conduct a national level "ransom-ware" attack against the U.S. in the crisis phase leading up to a major theater war. This would be accomplished by employing non-kinetic means to so disrupt our networks that the basic government and commercial functions fail, while also holding out the possibility of the CCP limiting the duration, or even reversing those effects if the U.S. acquiesces to Communist Chinese demands(Ariel E. Levite and June Lee; U.S. Army War College, 2023). The ransom that would be demanded by Communist China in this scenario would be for the U.S. to abandon Taiwan and not come to its defense. The Chinese Communists could largely refrain from using kinetic lethal operations that would inflict casualties in this phase, so that the U.S. would not experience deaths of its service members and civilians that would demand war in self-defense. The PRC would thereby avoid repeating the historical precedents where kinetic actions resulted in the U.S. declaring war on the attacker, including the sinking of the USS Maine in the Havana Harbor on February 15, 1898 (resulting in the U.S. Congress declaring War on the Empire of Spain)(See William C. Kashatus, 2018), the Imperial Japanese Navy attack on Pearl Harbor on December 7, 1941 (resulting in the U.S. Congress declaring War on the Empire of Japan), and the Islamic Terrorist attack on the World Trade Center on September 11, 2001 (launching the Global War on Terror as declared by President George W. Bush). Recent ransomware attacks in the U.S. against infrastructure have been carried out for financial ransoms, but they point out our vulnerabilities to the networks the PLA are likely to attack. The U.S. FBI reported an increase in such attacks against public infrastructure networks for the year 2023. More than 20% of the ransomware attacks in 2023 were against organizations in a critical infrastructure sector (1,193 out of 2,825 ransomware attacks)(Matt Kapko, 2024). The effected critical infra-structure sectors attacked included (in order of most attacks to least): 1) Public Health/Healthcare, 2) Critical Manufacturing, 3) Government Facilities, 4) Information Technology, 5) Financial Services, 6) Commercial Facilities, 7) Food and Agriculture, 8) Transportation, 9) Communications, 10) Energy, and; 11) Chemical production. (Matt Kapko, 2024; Statista, 2024)

全國範圍的網絡勒索攻擊？

不難想像在通往一場主要戰區戰爭的危機階段，中共可能會對美國發動全國性規模的「勒索軟件」攻擊。這將通過採用非物理手段干擾美國的網路實現，導致基礎政府和商業功能癱瘓，同時暗示如果美國接受中共的要求，他們可以限制這些影響的持續時間，甚至逆轉這些影響。在此情境中，中共提出的勒索條件將是美國放棄臺灣，並停止對其防衛的支持。中共可能在這一階段避免使用會造成傷亡的物理性致命行動，從而使美國無法因其軍人和平民的死亡而要求進行自衛戰爭。中共將因此避免重蹈過去歷史的覆轍，其中動態行動導致美國向襲擊者宣戰，包括1898年2月15日「緬因號」戰艦在哈瓦那港被擊沉(美國國會向西班牙帝國宣戰)、1941年12月7日日本帝國海軍對珍珠港的襲擊(美國國會向日本帝國宣戰)，以及2001年9月11日對世界貿易中心的伊斯蘭恐怖襲擊(喬治·布希總統宣布的全球反恐戰爭)。近期美國針對基礎設施的勒索軟件攻擊主要是為了金錢贖金，但這暴露了我們的網路漏洞，這些漏洞可能成為解放軍攻擊的目標。美國聯邦調查局(FBI)報告稱，2023年針對公共基礎設施網絡的此類攻擊有所增加。2023年超過20%的勒索軟件攻擊，針對關鍵基礎設施部門的組織(在2,825起勒索軟件攻擊中有1,193起)，受影響的關鍵基礎設施部門包括(按攻擊數量從多到少排列)：1、公共健康/醫療；2、關鍵製造業；3、政府設施；4、資訊技術；5、金融服務；6、商業設施；7、食品與農業；8、交通運輸；9、通信；10、能源；11、化工生產。

These networks, essential to daily living, are likely to be targeted in the crisis phase, as they are already being targeted now by state and non-state actors. Recent reports published by the U.S. government demonstrate that the threats to U.S. critical infrastructure described above are worsening. Security Magazine reported in January of 2024 that the U.S. had suffered 420 million cyber attacks carried out by 168 threat actors in 2023, at a rate of 13 attacks per-second, and representing an increase of 30% over the previous year. (Security Staff, 2024) Regarding healthcare and hospitals, the July 2024 indictment of a member of the Communist North Korean Military's Reconnaissance General Bureau by the U.S. FBI for ransomware cyberattacks against U.S. hospitals and healthcare providers carried out in 2022 demonstrated the threat posed by our adversaries(Associated Press, 2024). Such attacks disrupt the treatment of patients, especially if patient records are altered or locked by ransomware. In this case, the North

Korean hackers used their ill-gotten ransom money to fund theft of sensitive information from defense and government agencies and technology organizations worldwide(Public Affairs, 2024).

這些對日常生活至關重要的網路，可能在危機階段成為目標，因為目前它們已經受到國家和非國家行為者的攻擊。美國政府最近發布的報告顯示，上述針對美國關鍵基礎設施的威脅正在惡化。《安全雜誌(Security Magazine)》於2024年1月報導稱，2023年美國遭受由168個威脅行為者發動的4.2億次網路攻擊，平均每秒發生13次攻擊，比前一年增加30%。關於醫療保健和醫院，2024年7月美國聯邦調查局(FBI)起訴一名北韓軍事偵察總局成員，指控其於2022年對美國醫院和醫療保健提供者，進行勒索軟件網路攻擊，這進一步顯示敵對勢力帶來的威脅。此類攻擊干擾病人的治療，尤其是在病歷被勒索軟件更改或鎖定的情況下。在此案例中，北韓駭客利用非法獲得的贖金，資助從全球防務和政府機構以及技術組織中盜取敏感資訊的活動。

Tele-Communications Networks

In the case of a major conflict with either our pacing challenger the PRC, or the acute challenger Russia, the U.S. should expect attacks against our international communications networks to include attacks on space-based communications and undersea cables. The ODNI reported in 2024, that "[c]ounterspace operations will be integral to potential PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites," while Russia will work to improve its already significant counterspace capabilities while it rebuilds its ground forces(Office of the Director of National Intelligence, 2024; Jane Harman, et al, 2024). Both China and Russia could hold U.S. space assets at risk, upon which are necessary both the daily lives of the citizenry, and which are essential for military capabilities(Office of the Director of National Intelligence, 2024; Jane Harman, et al, 2024). John F. Plumb, in his testimony to House Armed Services Strategic Forces subcommittee hearing on national security space activities on April 6, 2023, reported that "China has already fielded ground-based counterspace weapons and it continues to seek new methods to hold U.S. satellites at risk."(David Vergun, 2023) A recent example of

counterspace attacks is the Russian use of cyber-attacks at the resumption of fighting against Ukraine in January 2022, ahead of and during the invasion. In this case, the attacks were carried out against commercial satellite communications networks to achieve information advantage by disrupting Ukrainian command and control during the transition from crisis into conflict(Antony J. Blinken, 2022). These attacks, launched one hour before the invasion into Ukraine, disabled very small aperture terminals (VSAT) in Ukraine and across Europe, disrupting internet and energy networks impacting the daily lives of citizens(Foreign, Commonwealth & Development Office and The Rt Hon Elizabeth Truss, 2022). The Russian attack on space capabilities reinforced Air Force Secretary Frank Kendall's arguments for a more resilient U.S. space-based infrastructure and networks that would able to withstand such attacks(Courtney Albon, 2024; Linda Kane).

電信網絡

在與主要競爭對手中共或可能挑戰者俄羅斯發生重大衝突的情況下，美國應該預期其國際通信網絡將遭受攻擊，包括針對太空通信和海底電纜的攻擊。美國國家情報總監辦公室(ODNI)在2024年報告中指出：「反太空作戰將成為解放軍潛在軍事行動的關鍵組成部分，中共擁有針對美國及其盟國衛星的反太空武器能力」，而俄羅斯則將在重建其地面部隊的同時，努力提升其已經顯著的反太空能力。中共和俄羅斯都可能威脅到美國的太空資產，而這些資產既對公民日常生活至關重要，也對軍事能力至關重要。約翰·F·普拉姆(John F. Plumb)在2023年4月6日的眾議院《軍事戰略部隊小組委員會》關於國家安全太空活動的聽證會上表示：「中共已經部署了地面反太空武器，並且持續尋求新方法以威脅美國的衛星。」最近一個反太空攻擊的例子是，俄羅斯在2022年1月恢復對烏克蘭的戰鬥期間，於入侵前及入侵期間使用網路攻擊。在此情況下，這些攻擊針對商業衛星通信網絡，通過破壞烏克蘭在危機向衝突過渡期間的指揮與控制，實現了資訊優勢。這些攻擊在入侵烏克蘭前一小時發動，癱瘓烏克蘭及整個歐洲的「極小孔徑終端(VSAT)」，破壞互聯網和能源網絡，影響公民的日常生活。俄羅斯對太空能力的攻擊強化了空軍部長法蘭克·肯德爾(Frank Kendall)提出的觀點，即需要建設更具彈性的美國太空基礎設施和網絡，以抵禦此類攻擊。

The Office of the Director of National Intelligence (ODNI) reported last year that "Russia is particularly focused on improving its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis.'(Office of the Director of National Intelligence, 2023) In August 2024, the Center for International Security Studies also identified the threat posed to undersea cables by Communist China(Daniel Runde, et al, 2024). The Wall Street Journal reported that U.S. officials are warning telecommunications companies that critical undersea cables connecting the U.S. with the Indo-Pacific region are vulnerable to Communist Chinese repair ships(Dustin Volz, et al, 2024). As the Communist Chinese Military, Coast Guard, and Peoples Armed Force Maritime Militia continue to hone their grey zone warfare skills, it is not a stretch that these forces could carry out such attacks simultaneously at scale. Such attacks on infrastructure would be accompanied by cyber-attacks aimed at disrupting critical communications infrastructure between the U.S. and Asia(Sam Barron, 2024).

根據美國國家情報辦公室(ODNI)去(2003)年發布的報告：「俄羅斯特別專注於增強針對關鍵基礎設施的攻擊能力，包括美國及盟國/夥伴國家的水下電纜和工業控制系統，因為破壞此類基礎設施有助於提高並展示其在危機中摧毀基礎設施的能力。」2024年8月，國際安全研究中心(Center for International Security Studies)亦指出，中共對海底電纜構成威脅。《華爾街日報》報導，美國官員警告電信公司，美國與印太地區連接的關鍵海底電纜容易受到中共維修船的威脅。隨著中共軍隊、海警以及民兵海上武裝力量持續提高其灰色地帶作戰技能，可以合理推測，這些力量可能在大規模協同行動中，對基礎設施進行同時攻擊。此類針對基礎設施的攻擊，將伴隨針對美國與亞洲之間關鍵通信基礎設施的網路攻擊，目標是徹底破壞兩地之間的通信能力。

The February 2024 outage of AT&T networks resulted in more than 92 million calls being disrupted for a 12-hour period, including more than 25,000 attempts to call 911 emergency services(David Shepardson, 2024). Although this was not an attack by outsiders, but rather the result of an equipment configuration error, it is not a stretch to conclude that such results could be achieved via disruption attacks by adversary state

actors. It is worth noting that the PLA sees the Strategic Support Force as having "an important role" in "protecting the country's financial security and the security of people's daily lives," indicating that the PLA would see financial networks, and other networks needed for the functioning society, as capabilities the military would defend or attack."(John Colstello, and Joe McReynolds, 2019) Related to this is the threat of State, and State-sponsored cyber actors hacking into the networks of Internet Service Providers (ISP) for the purpose of spying on U.S. government and military personnel to collect intelligence data and support preparations for precision targeting in the crisis phase(Joseph Menn, 2024).

2024年2月，「美國電話與電報公司(AT&T)」網路的中斷，導致超過9,200萬通電話在12小時內無法完成，其中包括超過25,000次撥打911緊急服務。雖然這次事件並非外部攻擊所致，而是由設備配置錯誤引起，但不可否認，類似的結果完全可能通過敵對國家的破壞性攻擊達成此種狀況。值得注意的是，解放軍認為其戰略支援部隊，在「保護國家的金融安全與人民日常生活安全」中扮演「重要角色」，這表明解放軍將金融網絡和其他維持社會正常運作的網絡，視為軍事力量防禦或攻擊的目標。與此相關的威脅還包括國家及國家支持的網路行動者，入侵互聯網服務提供商(ISP)的網路，以對美國政府和軍事人員進行間諜活動，目的是情蒐，並為危機階段的精準打擊提供支援準備。

Financial networks

Data breaches of individual U.S. citizens' financial accounts put them at risk of hacking by state actors for the purpose of depleting their accounts at will during the crisis to create panic. The digitalization of most financial services has complicated the task of protecting the personal and account data of users in the face of cyber attacks, with the number of data compromise incidents involving financial institutions increasing by over 330 percent between 2019 and 2023(Ani Petrosyan, 2024). North Korea could also "engage in economic warfare to steal massive amounts of money or undermine the stability of the international financial system or worldwide markets" and "conduct ransomware attacks on banks to gain money or to disable or destroy computer networks as well as flood the SWIFT [financial messaging] system with fraudulent

transactions."(Heritage Foundation, 2024) In July, AT&T suffered a data breach that disclosed the personal data of approximately 10 million AT&T customers, putting them at risk for identify theft and fraud, as names, phone numbers, addresses, dates of birth, passcodes and Social Security numbers were stolen(Jodi Pierce, 2024). While this attack was attributed to cyber criminals, that does not mean that the PLA would not use the same techniques to launch attacks against individual American citizens as part of a financial network attack.

金融網絡

資料外洩使美國公民的金融帳戶面臨被國家行為者駭入的風險，可能在危機期間隨時掏空帳戶，進一步製造恐慌。金融服務的數位化使得保護使用者個人及帳戶資料的工作更加複雜，根據統計，2019年至2023年間，涉及金融機構的資料洩漏事件數量增長超過330%。此外，北韓可能會「發動經濟戰爭，竊取大筆資金，或破壞國際金融體系和全球市場的穩定性」，並「對銀行進行勒索軟體攻擊以獲取金錢，或者癱瘓甚至摧毀電腦網絡，同時利用偽造交易癱瘓SWIFT金融訊息系統」。2024年7月，「美國電話與電報公司」發生資料洩漏事件，導致約1,000萬名客戶的個人資料被曝光，其中包括姓名、電話號碼、地址、出生日期、密碼及社會安全碼，進一步引發身份盜竊和詐欺風險。儘管此事件歸因於網路犯罪分子，但這並不意味著解放軍不會採取類似手段針對美國個人發動金融網路攻擊。

Water and agriculture networks

Drinking and irrigation water distribution networks, and wastewater treatment networks are also of great concern, with many reports in 2024 of America's adversaries conducting cyber attacks against these networks. Trevor Jockims, from NBC News reported in June of 2024 on cyber attacks against water distribution systems and facilities across several U.S. states, highlighting the potential damage to infrastructure, disruption of the availability or flow of water, and possible chemical contamination of the public drinking water supply(Trevor Laurence Jockims, 2024). Similar attacks have taken place in Europe, as reported by Britain, Czech Republic, Ireland, Germany, and Poland(Newsmax, 2023). EPA Deputy Administrator Janet McCabe listed Communist

China, Russia and Iran as the countries that are "actively seeking the capability to disable U.S. critical infrastructure, including water and wastewater."(CBS News, 2024) Indeed, past attacks on America's water distribution system and utilities have been carried out by Iran and Russia, while the PRC appears for the most part to be focused on maintaining access to strike at a large scale across all the networks it has compromised(Trevor Jockims, 2024).

飲用水與灌溉水分配網絡

飲用水與灌溉水分配網絡及污水處理網絡也是關注重點。2024年多份報告指出，美國對手國家對這些網絡進行多次網路攻擊。根據NBC新聞記者Trevor Jockims的報導，2024年6月，針對多個美國州水分配系統與設施的網路攻擊，對基礎設施造成潛在破壞，干擾水資源的可用性與流量，並可能對公共飲用水供應造成化學污染。類似的攻擊也曾在歐洲發生，受影響的國家包括英國、捷克、愛爾蘭、德國及波蘭。美國環境保護署(EPA)副署長珍妮特 麥卡比(Janet McCabe)指出，中共、俄羅斯及伊朗是「積極尋求癱瘓美國關鍵基礎設施，包括水和污水系統的國家」。事實上，過去伊朗及俄羅斯就曾針對美國的水分配系統與公用事業發動攻擊，而中國大陸似乎專注於保持對大規模網絡的持續攻擊能力。

"Iran-affiliated and pro-Russia cyber actors gained access to, and in some cases have manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight a potential public safety threat and an avenue for malicious cyber actors to cause physical damage and deny critical services."(Office of the Director of National Intelligence, 2024) Attacks on public infrastructure and distribution networks have become more routine. The U.S. Environmental Protection Agency issued a report which revealed that many of the U.S. municipal water distribution systems have "alarming cybersecurity vulnerabilities," which are exemplified in recent attacks on a municipal water filtration plant in Texas close to a U.S. Air Force Base. According to a report, the U.S. Federal Government is not ready to react quickly to such events, especially if conducted at scale, and drinking and wastewater systems large and small, urban and rural are at risk(Sam Barro, 2024). EPA Deputy Administrator Janet McCabe listed

Communist China, Russia and Iran as the countries that are "actively seeking the capability to disable U.S. critical infrastructure, including water and wastewater."(CBS News, 2024)

「與伊朗相關，以及親俄的網路行動者已獲取美國關鍵工業控制系統(ICS)的存取權，並在某些情況下操控包括食品與農業、醫療保健以及水和污水處理領域的系統(2023年底至2024年)。這些攻擊凸顯潛在的公共安全威脅，以及惡意網路行動者造成實體損害與拒絕關鍵服務的可能性。」對公共基礎設施和分配網絡的攻擊已變得更加常見。美國環境保護署發布的一份報告顯示，美國許多市政供水系統存在「令人震驚的網路安全漏洞」，這在德克薩斯州靠近美國空軍基地的市政水過濾廠最近受到的攻擊中得到體現。根據報告，美國聯邦政府尚未準備好迅速應對此類事件，特別是在大規模發生時，大型和小型城市和農村的飲用水和污水系統均面臨風險。美國環境保護署副署長珍妮特 麥卡比指出，中共、俄羅斯和伊朗是「積極尋求癱瘓美國關鍵基礎設施，包括水和污水系統的國家」。

Energy distribution networks

Regarding the energy networks as a target set, it is useful to recall the anxiety across the U.S. that followed Russia's ransomware cyberattack against the Colonial Pipeline on May 27, 2021. That attack resulted in panic all across the eastern seaboard, captured in headlines around the world featuring images of long lines of cars at gas stations with American citizens uncertain of their ability to get fuel needed for getting to work and school, and for daily living(Jen Easterly, 2023). According to the Office of the Secretary of Defense, China is improving its cyberattack capabilities and already has the ability to disrupt U.S. natural gas pipelines for days to weeks(Office of the Secretary of Defense, 2020). Communist China also poses a significant threat to the U.S. electric power networks. Mr. Manny Cancel, Senior Vice President of the North American Electric Reliability Corporation (NERC) explained that "[t]he current geopolitical situation has significant ramifications for the North American [electric power] grid" as demonstrated by the more than doubling of physical attacks or threats on grid infrastructure from 2021 to 2023, and an accompanying "dramatic increase in malicious cyber activity."(Charlie McCarthy, 2024)

能源分配網絡

將能源網絡視為攻擊目標群，回顧2021年5月27日俄羅斯針對殖民管道(Colonial Pipeline)進行勒索軟體網路攻擊後，在美國引發的廣泛焦慮是有幫助的。該次攻擊導致東岸沿線的恐慌情緒，被全球媒體頭條報導，凸顯出美國民眾在加油站大排長龍、不確定是否能取得足夠燃料以應付工作、上學及日常生活需求的景象。根據美國國防部的資料，中共正在提升其網路攻擊能力，目前已具備中斷美國天然氣管道運作數天甚至數週的能力。中共同時對美國電力網路構成重大威脅。北美電力可靠性公司(NERC)高級副總裁曼尼·坎塞爾(Manny Cancel)解釋說：「當前的地緣政治局勢對北美(電力)電網具有重大影響」，這從2021年至2023年間電網基礎設施遭受的實體攻擊或威脅數量超過兩倍增長，以及隨之而來的「惡意網路活動大幅增加」可以得到印證。

Transportation networks

An assessment from the ODNI in 2023 explains that Communist China "…almost certainly is capable of launching cyberattacks that could disrupt critical infrastructure services within the United States," including the oil and gas pipelines needed for automobiles and the trucking industry, and also rail systems(Office of the Director of National Intelligence, 2023). Regarding the latter of these, the electromagnetic spectrum (EMS) and cyber threat to rail systems could achieve a range of effects on rail systems, ranging from disruptive effects on the use of computerized management systems to the destruction of rail stock and deliberate train derailments during the crisis phase. A recent example of a cyberattack for the purpose of disrupting the flow of military supplies and munitions to the theater of operation is found in the thousands of cyberattacks committed against the control systems of Poland and the Czech Republic railways by Russian cyber actors since the start of the Russo-Ukrainian War to disrupt European rail support to Ukraine(Alice Hancock, 2024).

交通運輸網絡

根據2023年美國國家情報總監辦公室(ODNI)的一份評估報告，中共「幾乎可以肯定」能夠發動網路攻擊，破壞美國關鍵基礎設施服務，包括汽車和卡車運輸業

所需的石油和天然氣管道，以及鐵路系統。針對後者，電磁頻譜(EMS)和對鐵路系統的網路威脅，可能對鐵路系統產生一系列影響，從破壞電腦化管理系統的運作，到摧毀鐵路設備，甚至在危機階段蓄意製造火車出軌事件。近期的一個例子是俄羅斯的網路行動者自俄烏戰爭爆發以來，針對波蘭和捷克共和國鐵路控制系統，發動數千次網路攻擊，目的是破壞向烏克蘭提供的歐洲鐵路支援，進一步妨礙軍事物資和彈藥的運輸。

Denying EMS “to train communications, jamming the assigned frequency range for positive train control (PTC) signals, and/or creating incorrect unauthenticated messages are all major security threats to PTC communication.”(Office of Research, Development and Technology, 2020) Cyberattacks on Centralized Traffic Control (CTC) systems (to include “wayside and onboard signaling and messaging systems to deliver the traffic commands to trains by traditional visual, audio or coded circuit signals), and infrastructure for physical control and safety(such as rail switches, interlockings, rail crossings barriers, movable bridges, and miscellaneous yard components) could also shut down rail networks needed both for the functioning of civil society, but also for the movement of forces to air and seaports of debarkation for flow into theater(Office of Research, Development and Technology, 2020). Rail systems have proven to be uniquely vulnerable to ransomware attacks with a history of the rail road companies paying high ransoms, due to the high value of the freight that stalled in transit after control of the system is hijacked(Dan Eness, 2023). The diverse nature of rail road systems networks, to include supervisor control and data acquisition systems, rail control, and dedicated information technologies for customer services, ticketing, onboard mobile applications, and many more, provide multiple attack surfaces for cyber actors to exploit(Israel Baron, 2023). The U.S. Transportation Security Administration (TSA) has responded in December 2022 by publishing a strategic directive establishing new cyberspace requirements on operators to shore up defenses(Transportation Security Agency, 2022), following a previous directive published in January 2022(Security Directive 1580-21-01, 2021).

屏蔽電磁頻譜(EMS)對列車通信的影響，「包括干擾正列車控制(PTC)信號指定頻率範圍，生成錯誤的未經驗證的訊息，都是PTC通信面臨的主要安全威脅。」

針對集中交通控制(CTC)系統的網路攻擊，包括「用於將交通命令傳達給列車的路旁和車載信號及通信系統」，以及基礎設施的物理控制和安全設施(如鐵路道岔、互鎖裝置、鐵路交叉口柵欄、活動橋樑和雜項場站組件)也可能關閉鐵路網絡，這些網絡不僅是民間社會運作所需，還是部隊向空港和海港進出戰區的重要交通工具。鐵路系統在勒索軟體攻擊中表現出特別的脆弱性，鐵路公司為了減少因系統被劫持而導致高價值貨物滯留的損失，曾多次支付高額贖金。鐵路系統網絡的多樣性，包括監控控制和數據採集系統、鐵路控制系統，以及專門針對客戶服務、售票、車載移動應用程序等的資訊技術，為網路行動者提供多個攻擊面。美國運輸安全管理局(TSA)於2022年12月發布一項戰略指令，為營運商設立新的網路空間要求以強化防禦，這是繼2022年1月發布的先前指令後的最新應對措施。

Logistics Networks

Not only do infrastructure attacks have an outsized impact on civilian and military morale, but they can also negatively impact our ability to deploy forces. According to Ms. Sherrod DeGrippo, Director of Threat Intelligence Strategy at Microsoft, indications are strong that Communist China will conduct cyberattacks against the U.S. to prevent and disrupt efforts to provide military assistance in defense of its allies(Sandy Fitzgerald, 2024). The U.S. Army Training and Doctrine Command assesses that our primary adversaries have maintained “the capability to target logistics infrastructure in the United States, which will impact deployment processes during a build-up to conflict” while also pointing out that the crisis phase could be fleeting, or even non-existent, with a quick transition from competition to conflict happening “immediately, leaving no crisis period to begin force flow.”(GEN Gary M. Brito, 2024)

後勤網絡

基礎設施攻擊不僅對平民和軍隊士氣造成巨大影響，還會負面影響我軍部隊的部署能力。根據微軟威脅情報戰略總監德格里波(Sherrod DeGrippo)女士的說法，有強烈跡象表明，中共將對美國發動網路攻擊，以阻止和破壞美國提供軍事援助，來保衛其盟友的努力。美國陸軍教育與準則司令部評估認為，我們的主要對手已具備「針對美國後勤基礎設施的能力，這將影響戰爭準備期間的部隊部署過程」，同

時指出危機階段可能是短暫的，甚至可能根本不存在，因為從競爭轉變為衝突可能「立即發生，沒有危機階段來開始部隊流動準備」。

Among the many infrastructure targets in the crosshairs of the PLA is the network of commercial seaports that would support force flow into the Indo-Pacific Theater to defend America's allies and partners. In 2023, the Department of Transportation Maritime Administration warned that U.S. seaports are vulnerable to cyberattacks due to the multiple stakeholders involved in the operation of the port, with risks identified related to facility access, terminal headquarters, operational technology systems such as communication systems and cargo handling equipment, positioning, navigation, and timing services(Lori Ann LaRocco, 2024). Exploiting these vulnerabilities would impact vessel movements and the complex logistics systems at port facilities. U.S. intelligence officials acknowledged the PRC cyber threat and its access to U.S. Pacific seaports and other infrastructure that would "enable China to sow panic and disrupt America's ability to move troops, weaponry and supplies to Taiwan if armed conflict breaks out."(Joseph Menn, 2024)

在解放軍瞄準的眾多基礎設施目標中，包含支撐部隊向印太戰區運輸的商業海港網絡，旨在防衛美國的盟友和夥伴。2023年美國交通部海事管理局警告，美國海港因涉及多個利益相關的操作而容易遭受網路攻擊，已發現的風險包括設施使用權、碼頭總部、操作技術系統(例如通信系統和貨物處理設備)、定位、導航和定時服務，利用這些漏洞將影響船隻的移動以及港口設施的複雜後勤系統。美國情報官員承認，中共的網路威脅及其對美國太平洋海港和其他基礎設施的威脅，可能「使中國能夠製造恐慌，並破壞美國在爆發武裝衝突時向臺灣運送部隊、武器和補給的能力」。

The Defense Industrial Base

The U.S. should also expect attacks against its Defense Industrial Base (DIB), which has struggled to produce and deliver major combat and combat support systems in a cost-effective and timely manner to the U.S. Military, and which now lacks the "ability to procure at scale the goods and services it needs to fight a major war."(John Ferrari & Charles Rahr, 2023; Sean Durns, 2024) The Heritage Foundation has made the case that

the current paradigm used to evaluate the health and productivity of our DIB, namely the three variables of cost, schedule, and performance, are no longer sufficient, and a “fourth factor—resilience—must be added to this paradigm.”(The Heritage Foundation, 2024) In the event of conflict with Communist China, the U.S. Defense Industrial Base would need to quickly shift to war-time requirements to be prepared for the unknown and worst-case scenarios. The inter-connectedness of the U.S. DIB globally for components and systems creates a vulnerability for Communist China to interdict in time of crisis.

國防工業基地(DIB)

美國應預期其國防工業基地(DIB)將遭受攻擊，該基地在以具成本效益和及時的方式，為美軍生產和交付主要戰鬥及支援系統，目前缺乏「大規模採購作戰所需商品和服務的能力」。傳承基金會(Heritage Foundation)認為，目前用來評估國防工業基地健康狀況和生產力的模式，即成本、時程和績效三個變量，已不足以應對當前挑戰，並主張必須加入「第四個因素—韌性」至該模式中。如果與中共爆發衝突，美國的國防工業基地必須迅速轉向戰時需求，以應對未知和最壞的情境。美國國防工業基地在全球的零組件和系統相互依賴性，使其在危機時易於被中共所中斷。

Conducting peacetime “Resources warfare” Communist China is 'quietly shutting down' material US needs to make weapons, namely special materials and minerals after the U.S. has become dependent on access to PRC markets(Fox News, 2024). In crisis, the PRC would completely cut off access to the critical minerals needed to run the U.S. economy and to build weapon systems(Michael E. O’Hanlon and Alejandra Rocha, 2024; Harman, et al, 2024). In peacetime, the PRC has near complete control over the global production of rare earth metals, which are vital to the technologies associated with modern communications, power generation and dissemination, military weapons, and electric vehicles. In 2023, in retaliation to Washington’s ban on the sale of advanced computer chips to China and restrictions on American investment in Chinese technology, the PRC cut off sales of these rare earth metals to the U.S(Milton Ezrati, 2023). If the U.S. DIB is not resilient, then it further complicates U.S. decision-making about entering into a war with Communist China. In the case of the Russo-Ukrainian War, the Russian defense industry was initially slow to make the shift to wartime production, and failed to

make this shift until the tide of battle had turned against Russian forces. Russian efforts to 'jump start' the Russian DIB in earnest came ten months after the full invasion of Ukraine commenced, but recovered enough capacity to provide Russian military forces much needed resources and the ability to sustain the offensive. According to a research paper published by the Chatham House, the Russian "military industry has displayed latent resilience in its ability to deliver military equipment and hardware in the war against Ukraine,"(Mathieu Boulègue, et al, 2024) and the U.S. must be prepared to do likewise now in the face of likely attacks from the PLA and Ministry of State Services to hobble it. Assessing the current state of the U.S. DIB, the DoD National Defense Strategy Commission reported it has a "severely limited surge capacity marked by underinvestment in idle capacity and modern infrastructure, equipment, and tooling" that might see the U.S. facing many of the same obstacles Russia has encountered in its war against Ukraine(Harman, et al, 2024). Other assessments of the U.S. DIB are more critical, saying that the inadequacy, and atrophied state of the U.S. DIB could mean defeat in a war against a great power(Tom Rogan, 2024; Sean Durns, 2024).

中共在和平時期進行「資源戰爭」，悄然切斷美國製造武器所需的材料，特別是特殊材料和礦物，因為美國已經對中國市場的供應形成依賴。在危機中，中共將完全切斷美國運行經濟及建造武器系統所需的關鍵礦物。在和平時期，中共幾乎完全控制稀土金屬的全球生產，而稀土金屬對現代通信技術、發電與傳輸、軍事武器和電動車的技術至關重要。2023年為報復華盛頓禁止向中共銷售先進電腦芯片，及限制美國投資於中國大陸的技術，中共停止向美國出售這些稀土金屬。如果美國的國防工業基地缺乏韌性，這將進一步使美國在與中共爆發戰爭時的決策，變得更為複雜。在俄烏戰爭中，俄羅斯的國防工業最初在轉向戰時生產方面反應遲緩，直到戰事形勢對俄羅斯部隊不利後才開始轉型。俄羅斯努力「重啟」其國防工業基地的工作，始於全面入侵烏克蘭10個月後，但仍足夠恢復供應俄羅斯軍隊急需的資源，以及支持攻勢的能力。根據查塔姆研究所(Chatham House)的一份研究報告，俄羅斯「軍事工業在提供軍事裝備和硬件方面顯示出潛在的韌性」，而美國現在也必須在應對解放軍和國家安全部可能對其造成的攻擊時，具備類似的應對能力。根據美國國防部國防戰略委員會的評估，美國國防工業基地「嚴重缺乏擴產能力，因閒置產能、現代化基礎設施、設備和工具投資不足」而陷入困境，可能會讓美國面臨俄羅

斯在對烏克蘭戰爭中遇到的同樣障礙。其他對美國國防工業基地的評估則更為批評，認為其不足和衰退的狀態可能意味著在與大國的戰爭中面臨失敗的風險。

The ultimate decision that Communist China would seek as a result of its disruptive decision superiority attacks in the Crisis Phase, would be that of the U.S. deciding whether to go to war following the PLA's opening gambit to invade and subjugate the free and democratic people of the Republic of China on Taiwan.
中共在危機階段透過其具有干擾性的決策優勢，攻擊所追求的最終目標，是讓美國在面臨解放軍開局的行動—侵略並征服中華民國(臺灣)自由與民主的人民後，做出是否開戰的決擇。

PRC Concept of 'War Control'

The PLA seeks to achieve "War Control" at the strategic level at the opening of the crisis, a concept that the PLA describes as controlling the pace, intensity, and escalation of a conflict vis-à-vis its adversary(Edmund J. Burke, 2023). The PLA's 2015 Science of Military Strategy explains that the objective of Communist China's "war control" strategy, "…is to prevent the occurrence of war and, once war is inevitable… to control its horizontal and vertical escalation and do the most to reduce the negative consequences or to gain a major victory at minor cost."(David Santoro, 2023) The PLA's 2020 Science of Military Strategy explains that War Control is achieved via managing the crisis phase in order to "control and guide" the developments of a crisis "in a direction that is beneficial." (David Santoro, 2023) The concept of "War Control" can be seen as the ultimate strategic level of information advantage to be obtained in the crisis phase. The goal for the CCP would be to convince U.S. leaders to choose not to fulfill the commitment made by President Joe Biden to defend a major non-NATO ally, and instead, make a *No War* decision. The general approach would be to conduct "decision superiority attacks" against the U.S. decision-making process at all levels, to profoundly disrupt decision making during the crisis phase. According to George Galdorisi, a major intent of cyberattacks against our networks "is to show – or completely stop – leaders in the country from making the timely decisions needed to mount an effective defense against military assaults…[and] manipulate individuals to make suboptimal decisions."(George Galdorisi, 2024) PRC attacks against U.S. networks provides the ability to accomplish this goal, by leveraging the panic and chaos resulting from the shutdown of critical networks via influence

operations to persuade Americans that “the cost of going to war over Taiwan are outweighed by any prospective benefits.”(Tom Rogan, 2024)

中共的「戰爭控制權」概念

解放軍試圖在危機初期於戰略層面實現「戰爭控制權」，這是一個解放軍所描述的概念，旨在控制與對手間的衝突節奏、強度及升級。解放軍《2015年軍事戰略科學》指出，中共「戰爭控制權」策略的目標是：「避免戰爭的發生；一旦戰爭不可避免……則控制其水平和垂直方向的升級，並竭盡全力減少負面影響，或以最小代價獲得重大勝利。」解放軍《2020年軍事戰略科學》進一步說明，「戰爭控制權」是通過管理危機階段來「控制並引導」危機發展朝有利方向演進。「戰爭控制權」概念可視為在危機階段，獲得最終的戰略層面資訊優勢。中共的目標是說服美國領導人選擇不履行拜登總統做出的防衛主要非北約盟友的承諾，並做出「不戰」的決定。中共的總體策略是針對美國各級決策過程實施「優勢攻擊決策」，以在危機階段徹底擾亂其決策。根據喬治·加多里西(George Galdorisi)的說法，針對美國網路的主要攻擊意圖在於「阻止或完全阻斷國內領導人做出有效防禦軍事攻擊所需的及時決策……並操控個人做出次優決策」。中共對美國網路的攻擊能力支持其實現這一目標，通過關鍵網絡被關閉所引發的恐慌與混亂，運用影響行動來說服美國民眾「為臺灣開戰的成本大於任何預期收益」。

When Deterrence Fails: Information Advantage in Conflict

Retaining information advantage through the crisis phase is critical to regaining the initiative and transitioning to offensive retaliatory action. In conflict, joint forces must be able to attain temporary and local information advantage in decisive areas and points in time where forces and effects are massed against enemy forces and capabilities. As the U.S. and her allies and partners develop new task-focused units, formations, and operations concepts designed disrupt adversary efforts to paralyze U.S., ally and partner military responses, we need to maintain a focus on the collective adversary and maintain information (and decision) advantage for both crisis and conflict. We also collectively need to be able to take the first blow and recover quickly. This will require efforts to harden the infrastructure over which military and government C2 networks

function. Accordingly, there are both offensive and defensive capabilities and actions that should be implemented now, to acquire capabilities to counter adversary command, control, computer, communication, cyber, intelligence, surveillance, and reconnaissance (C5ISR) when the crisis erupts, along with the counter-coercion, counter malign influence, and counter propaganda in peacetime competition to deny our adversaries' efforts to achieve the desired effects.

當威懾失效時：衝突中的資訊優勢

在危機階段保持資訊優勢，對於奪回主動權並過渡到攻勢報復行動至關重要。在衝突中，聯合部隊必須能夠在關鍵地區和時間點，獲得暫時且局部的資訊優勢，這些地區和時間點是集中力量與效果，對抗敵方部隊和能力的核心所在。隨著美國及其盟友和夥伴發展新的專項單位、編隊和作戰概念，來破壞敵方企圖癱瘓美國、盟友及夥伴軍事反應的努力，我們需要聚焦於共同的對手，同時在危機和衝突中保持資訊及決策優勢。我們還需要共同具備承受首次打擊及迅速恢復的能力。這將需要加強軍事和政府指揮控制(C2)網絡運行所依賴的基礎設施。因此必須立即實施進攻性和防禦性能力及行動，以獲得對抗敵方指揮、控制、電腦、通信、網路、情報、監視和偵察(C5ISR)的能力，同時在和平競爭中採取反脅迫、反惡意影響和反宣傳行動，以阻止敵方達成其預期效果。

The hardening of our numerous U.S. networks that are vital to the normal functions of society should be a priority, in order to deny our adversaries the "awing" effects they seek to demoralize and fragment our society in the crisis phase. Success in this task will enable friendly forces to mobilize and deploy more quickly, and in a deliberate and controlled manner. Colin Kahl, the Under Secretary of Defense for Policy explained the importance of resilience as a component of the U.S. National Defense Strategy by highlighting the nature of the threat: ""The reason resilience is important is that our adversaries have gone to school on the American way of war" and "[t]hey understand the American reliance on various networks in cyber and space in the informational domain, and they have spent hundreds of billions of dollars to try to hold those networks at risk." (Jim Garamone, 2022)

加固美國眾多對社會正常運作至關重要的網絡應該是優先事項，目的是防止

敵方在危機階段試圖透過「震懾」，使我們的社會陷入士氣低落和分裂。完成這一任務將使友軍能夠更快、更有條理地動員和部署，以達到可控的效果。美國國防政策次長科林·卡爾(Colin Hackett Kahl)強調，「韌性」做為美國國家防務戰略組成部分的重要性，他指出：「韌性之所以重要，是因為對手已經深入學習美國的作戰方式」，並表示，「他們理解美國在網路與空間資訊領域的依賴，並投入數千億美元試圖使這些網路處於風險之中。」

Maintaining information advantage at the opening of the conflict will require resilient and redundant C2 systems for military operations, as well as resilient civilian infrastructure networks vital to the functioning of society. Our adversaries will go after military and civilian targets to achieve non-kinetic effects and create multiple military operational challenges in the theater of operations, while continuing their attacks in the homeland to create multiple and cascading challenges for the civilian population. Communist Chinese cyberattacks against the U.S. launched in the crisis phase would be part of an early shaping campaign, seeking to seize the advantage(Marco J. Lyons, 2024). As crisis transitions to conflict, the PLA's military science of campaigns emphasizes the importance of achieving information superiority at the battlefield, campaign, and strategic levels of war. The PLA conceives of "an information offensive" that is "the application of a variety of information operation weapons in "soft"-"hard" integrated assault activities conducted against the enemy's information systems, with the goal of damaging or disrupting friendly information systems, thus creating the "the conditions for seizing information superiority." (China Aerospace Studies Institute, 2006) The U.S. Army TRADOC G2 assesses that such attacks "can create outsized effects at relatively low cost and effort and with less risk of escalation than traditional kinetic strikes." (GEN Gary M. Brito, 2024)

在衝突初期維持資訊優勢，需要具備韌性及充份的軍事行動指揮與控制(C2)系統，以及對社會正常運作至關重要的韌性民用基礎設施網絡。敵方將針對軍事和民用目標以實現非物理效果，並在作戰區域內創造多重軍事行動挑戰，同時持續對本土發動攻擊，為平民帶來多層次的連鎖性挑戰。中共在危機階段針對美國發起的網絡攻擊將屬於早期塑造行動的一部分，旨在奪取優勢。隨著危機向衝突轉變，中共解放軍的戰役軍事科學強調在戰場、戰役和戰略層面實現資訊優勢的重要性。解放

軍將「資訊進攻」構想為運用多種資訊作戰武器，採取「軟硬」結合的綜合攻擊行動，針對敵方的資訊系統進行打擊或破壞，從而創造「奪取資訊優勢的條件」。美國陸軍教育與準則司令部(TRADOC)G2評估認為此類攻擊「能以相對低的成本和努力產生巨大效果，並且比傳統物理打擊面臨的升級風險更小」。

In the initial stages of a conflict, the PRC will seek to "create disruptive and destructive effects—from denial-of-service attacks to physical disruptions of critical infrastructure — to shape decision-making and disrupt military operations" by targeting and exploiting perceived weaknesses of militarily superior adversaries that rely on technology(Office of the Secretary of Defense, 2020). PLA doctrines emphasize that operations will be undertaken to achieve information superiority before kinetic operations begin which would include ramping up the information operations carried out in the crisis phase. According to PLA operational concepts, "non-kinetic activities, such as attacks on adversary space or intelligence, surveillance, and reconnaissance (ISR) assets, may be conducted to enable operations in the information domain, but major conventional attacks may be withheld until commanders feel that they have established information superiority and set conditions for rapid and decisive application of kinetic capabilities." (Edmund J. Burke, 2023) These activities would take place during a murky and then very abrupt transition between the crisis and conflict phases.

在衝突初期，中共將尋求「製造破壞性和毀滅性的影響—從阻斷服務攻擊(DoS)到對關鍵基礎設施的實體破壞，以影響決策並干擾軍事行動」，其目標是針對並利用對手的倚賴軍事技術優勢的認知弱點。解放軍的教條強調，行動將以實現資訊優勢為目標，並在「物理殺傷」(Kinetic Operations)開始之前進行，這包括在危機階段加強進行的資訊作戰。根據解放軍的作戰概念，「非物理殺傷，例如對敵方太空或情報、監視與偵察(ISR)資產的攻擊，可能會用於支援信息領域的作戰，但重大常規攻擊可能會被推遲，直到指揮官認為他們已建立起資訊優勢，並創造快速且果斷運用物理殺傷能力的條件。」這些活動通常發生在危機階段與衝突階段之間的一個模糊且極為迅速的過渡期內。

As the PLA transitions from crisis into conflict, its SSF will execute its wartime of achieving "decision superiority," which supports and coordinating information-related capabilities to capitalize on kinetic strikes(Patrick Cunningham, 2023). Decision

Superiority was defined in the year 2000 by RAND as “the ability to make better decisions and to arrive at and implement them faster than an opponent can react.”(Dan Gonzales, et al, 2000) More recently, Gen, USAF, Ret. Glen D. VanHerck, former commander of U.S. Northern Command (USNORTHCOM) described decision superiority as “a condition that follows from “the dissemination of data and information to the right leaders at the right time from the tactical to the strategic level.”(Jim Garamone, 2023) ADM John Aquilino, former Commander of INDOPACOM, described decision superiority for U.S. forces as “the ability to blind, see and kill any adversary that decides to take us on” enabled by technologies that degrade the enemy’s ability to see and understand the battlefield with regard to friendly and enemy force disposition, while accelerating the same for the friendly force and permitting them acquire, target and strike enemy forces(Jennifer Griffin, 2023). This definition shares the same practical focus of the PLA version focused on destroying enemy forces and systems.

隨著解放軍從危機階段轉向衝突階段，其戰略支援部隊將執行其戰時目標—實現「決策優勢」，該目標支援並協調資訊相關能力，以充分發揮物理打擊的效用。「決策優勢」在2000年由RAND公司定義為「能夠做出更好的決策，並以比對手反應更快的速度達到和實施這些決策的能力。」最近，前美國空軍上將格倫·德·范赫克(Glen D. VanHerck)，曾任美國北方司令部(USNORTHCOM)司令，描述了決策優勢為「一種狀態，這種狀態源自於從戰術到戰略層級，將數據和資訊傳遞給正確領導者的能力。」而前印太司令部司令約翰·阿奎利諾(John Aquilino)進一步闡釋美軍的決策優勢，他將其描述為「使我們能夠遮蔽敵人、洞察敵人，並擊殺挑戰我們的對手的能力」，這是通過削弱敵人對戰場友軍和敵軍力量分布的洞察能力，同時加速友軍的洞察和打擊能力來實現的。這些定義與解放軍的實踐重點一致，均聚焦於摧毀敵方部隊和系統。

The PLA’s theory of victory in modern warfare also incorporates “system destruction warfare “as the current method of modern war fighting that seeks to disrupt, paralyze, or destroy the operational capability of the enemy’s operational system.”(Jeffrey Engstrom, 2018) Operations designed and carried out under this construct support decision superiority. Likewise, Russian “informational-technical operations” also seek to manipulate or destroy information systems and networks(GEN

Gary M. Brito, 2024). The Office of the Secretary of Defense's annual report to the U.S. Congress in 2020 explained that the PLA would coordinate the employment of space, cyber, and electromagnetic warfare (EW) as strategic weapons to "paralyze the enemy's operational system of systems" and "sabotage the enemy's war command system of systems" early in a conflict(Office of the Secretary of Defense, 2020). The PLA's SSF would be ready to employ both kinetic and non-kinetic strikes as the crisis-phase gives way to conflict. This would be consistent with PLA military writings emphasizing that "…the employment of cyber and kinetic strikes can create a self-reinforcing cycle that paralyzes an adversary at the outset of conflict."(John Costello and Joe McReynolds, 2019)

解放軍的現代戰爭勝利理論還融入「系統破壞戰」，這被視為當前現代戰爭的主要作戰方法，目的是干擾、癱瘓或摧毀敵方作戰系統的運作能力。在此理論框架下，設計和執行的行動支持了決策優勢。同樣，俄羅斯的「資訊-技術作戰」也旨在操縱或摧毀資訊系統和網路。美國國防部長辦公室2020年向國會提交的年度報告中解釋道，解放軍將協調運用太空、網路和電磁戰作為戰略武器，以「癱瘓敵方的作戰系統」，並在衝突初期「破壞敵方的戰爭指揮系統」。解放軍的戰略支援部隊已經準備好在危機階段向衝突過渡時，同時實施物理和非物理打擊，這與解放軍的軍事著作強調的內容一致，即「網路和物理打擊的協同運用，可以創造一個自我強化的循環，從而在衝突初期癱瘓對手。」

To carry out supporting operations enabling decision superiority attacks, the PLA will also employ the SSF's Information operations group, whose purpose" is to command all information operations units within the operational system, specifically various electronic and network warfare units."(Jeffrey Engstrom, 2018) The PLA's concept of "campaign information warfare" refers to the comprehensive "operational activities on the battlefield directed at the enemy's information systems" for the purpose of "seizing information superiority and thus forming strategic and campaign superiority in order to create conditions for winning a decisive engagement(China Aerospace Studies Institute, 2006). The PLA will also ramp up psychological operations (PSYOP) initiated in the crisis phase to erode the will of its opponents. The U.S. Army assesses that the ability of adversaries to rapidly influence the information and human dimensions will further

challenge the ability of U.S. joint forces to achieve information advantage in a large scale combat operations(GEN Gary M. Brito, 2024).

為了支持實現決策優勢的作戰，解放軍還將動用戰略支援部隊的資訊作戰群，其目的是「指揮作戰系統內的所有資訊作戰單位，特別是各種電子和網路戰單位。」解放軍的「戰役信息戰」概念是指一種綜合性的「在戰場上針對敵方信息系統的作戰行動」，目的是「奪取信息優勢，從而形成戰略和戰役優勢，為贏得決定性交戰創造條件。」此外，解放軍還將在危機階段加強心理作戰(PSYOP)，旨在削弱對手的意志力。美國陸軍評估指出，敵方快速影響資訊和人類維度的能力，將進一步挑戰美軍聯合部隊在大規模作戰中實現資訊優勢的能力。

Quo tendimus - Where do we go from here?

As the preceding analysis makes clear, if the U.S. and her allies and partners seek to remain in peacetime competition, then the integration of national deterrence strategies must include demonstrating that we are capable of withstanding a concerted attack on our infrastructure networks, which requires making them more durable and resilient. According to the 2023 Joint Chiefs of Staff Joint Concept for Competing, deterrence by denial can be achieved in multiple ways, starting with building national resilience to be able to withstand actions the adversary may take(GEN Mark Milley, 2023). Taking steps to counter and reverse adversary footholds in our critical infrastructure networks would contribute to deterrence, but this will be a challenge. Our adversaries are entrenched in our infrastructure networks. If not countered, this access provides them the ability to create the chaos that could potentially sap the will to resist or retaliate in a crisis/conflict in the face of a breakdown of modern society following network attacks. Accordingly, if our deterrence efforts fail and a conflict breaks out in the Indo-Pacific Theater, we must be ready to counter and blunt the effects of the adversaries' disruptive effects, which might initially be of a primarily non-kinetic nature, and which are intended to ultimately confound, delay, and disrupt U.S. policy making and response actions. Protecting against these largely non-lethal attacks described in the previous sections, by hardening and making more resilient the systems we expect our adversaries will target, can deny them the information advantage they seek.

我們目標是什麼？接下來何去何從？

根據上述分析，如果美國及其盟友與夥伴，希望繼續在和平競爭中佔據主導地位，那麼國家威懾戰略的整合，必須包括展示我們有能力抵禦，針對基礎設施網路的有計畫攻擊。這需要使這些網路更加耐用且具有韌性。根據2023年聯席參謀部《競爭聯合概念》的說法，可以通過多種方式實現拒止威懾，首先是建立國家韌性，以承受敵方可能採取的行動。採取措施反制並逆轉敵人在我們關鍵基礎設施網絡中的立足點，將有助於威懾，但這將是一項挑戰。敵人已經深嵌入我們的基礎設施網絡，如果不加以遏制，這種滲透將賦予他們在危機或衝突中，通過網路攻擊導致現代社會瓦解的情況，製造混亂、削弱美國抵抗或反擊意志的能力。因此，如果威懾努力失敗，印太地區爆發衝突，我們必須做好準備，反制並減弱敵方破壞性效果的影響，這些破壞性行動最初可能主要是非物理性質，最終旨在混淆、延遲並破壞美國的政策制定和應對行動，通過強化並提高我們預期敵方將針對的系統的韌性，可以防止他們獲得所尋求的資訊優勢。

The U.S. needs to improve dramatically the level of resilience of the various networks that Communist China is likely to attack in a bid to keep America out of the war it plans to wage on the Republic of China on Taiwan. This is not a problem for the U.S. military alone, and certainly not one that it can solve single-handedly. Knowing what kinds of decision superiority attacks to expect in the crisis phase; countering CCP malign influence, Three Warfares, United Front Work and other influence operations, and; combatting CCP efforts to further penetrate our networks in preparation for Network Attacks intended to create chaos and panic will enables the U.S. military to plan with a clear appreciation of the problem to address these threats in peacetime competition. Ultimately however, the decision to fight, *War or No War,* is not one for the U.S. military to make. Demonstrable and credible improvements in the resilience of the U.S. networks already in the target sights of Communist China as described in this paper will contribute to overall deterrence. The PLA may lose confidence in its ability to exercise "War Control" during the crisis phase if its "decision superiority attacks" fizzle out against more resilient and well-defended networks. This paper also attempted to highlight the importance of countering Communist Chinese efforts to improve their odds in crisis via their peacetime "Unrestricted Warfare," United Front Work, and influence operations

aimed to polarize U.S. society to prevent unanimity and cohesion when the PLA commences its invasion across the Taiwan Strait. For the “decision superiority attacks” to create domestic political problems for the U.S. President, there must first be success in peacetime influence operations against the U.S. citizenry. Improving our peacetime competition strategic communications, both externally and domestically, and educating American citizens on the threats faced is a first step to inoculate America from the malign influence of Communist China in the homeland that creates the conditions necessary for the transition from peacetime competition, to crisis and conflict.

美國需要顯著提高其各種網絡的韌性，這些網絡可能成為中共攻擊目標，目的是阻止美國介入中共針對中華民國(臺灣)的作戰計畫。這不僅僅是美國軍方的問題，也絕非美國能單方面解決的問題。瞭解危機階段可能面臨哪些決策優勢攻擊；反制中共的惡意影響行為、「三戰」、統戰工作及其他影響行動；以及遏制中共進一步滲透我們網路，為進一步的網路攻擊做準備，這些都使美國軍方能夠清楚地認識問題，並在和平競爭中應對這些威脅，然而，最終決定是否參戰並非美國軍方可決定。本文所描述的，提高美國網路韌性的顯著和可信的努力，將有助於整體威懾。如果中共的「決策優勢攻擊」在更具韌性和防禦力的網絡面前失敗，中共可能會對其在危機階段實施「控制戰爭」的能力失去信心。本文還試圖強調，反制中共通過和平時期的「超限戰」、統戰工作及影響行動來提高其成功機率，這些行動旨在分裂美國社會，防止在解放軍穿越臺灣海峽展開入侵時美國達成一致和凝聚力。為了使「決策優勢攻擊」能夠給美國總統製造國內政治問題，首先必須在和平時期的對美國民眾造成適度的影響，而改善我們在和平競爭時期的戰略傳播能力，無論是對外還是國內，並教育美國公民瞭解所面臨的威脅，是保護美國免受中共在美國國內惡意影響的第一步，為從和平競爭過渡到危機與衝突創造必要條件。

參考文獻

Air and Space Forces Magazine (2023/1/ 30). Read for yourself: The full memo from AMC Gen. Mike Minihan. *Air & Space Forces Magazine*. Retrieved fr om https://www.airandspaceforces.com/read-full-memo-from-amc-gen-mike-mini han/.

Albon, C. (2024/8/26). Securing US space assets is busting the Air Force budget , Kendall says. *Defense News*. Retrieved from https://www.defensenews.com/s pace/2024/08/27/securing-us-space-assets-is-busting-the-air-force-budget-kendall-s ays/.

Associated Press. (2024/7/25). North Korean charged in cyberattacks on US hospi tals, NASA, and military bases. *U.S. News & World Report*. Retrieved from https://www.usnews.com/news/world/articles/2024-07-25/alleged-north-korean-hac ker-indicted-for-cyber-attacks-on-american-hospitals.

Avdaliani, E. (2024/3/6). Iran and Russia enter a new level of military cooperati on. *The Stimson Center*. Retrieved from https://www.stimson.org/2024/iran-and -russia-enter-a-new-level-of-military-cooperation/.

Baggage, R. (2023/2/27). A war with China would be unlike anything Americans faced before. *The New York Times*. Retrieved from https://www.nytimes.com /2023/02/27/opinion/a-war-with-china-would-reach-deep-into-american-society.ht ml.

Bardolf, D.(2023/10/12). Putin, Iranian President Masoud Pezeshkian meet for firs t time, hailing ‘robust’ relationship. *New York Post*. Retrieved from https://ny post.com/2024/10/12/world-news/russian-iranian-presidents-proclaim-robust-relati onship/.

Baron, I. (2023/9/13). Rail cybersecurity is a complex environment. *Informatech*. Retrieved from https://www.darkreading.com/ics-ot-security/rail-cybersecurity-is-a-complex-environment.

Barron, S. (2024/6/3). Report: Chinese hackers target U.S. infrastructure. *Newsma x*. Retrieved from https://www.newsmax.com/newsfront/china-us-hacking/2024/0 6/03/id/1167303/.

Barron, S. (2024/6/26). Report: Water systems vulnerable to hackers. *Newsmax*. Retrieved from https://www.newsmax.com/newsfront/water-systems-hackers-cyberc rime/2024/06/26/id/1170248/.

Bennett, B. W. (2023/9/13). North Korea, Russia and China: The developing trilateral imperialist partnership. *RAND Corporation*. Retrieved from https://www.rand.org/pubs/commentary/2023/09/north-korea-russia-and-china-the-developing-trilateral.html.

Blinken, A. J. (2022/5/10). Attribution of Russia's malicious cyber activity against Ukraine [Press statement]. *U.S. Department of State*. Retrieved from https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

Bloomberg News (2019/5/14). China vows 'people's war' as trade fight takes nationalist turn. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-05-14/china-vows-people-s-war-as-trade-fight-takes-nationalist-turn.

Boulègue, M., Bronk, J., Hird, K., Kerr, J., Lee, R., Petersen, M. B., & others. (2024/7/9). Assessing Russian plans for military regeneration. *Chatham House*. Retrieved from https://www.chathamhouse.org/2024/07/assessing-russian-plans-military-regeneration/08-conclusion.

Brito, G. M. (2024). Operational environment 2024-2034: Large-scale combat operations, pp. 2-19. *U.S. Army Training and Doctrine Command*. Retrieved from https://g2webcontent.z2.web.core.usgovcloudapi.net/OEE/Story%20Posts/TRADOCG2_2024JUL30_OE_2024_2035_Lg_Scale_Comb_anonymous.pdf.

Burke, E., Gunness, K., Cooper, C. A. III, & Cozad, M. (2020). People's Liberation Army operational concepts, pp. 1-14. *RAND Corporation*. Retrieved from https://www.rand.org/pubs/research_reports/RR3139.html.

Carlson, C., Bouffard, T., & Burke, R. (2024/7/1). Defining pacing threats and challenges to homeland defense and security. *Journal of Indo-Pacific Affairs*. Retrieved from https://www.bloomberg.com/news/articles/2019-05-14/china-vows-people-s-war-as-trade-fight-takes-nationalist-turn.

CBS News (2024/1/1). North Korea's Kim Jong Un orders military to "thoroughly annihilate" U.S. if provoked, state media say. *Associated Press*. Retrieved f

rom https://www.cbsnews.com/news/north-korea-kim-jong-un-us-missile-tests-threat-nuclear-war/.

CBS News (2024/5/20). Cyberattacks on water systems: EPA, utilities take action. Retrieved from https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/.

Channel 1 (Iran) (2023/11/1). Iranian Supreme Leader Ayatollah Ali Khamenei: Death to America is not just a slogan, it is a policy. *Memri TV*. Retrieved from https://www.memri.org/tv/iran-supreme-leader-ayatollah-ali-khamenei-death-america-not-slogan-policy-west-protests.

Cheng, D. (2022/2/17). PLA perspectives on network warfare in "informationized local wars" [Testimony before U.S.–China Economic and Security Review Commission]. *U.S.–China Economic and Security Review Commission*. Retrieved from https://www.uscc.gov/sites/default/files/2022-02/Dean_Cheng_Testimony.pdf.

China Aerospace Studies Institute (2006). *In their own words: Foreign military thought science of campaigns,* pp. 175-660.

CIO staff (2024/8/1). CrowdStrike failure: What you need to know. *CIO*. Retrieved from https://www.cio.com/article/3476789/crowdstrike-failure-what-you-need-to-know.html.

Costello, J., & McReynolds, J. (2019). China's Strategic Support Force: A force for a new era. In P. C. Saunders, A. S. Ding, A. Scobell, A. N. D. Yang, & J. Wuthnow (Eds.), Chairman Xi remakes the PLA, P. 480. National Defense University Press.

Cunningham, P. (2023/2/19). PLA information warfare and military diplomacy: A primer on modernization trends. *Small Wars Journal*. Retrieved from https://smallwarsjournal.com/jrnl/art/pla-information-warfare-and-military-diplomacy-primer-modernization-trends#_ftnref15.

Dahl, Z. (2024/8/2). Radical Marxists, Islamists united against the rest of us. *Newsmax*. Retrieved from https://www.newsmax.com/zivadahl/marxists-islamists-antisemitism/2024/08/02/id/1174991/.

Davenport, K. (2024/6/19). North Korea, Russia strengthen military ties. *Arms Co ntrol Today*. Retrieved from https://www.armscontrol.org/act/2024-07/news/nort h-korea-russia-strengthen-military-ties.

Demarest, C. (2024/6). Volt Typhoon hacks likely to inspire copycats, Mahlock s ays. *Defense News*, 39(6), 28.

Donlevy, K. (2024/10/19). Ukraine warns 11K North Korean troops 'ready to fig ht' alongside Russia. *New York Post*. Retrieved from https://nypost.com/2024/ 10/19/world-news/11k-n-korean-troops-ready-to-fight-with-russia-ukraine/.

Dougherty, C. (2021/9/9). Confronting chaos: A new concept for information adv antage. *War on the Rocks*. Retrieved from https://warontherocks.com/2021/09/ confronting-chaos-a-new-concept-for-information-advantage/.

Durns, S. (2024/5/14). *Washington Examiner*, 30(17), 24–47.

Durns, S. (2024/5/14). Taking the China threat seriously means getting on a war footing now. *Washington Examiner*, 30(17), 46-47.

Engstrom, J. (2018/2/1). Systems confrontation and system destruction warfare. *R AND Corporation*. Retrieved from https://www.rand.org/content/dam/rand/pubs/ research_reports/RR1700/RR1708/RAND_RR1708.pdf.

Easterly, J. (2023/5/7). The attack on Colonial Pipeline: What we've learned & what we've done over the past two years. *Cybersecurity and Infrastructure S ecurity Agency (CISA)*. Retrieved from https://www.cisa.gov/news-events/news/ attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years#: ~:text=On%20May%207%2C%202021%2C%20a,get%20their%20kids%20to%20 school.

Eness, D. (2023/1/5). Managing cybersecurity risk in America's modern railroads. *Heartland Business Systems*. Retrieved from https://www.hbs.net/blog/managi ng-cybersecurity-risk-in-americas-modern-railroads/.

Ezrati, M. (2023/12/11). How much control does China have over rare earth ele ments? *Forbes Magazine*. Retrieved from https://www.forbes.com/sites/miltone zrati/2023/12/11/how-much-control-does-china-have-over-rare-earth-elements/

FBI News (2024/4/18). Chinese government poses 'broad and unrelenting' threat to U.S. critical infrastructure, FBI director says. *Federal Bureau of Investigation*. Retrieved from https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says#:~:text=Similarly%2C%20he%20said%2C%20during%20the,has%20also%20targeted%20critical%20infrastructure.

Ferrari, J., & Rahr, C. (2023/6/5). The Pentagon is to blame for industrial base failures. *Defense News*. Retrieved from https://www.defensenews.com/opinion/commentary/2023/06/05/the-pentagon-is-to-blame-for-industrial-base-failures/.

Fitzgerald, S. (2024/8/10). Chinese hackers active despite WH warnings, 'Feds' efforts'. *Newsmax*. Retrieved from https://www.newsmax.com/politics/china-volt-typhoon-hackers/2024/08/10/id/1176014/.

Foley, J. (2024/5/28). Multi-domain legal warfare: China's coordinated attack on international rule of law. *Lieber Institute, West Point.* Retrieved from https://lieber.westpoint.edu/multi-domain-legal-warfare-chinas-coordinated-attack-international-rule-law/.

Foreign, Commonwealth & Development Office, & Truss, E. (2022/5/10). Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion [Press release]. *GOV.UK*. Retrieved from https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion.

FORUM Staff (2024/2/14). CCP weaponizes law to gain strategic advantage. *Indo-Pacific Defense Forum*. Retrieved from https://ipdefenseforum.com/2024/02/ccp-weaponizes-law-to-gain-strategic-advantage/.

Fox News (2024/4/26). Jack Keane warns Russia, China, Iran, and North Korea are all 'collaborating'. *Fox & Friends*. Retrieved from https://www.foxnews.com/video/6351801113112.

Fox News (2024/4/26). China is 'quietly shutting down' material US needs to make weapons: Rob Spalding. Fox & Friends. Retrieved from https://www.foxnews.com/video/6361032505112.

Fox News (2022/7/25). Gen. Keane: 'We're reaching a much more dangerous mo ment' [Video]. *YouTube*. Retrieved from https://www.youtube.com/watch?v=4H C6XAAy6yI.

Foundation for Defense of Democracies (2024/7/10). Flash brief: Iran supporting and funding pro-Hamas protests in the U.S. *Foundation for Defense of Demo cracies.* Retrieved from https://www.fdd.org/analysis/2024/07/10/iran-supporting -and-funding-pro-hamas-protests-in-the-u-s/.

Funk, P. (2021/4). The operational environment (2021-2030): Great power compet ition, crisis, and conflict. *U.S. Army Training and Doctrine Command*. Retrie ved from https://community.apan.org/cfs-file/__key/telligent-evolution-componen ts-attachments/01-9016-00-00-00-16-55-27/OEAddendum_5F00_04292021.pdf.

Galdorisi, G. (2024/7). Leveraging social engineering for successful cyber operati ons: Enhancing the minds of decision-makers. *Signal Magazine,* 23-25.

Garamone, J. (2022/11/7). New strategy seeks to reinvigorate deterrence in a cha nging world. *DOD News*. Retrieved from https://www.defense.gov/News/News -Stories/Article/Article/3212005/new-strategy-seeks-to-reinvigorate-deterrence-in-a -changing-world/.

Garamone, J. (2023/3/8). DOD officials testify about homeland defense before H ouse panel. *DOD News*. Retrieved from https://www.defense.gov/News/News-S tories/Article/Article/3323297/dod-officials-testify-about-homeland-defense-before -house-panel/.

Gertz, B. (2021/7/8). U.S. Pacific intel chief: Coming Chinese attack on Taiwan could target other nations. *The Washington Times*. Retrieved from https://ww w.washingtontimes.com/news/2021/jul/8/us-pacific-intel-chief-coming-chinese-atta ck-taiwa/.

Gerecht, R. M., & Takeyh, R. (2024/2/1). The mullahs and the dragon: Tehran a nd Beijing, in a dangerous alliance. *National Review*, 76(2), 39-42.

Global News (2024/4/5). Microsoft report finds China, *North Korea 'likely' to tr y to interfere in U.S. elections*. Retrieved from https://globalnews.ca/video/104

06489/microsoft-report-finds-china-north-korea-likely-to-try-to-interfere-in-u-s-elections.

Gonzales, D., Moore, L., Pernin, C., Matonick, D., & Dreyer, P. (2000/12/1). *Assessing the value of information superiority for ground forces - Proof of concept,* P. 5. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA394791.pdf.

Gordon, C. (2024/7/29). Not prepared for major war: Commission slams US defense strategy [Remarks of Commission member Thomas Mahnken]. *Air & Space Forces*. Retrieved from https://www.airandspaceforces.com/not-prepared-major-war-commission-slams-us-defense-strategy/.

Grano, S. A., & Wu, H. Y. W. (2021/4/ 26). Xi Jinping's 2.0 version of the 'Letter to Compatriots in Taiwan'. *Taiwan Insight*. Retrieved from https://taiwaninsight.org/2021/04/26/xi-jinpings-2-0-version-of-the-letter-to-compatriots-in-taiwan/.

Griffin, J. (2023/12/5). Panel 9: Supremacy or parity? Aligning the national defense strategy for techno-competition with the PRC. Reagan National Defense Forum. *U.S. Indo-Pacific Command*. Retrieved from https://www.pacom.mil/Media/Speeches-Testimony/Article/3608020/panel-9-supremacy-or-parity-aligning-the-national-defense-strategy-for-techno-c/.

Guan, J. (2022/8/17). Why can't Beijing renounce force against Taiwan? The Interpreter. *The Lowy Institute*. Retrieved from https://www.lowyinstitute.org/the-interpreter/why-can-t-beijing-renounce-force-against-taiwan.

Hancock, A. (2024/4/4). Russia is trying to sabotage European railways, warns Prague. *Financial Times*. Retrieved from https://www.ft.com/content/f8207823-f5e1-4caf-934d-67c648f807bf.

Harman, J., Mahnken, T. G., Rudman, M., Sixkiller, M., Starzak, A., & Zakheim, R. (2024/7/29). Commission on the National Defense Strategy, pp. viii-52. *RAND Corporation*. Retrieved from https://www.rand.org/nsrd/projects/NDS-commission.html.

Headquarters, United States Marine Corps (2022). Marine Corps doctrinal publication 8: Information. *HQ USMC*.

Heritage Foundation (2024). *Index of U.S. Military Strength*, P. 364. Retrieved fr om https://www.heritage.org/military.

Jiménez, D. (2024/7/9). Iran is targeting Americans amid Gaza war protests, US intelligence chief warns. *USA Today*. Retrieved from https://eu.usatoday.com/st ory/news/investigations/2024/07/09/us-protesters-targeted-by-iran-influence-campa ign-official-warns/74342981007/.

Jockims, T. L. (2024/6/26). America's drinking water is facing attack, with links back to China, Russia and Iran. *CNBC*. Retrieved from https://www.cnbc.com /2024/06/26/americas-drinking-water-under-attack-china-russia-and-iran.html.

Kania, E. (2020/12/19). A people's war: COVID-19 response reveals China's mili tary mobilization strategy. *Institute for the Study of War*. Retrieved from http s://understandingwar.org/sites/default/files/E46%20-%20A%20People%27s%20W ar%20-%20COVID-19%20Response%20Reveals%20China%27s%20Military%20 Mobilization%20Strategy.pdf.

Kane, L. Space Systems Command targets 2026 for key resilience goals. *Space Systems Command Public Affairs*. Retrieved from https://www.ssc.spaceforce.m il/Portals/3/Race%20to%20Resilience%20SSC_1.pdf.

Kania, E. B. (2016). The PLA's latest strategic thinking on the three warfares. *C hina Brief,* 16(12), 10. Jamestown Foundation.

Kapos, S. (2024/5/5). Pro-Palestinian protesters are backed by a surprising source : Biden's biggest donors. *Politico*. Retrieved from https://www.politico.com/ne ws/2024/05/05/pro-palestinian-protests-columbia-university-funding-donors-00156 135.

Kashatus, W. C. (2018/2/26). This was a real "fake news" story – and it landed us in a war. *History News Network*. Retrieved from https://www.historynewsn etwork.org/article/this-was-a-real-fake-news-story-and-it-landed-us-i.

Katz, M. (2024/3/ 21). Indo-Pacific chief warns China set to invade Taiwan by 2027. *Newsmax*. Retrieved from https://www.newsmax.com/newsfront/admiral-j ohn-aquilino-china/2024/03/21/id/1158161/.

Kapko, M. (2024/3/11). Ransomware attacks are hitting critical infrastructure more often, FBI says. *Cybersecurity Dive*. Retrieved from https://www.cybersecuritydive.com/news/ransomware-hitting-critical-infrastructure-fbi/709814/.

Kemp, R., & Driver-Williams, C. (2015). Killing Americans and their allies: Iran's continuing war against the United States and the West. *Jerusalem Center for Public Affairs*. Retrieved from https://jcpa.org/killing-americans-allies-irans-war/.

Kendall-Taylor, A., & Fontaine, R. (2024/5/23). The axis of upheaval: How America's adversaries are uniting to overturn the global order. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/china/axis-upheaval-russia-iran-north-korea-taylor-fontaine.

Klepper, D. (2024/7/9). Iran encourages Gaza war protests in US to stoke outrage and distrust, intelligence chief says. *AP News*. Retrieved from https://apnews.com/article/gaza-war-protests-iran-foreign-influence-95e0a161119ed0e060332feda95b4e4f.

Klinger, B. (2024/4/5). China–Russia–North Korea solidarity poses risk to the U. S. and its allies. *The Heritage Foundation*. Retrieved from https://www.heritage.org/asia/report/china-russia-north-korea-solidarity-poses-risk-the-us-and-its-allies.

Koutsobinas, N. (2024/10/19). SKorea: NKorean troops in Russia readying for combat in Ukraine. *Newsmax*. Retrieved from https://www.newsmax.com/world/globaltalk/south-korea-north-korea-russia/2024/10/19/id/1184722/.

Kube, C., & Lee, C. E. (2024/5/24). Are Russia and North Korea planning an ' October surprise' that aids Trump? *NBC News*. Retrieved from https://www.nbcnews.com/news/investigations/are-russia-north-korea-planning-october-surprise-aids-trump-rcna153828.

Lagrone, S. (2021/6/23). Milley: China wants capability to take Taiwan by 2027. *USNI News*. Retrieved from https://news.usni.org/2021/06/23/milley-china-wants-capability-to-take-taiwan-by-2027-sees-no-near-term-intent-to-invade.

LaRocco, L. A. (2024/4/17). Biden admin, U.S. ports prep for cyberattacks as na tionwide infrastructure is targeted. *CNBC*. Retrieved from https://www.cnbc.co m/2024/04/17/biden-admin-ports-prep-for-cyberattacks-as-us-infrastructure-targete d.html.

Lawrence, S. S. (2024/8). Protecting and sharing critical infrastructure. SIGNAL Magazine, 9. *Armed Forces Communications and Electronics Association*.

Leaf, D. (2024/4/1). It's time to resolve the Korean War. *United States Institute of Peace*. Retrieved from https://www.usip.org/publications/2024/04/its-time-res olve-korean-war.

Lee, J.-H. (2024/1/9). Kim Jong Un labels S Korea as 'principal enemy,' boasts war readiness: The North is ready to 'devastate' the South if the latter conte mplates use of force or poses a threat, Kim says. *Radio Free Asia*. Retrieve d from https://www.rfa.org/english/news/korea/nk-sk-warning-01092024210827.h tml.

Levite, A. E., & Lee, J. (2022). Attribution and characterization of cyber attacks, p. 36. Carnegie Endowment for International Peace. https://carnegie-productio n-assets.s3.amazonaws.com/static/files/Perkovich_et_al_Cyber_Attribution_web.pd f.

Lyons, M. J. (2024/4/11). War with China: A view from early 2024. *China Lan dpower Studies Center, Strategic Studies Institute, U.S. Army War College*. R etrieved from https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Disp lay/Article/3738629/war-with-china-a-view-from-early-2024/#text7.

Martina, M., & Brunnstrom, D. (2023/2/2). CIA chief warns against underestimat ing Xi's ambitions toward Taiwan. *Reuters*. Retrieved from https://www.reuter s.com/world/cia-chief-says-chinas-xi-little-sobered-by-ukraine-war-2023-02-02/.

Martin, A. (2023/12/11). Two-day water outage in remote Irish region caused by pro-Iran hackers. *The Record*. Retrieved from https://therecord.media/water-out age-in-ireland-county-mayo.

McCarthy, C. (2024/8/27). Rising attacks on U.S. power grid. *Newsmax*. Retrieved from https://www.newsmax.com/newsfront/u-s-power-grid-attacks/2024/08/27/id/1178031/.

Menn, J. (2024/8/27). Chinese government hackers penetrate U.S. internet providers to spy. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2024/08/27/chinese-government-hackers-penetrate-us-internet-providers-spy/.

Milley, G. M. (2023). *Joint Concept for Competing*, P. 25. *U.S. Naval Institute*. Retrieved from https://s3.documentcloud.org/documents/23698400/20230213-joint-concept-for-competing-signed.pdf.

Milmo, D., Kollewe, J., Quinn, B., Taylor, J., & Ibrahim, M. (2024/7/19). Slow recovery from IT outage begins as experts warn of future risks: Fault in CrowdStrike caused airports, businesses, and healthcare services to languish in 'largest outage in history'. *The Guardian*. Retrieved from https://www.theguardian.com/australia-news/article/2024/jul/19/microsoft-windows-pcs-outage-blue-screen-of-death.

NBC News (2022/5/23). Biden says U.S. will defend Taiwan militarily if China invades [Video]. *YouTube*. Retrieved from https://www.youtube.com/watch?v=g0p4f1BSzts.

Newsmax (2024/8/19). US intelligence: Iran to blame for hack of Trump campaign. Retrieved from https://www.newsmax.com/newsfront/iran-fbi-trump-intelligence-community/2024/08/19/id/1177104/.

Newsmax (2024/8/14). Germany probing possible sabotage of water supply at military base. Retrieved from https://www.newsmax.com/world/globaltalk/germany-investigation-sabotage/2024/08/14/id/1176482/.

O'Connor, T. (2021/3/23). China, Russia, North Korea, Iran build ties as U.N. friends feud with U.S. *Newsweek*. Retrieved from https://www.newsweek.com/china-russia-north-korea-iran-build-ties-un-friends-feud-us-1578169.

Office of the Director of National Intelligence (ODNI) (2024/2/5). *Annual threat assessment of the U.S. intelligence community*, p. 18. Retrieved from https://

www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

Office of the Director of National Intelligence (2024/2/5). Annual Threat Assessment of the U.S. *Intelligence Community*. Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

Office of the Director of National Intelligence (2023/2/6). Annual threat assessment of the U.S. intelligence community, P. 10. Retrieved from https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Office of the Director of National Intelligence (2024/6). Recent cyber attacks on US infrastructure underscore vulnerability of critical US systems, November 2023–April 2024. Retrieved from https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf.

Office of the Secretary of Defense (2023/10/19). Annual report to Congress: Military and security developments involving the People's Republic of China, p. 88-96. *U.S. Department of Defense*. Retrieved from https://www.defense.gov/Portals/1/Documents/pubs/2023-Report-on-the-Military-and-Security-Developments-Involving-the-Peoples-Republic-of-China-CMPR.pdf.

Office of the Director of National Intelligence (2023/2/6). *Annual threat assessment of the U.S. intelligence community*, pp. 10-16. Retrieved from https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Office of the Secretary of Defense (2020/8/21). *Annual report to Congress: Military and security developments involving the People's Republic of China*, P. 83.

Office of Research, Development and Technology (2020/6). *Cyber Security Risk Management for Connected Railroads. U.S. Department of Transportation Federal Railroad Administration*, Washington D.C., P. 138. https://railroads.dot.gov/sites/fra.dot.gov/files/2020-06/Cyber%20Security%20Risk%20Management-A_0.pdf.

O'Hanlon, M. E., & Rocha, A. (2024/6/20). Strengthening America's defense industrial base. *Brookings Institution*. Retrieved from https://www.brookings.edu/articles/strengthening-americas-defense-industrial-base/.

Paganini, P. (2024/4/16). Russia is trying to sabotage European railways, Czech minister said. *Security Affairs*. Retrieved from https://securityaffairs.com/161899/cyber-warfare-2/russia-sabotage-european-railways-czech.html.

Petrosyan, A. (2024/4/16). Cybercrime and the financial industry in the United States - Statistics & Facts. *Statista*. Retrieved from https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/.

Pierce, J. (2024/7/29). AT&T data breach: Even most secure networks vulnerable. *Newsmax*. Retrieved from https://www.newsmax.com/jodipierce/at-and-t-data-breach/2024/07/29/id/1174368/.

Pottinger, M. (2024/6/16). The case for deterrence. *The Wire*. Retrieved from https://www.thewirechina.com/2024/06/16/the-case-for-deterrence-china-taiwan-xi-jinping/.

Public Law 107-228, 107th Congress (2002/9/30). Foreign relations authorization act, fiscal year 2003, *Section 1206*. Retrieved from https://www.congress.gov/107/plaws/publ228/PLAW-107publ228.pdf.

Public Affairs, U.S. Department of Justice (2024/7/25). North Korean government hacker charged for involvement in ransomware attacks targeting U.S. hospitals and health care providers. *U.S. Department of Justice*. Retrieved from https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

Qiao, L., & Wang, X. (1999). Unrestricted warfare. *PLA Literature and Arts Publishing*.

Reuters (2023/12/31). China's Xi says 'reunification' with Taiwan is inevitable. *Reuters*. Retrieved from https://www.reuters.com/world/asia-pacific/china-calls-taiwan-president-frontrunner-destroyer-peace-2023-12-31/.

Robertson, N. (2024/5/30). They've grown back: How Russia surprised the West and rebuilt its force. *Defense News*, 13-15. Retrieved from https://www.defens

enews.com/global/europe/2024/05/21/theyve-grown-back-how-russia-surprised-the-west-and-rebuilt-its-force/.

Robertson, N. (2024/5). Lost in translation: How the year 2027 changed Washington's debate over China. *Defense News*, 36(5), 16-18.

Rogan, T. (2024/4/23). US unprepared as China boosts preparations for Taiwan war. *The Washington Examiner*, 30(14), 20-23.

Rogan, T. (2024/7/9). Restoring America's industrial base. *Washington Examiner*, 30(24), 21-22.

Rogan, T. (2024/8/21). Examining China's multipronged threat. *Washington Examiner*, 30(30), P. 55. Retrieved from https://www.washingtonexaminer.com/opinion/3129318/examining-chinas-multipronged-threat/.

Runde, D. F., Murphy, E. L., & Bryja, T. (2024/8/18). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. *Indian Strategic Studies*. Retrieved from https://www.strategicstudyindia.com/2024/08/safeguarding-subsea-cables-protecting.html.

Santoro, D. (2023/10/5). In a crisis, China's objective is to gain the upper hand. *Asia Times*. Retrieved from https://asiatimes.com/2023/10/in-a-crisis-chinas-objective-is-to-gain-the-upper-hand/#:~:text=This%20is%20the%20crux%20of,prevented%20through%20prediction%20and%20monitoring.%E2%80%9D.

Saxena, A. (2024/5/27). 75 years of China-Russia relations: Indeed a 'no limits' partnership. *Institute for Security and Development Policy*. Retrieved from https://www.isdp.eu/75-years-of-china-russia-relations-indeed-a-no-limits-partnership/

Seffers, G. I. (2024/8). What does the future hold for Jack Voltaic cyber exercise? SIGNAL Magazine, 13. *Armed Forces Communications and Electronics Association*.

Security Staff (2024/7/5). US suffered cyberattacks from 168 threat actors in 2023. *Security Magazine*. Retrieved from https://www.securitymagazine.com/articles/100346-us-suffered-cyberattacks-from-168-threat-actors-in-2023.

Shelbourne, M. (2021/3/ 9). Davidson: China could try to take control of Taiwan in ‘next six years’. *USNI News*. Retrieved from https://news.usni.org/2021/03/09/davidson-china-could-try-to-take-control-of-taiwan-in-next-six-years.

Shepardson, D. (2024/7/23). AT&T February wireless outage blocked more than 92 million calls, agency says. *Reuters*. Retrieved from https://www.reuters.com/business/media-telecom/att-wireless-outage-february-blocked-more-than-92-million-calls-agency-says-2024-07-22/.

Shalal, A., & Flowers, B. (2024/5/4). Explainer: How US campus protests over Gaza differ from Vietnam war era. *Reuters*. Retrieved from https://www.reuters.com/world/us/how-us-campus-protests-over-gaza-differ-vietnam-war-era-2024-05-04/.

Statista (2023). Industry sectors most targeted by ransomware attacks in the United States in 2023. *Statista*. Retrieved from https://www.statista.com/statistics/1323599/us-most-targeted-industries-by-ransomware-attacks/.

Swanson, M. (2024/8/27). Chinese hackers take aim at U.S. internet providers. Retrieved from https://www.newsmax.com/newsfront/chinese-hackers-attacks/2024/08/27/id/1178047/.

Tadjdeh, Y. (2021/7/7). Defense Department further accelerating 5G development. *National Defense Magazine*. Retrieved from https://www.nationaldefensemagazine.org/articles/2021/1/7/defense-department-further-accelerating-5g-development#:~:text=%E2%80%9CDue%20to%20information%20sharing%20requirements,was%20related%20in%20September%20%E2%80%94%20said.

Tang, D., & Tucker, E. (2024/7/31). FBI director: Chinese hackers determined to ‘wreak havoc.’ *Newsmax*. Retrieved from https://www.newsmax.com/world/globaltalk/fbi-director-wray/2024/01/31/id/1151671/.

The Center for National Interest. China, Russia, Iran, North Korea—the CRANKs. Crank Call, a monthly compendium of cooperation among China, Russia, Iran and North Korea. Retrieved from https://cftni.org/publications/china-russia-iran-north-korea-the-cranks/

The Economist (2023/3/18). How China, Russia and Iran are forging closer ties. *The Economist*. Retrieved from https://www.economist.com/finance-and-economics/2024/03/18/how-china-russia-and-iran-are-forging-closer-ties.

The Guardian (2021/10/6). China could mount full-scale invasion by 2025, Taiwan Defence Minister says. *The Guardian*. Retrieved from https://www.theguardian.com/world/2021/oct/06/biden-says-he-and-chinas-xi-have-agreed-to-abide-by-taiwan-agreement.

The Heritage Foundation (2024/1/24). The U.S. defense industrial base: Past strength, current challenges, and needed change. Retrieved from https://www.heritage.org/node/25156162/print-display#TheUSDefenseIndustrialBasePastStrengthCurrentChallengesandNeededChange_ednref20.

The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (2024/4/16). *The CCP's role in the fentanyl crisis*. Retrieved from https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/The%20CCP%27s%20Role%20in%20the%20Fentanyl%20Crisis%204.16.24%20%281%29.pdf.

The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (2024/4/16). *Investigation findings: The CCP's role in the fentanyl crisis*. Retrieved from https://selectcommitteeontheccp.house.gov/media/investigations/investigation-findings-ccps-role-fentanyl-crisis.

The Heritage Foundation (2024). *Index of U.S. military strength*, p. 275. Retrieved from https://www.heritage.org/military.

Times of India (2024/3/18). United States is at war with us, 'Kremlin says after Putin wins record 5th term. *Times of India*. Retrieved from https://timesofindia.indiatimes.com/world/rest-of-world/united-states-is-at-war-with-us-kremlin-says-after-putin-wins-record-5th-term/articleshow/108595228.cms.

Transportation Security Administration (2022/10/24). Security Directive 1580/82-2022-01: Rail cybersecurity mitigations and testing. Retrieved from https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf.

Transportation Security Administration (2021/12/31). Security Directive 1580-21-01: Enhancing rail cyber security. Retrieved from https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf.

Troxell, J. (1997). Force planning in an era of uncertainty: Two MRCs as a force sizing framework (p. vii, emphasis added). *U.S. Army War College Press.* Retrieved from https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1179&context=monographs.

United States Department of State, Bureau of Arms Control (1953). Text of the Korean War Armistice Agreement. *U.S. Department of State*. Retrieved from https://2001-2009.state.gov/t/ac/rls/or/2004/31006.htm#:~:text=This%20Armistice%20Agreement%20shall%20apply,of%20any%20kind%20of%20Korea.

United States Marine Corps. Marine Corps doctrinal publication (MCDP) 8: Information, pp. 1-25. *United States Government Publishing Office*.

U.S. Army War College (2023/12/18). *Strategic cyberspace operations primer*, P. 165.

Vergun, D. (2023/4/26). Official details space-based threats and U.S. countermeasures. *DOD News*. Retrieved from https://www.defense.gov/News/News-Stories/Article/Article/3375577/official-details-space-based-threats-and-us-countermeasures/.

Volz, D., Fitzgerald, D., & Champelli, P. (2024/5/19). U.S. fears undersea cables are vulnerable to espionage from Chinese repair ships. *The Wall Street Journal*.

Vu, K. (2021/7/30). Why China and North Korea decided to renew a 60-year-old treaty. *The Lowy Institute*. Retrieved from https://www.lowyinstitute.org/the-interpreter/why-china-north-korea-decided-renew-60-year-old-treaty.

Wells, N. (2024/8/12). Intel officials say Iran top threat to US election. *Newsmax*. Retrieved from https://www.newsmax.com/newsfront/intelligence-iran-hackers/2024/08/12/id/1176234/.

Welker, K., Kube, C., Lee, C. E., & Mitchell, A. (2023/12/20). Xi warned Biden during summit that Beijing will reunify Taiwan with China. *NBC News*. R

etrieved from https://www.nbcnews.com/news/china/xi-warned-biden-summit-beijing-will-reunify-taiwan-china-rcna130087.

Welch, C. (2024/6/27). China ‘actively targeting US industrial base,’ warns CYBERCOM chief. *Breaking Defense*. Retrieved from https://breakingdefense.com/2024/06/china-actively-targeting-us-industrial-base-warns-cybercom-chief/.

Xinhua (2022/8/10). Full text: The Taiwan question and China's reunification in the new era. *Xinhua*. Retrieved from https://english.news.cn/20220810/df9d3b8702154b34bbf1d451b99bf64a/c.html.