

AIR WAR COLLEGE
AIR UNIVERSITY
COUNTERING UNRESTRICTED WARFARE
PREPARING TO COMPETE AGAINST CHINA'S ACTUAL STRATEGY

by

Victor Norris, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Dawn Murphy

27 March 2020

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.



Biography

Lieutenant Colonel Victor “Vic” Norris is a student at the Air War College. Previously, Lt Col Norris served as the Corporate Branch Chief in the “Engine Room,” where he was responsible for defending the Air Force Program Objective Memorandum to the Combatant Commands, sister services, Defense Agencies, and Congress. Lt Col Norris is a core cyber effects operator and has performed operational tours in support of homeland defense missions.

Lt Col Norris entered the United States Air Force after graduating from Azusa Pacific University in 2000 and commissioned through the University of Southern California. He has served in various positions at the squadron, Number Air Force, Major Command, Combatant Command, and Air Staff, levels including commanding the 552 Air Control Networks Squadron at Tinker Air Force Base. Lt Col Norris has deployed in support of Operation IRAQI FREEDOM, Operation ENDURING FREEDOM, Operation INHERENT RESOLVE, Operation FREEDOM SENTINEL, along with multiple shorter deployments in support of special operations missions.

Abstract

What is the future of the United States' relations with China? Is it competition, cooperation, or conflict? The People's Republic of China's (PRC) Three Warfares and Informatization Strategy assures the Chinese Communist Party (CCP) social, territorial, and economic national interests. The PRC seeks to broaden its influence on a global scale, but only to protect its national interests inside what they perceive as their territory. The U.S. national security apparatus does not appear to understand how to compete with China across the diplomatic, informational, military, and economic (DIME) spectrum. China has mastered the ability to control information inside its virtual borders. Simultaneously, Chinese programs are infiltrating economic and social spheres around the globe to create broader influence. An inadequately organized Department of Defense (DoD) and U.S. national security apparatus, writ large, are ill-prepared to compete with Chinese influence. The most likely scenario driving conflict between the United States and China involves Taiwan. Any U.S. attempt to blunt Chinese aggression toward Taiwan will fail without competing for influence in advance of hostilities. Competition with China requires decoding their information control mechanisms and preparing counter influence campaigns. This paper will identify the core components of China's influence strategy and detail how it threatens the United States. It will also describe several recommendations for how to compete in the cognitive domain utilizing the information instrument of power (IOP) to create multiple dilemmas for China and deter an invasion of Taiwan.

Introduction

P.W. Singer and August Cole's novel *Ghost Fleet* is a work of techno-fiction. This novel casts a future world where a risen and reformed China has stolen or infiltrated all of America's technology.¹ Systemically erasing America's advantages across the air, land, sea, space, and cyber domains, China neutered America's ability to defend the homeland from an invasion. The dystopian world Singer and Cole build naturally creates anxiety within America's National Security apparatus. However, Singer's painting of China as an expansionist power is wholly fictional. China's strategy identifies the importance of ensuring their social, territorial, and economic national interests. Brigadier General Robert Spalding described China's strategy succinctly in his book *Stealth War* when he said, "For the past forty years, the Chinese Communist Party (CCP) has been playing a beautiful game. It is sophisticated yet simple. It is a competition to gain control and influence across the planet—and to achieve that outcome without resorting to military engagement."² There is a significant "ah but" to General Spalding's influence concept, and that is regarding China's territorial integrity, specifically concerning Taiwan.

In 2019, the PRC's State Council of Information Office published a document entitled "China's National Defense in the New Era," where the language regarding Taiwan was highly inflammatory.

"China adheres to the principles of "peaceful reunification", and "one country, two systems", promotes peaceful development of cross-strait relations, and advances peaceful reunification of the country. Meanwhile, China resolutely opposes any attempts or actions to split the country and any foreign interference to this end. China must be and will be reunited. China has the firm resolve and the ability to safeguard national sovereignty and territorial integrity, and will never allow the secession of any part of its territory by anyone, any organization or any political party by any means at any time."³

The document continues by saying the People's Liberation Army (PLA) "will resolutely defeat anyone attempting to separate Taiwan from China" and that the CCP "resolutely opposes the wrong practices and provocative activities of the U.S. side regarding arms sales to Taiwan."⁴

China is competing for global influence with the United States because of perceived U.S. infringement in the Taiwan Strait and the broader Indo-Pacific region. The United States must compete with the information IOP and challenge Chinese influence. America must find opportunities to create multiple dilemmas and deescalate potential conflict by targeting Chinese information control vulnerabilities.

According to Rybeck, Cornwell, and Sagan's *War on the Rocks* article: "Chinese leaders are exploiting converged data, communications, machines, and humans...uniting its government, military, and society at large behind a comprehensive, coordinated strategy to enter what President Xi Jinping sees as a game-changing new era. Chinese Leaders call this informatization."⁵ Over the last few years, Chinese literature and public documents have discussed a broad, yet ambiguous, informatization strategy. The strategy's social, military, and economic impacts assure China's national interests with the added benefit of China's global leadership in 5th Generation Cellular (5G). China's core national interests are: first, the protection and the stability of the Chinese Communist Party. Second, Chinese sovereignty and national reunification. Third, build and sustain China's economic and social interests.⁶

In 1999, two senior PLA colonels penned *Unrestricted Warfare*, as a roadmap for future Chinese warfare. The following excerpt is a chilling summary of their manifesto.

"War in the age of technological integration and globalization has eliminated the right of weapons to label war and, with regard to the new starting point, has realigned the relationship of weapons to war, while the appearance of weapons of new concepts, and particularly new concepts of weapons, has gradually blurred the face of war. Does a single "hacker" attack count as a hostile act or not? Can using financial instruments to destroy a country's economy be seen as a battle? Did CNN's

broadcast of an exposed corpse of a U.S. soldier in the streets of Mogadishu shake the determination of the Americans to act as the world's policeman, thereby altering the world's strategic situation? And should an assessment of wartime actions look at the means or the results? Obviously, proceeding with the traditional definition of war in mind, there is no longer any way to answer the above questions. When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war: Warfare which transcends all boundaries and limits, in short: unrestricted warfare.”

7

The first section of this paper will begin by describing China's broad informatization strategy. The second will describe China's internal information control program, including the human resources and technology utilized. Section three will address China's external propaganda and influence campaigns. And section four will put it all together, painting a composite picture of the problem. This paper concludes with recommendations for competing with China's influence campaign utilizing a whole of government approach to monitor, assess, and target China's weaknesses in the cognitive domain.

1. Informatization Strategy

What is China's Informatization strategy? Informatization requires and understanding of 5th Generation Cellular (5G), and China's historical reliance on active defense. Roger Cliff, in his book *China's Military Power*, provides a complete military definition when he calls Informatization:

“...environments characterized by intensive use of the electromagnetic spectrum both for surveillance and reconnaissance and for communications, along with extensive electronic jamming and deception measures, cyber warfare, and other conditions that could affect the smooth collection, processing, and dissemination of battlefield information.”⁸

Succinctly stated, informatization (also called informationized warfare) is integrating, protecting, and controlling information across disparate systems in multiple domains (Air, Land, Sea, Cyber, Space, *Psychological*) and presenting decision quality information to Chinese leadership while denying their adversary the ability to do the same. Informatization weaponizes information; it enables the PRC to compete in a battle of cognition inside their borders as well as the battle for influence on a global scale. Technology, and 5G specifically, is the backbone behind the PRC's internal information control and external influence operations.

5G, or the “internet of things,” allows everything from cellular phones and televisions to dishwashers and washing machines to communicate utilizing artificial intelligence and broadband data to enable integration. 5G technology can broadly apply to the social, economic, even military aspects of Informatization.⁹ China believes success in future conflict will rely on successful IT integration of all capabilities. Chinese investment in homegrown automation and artificial intelligence are a source of national pride and serve as the platform for China's leadership in 5G cellular.¹⁰ In a September 2018 *War on the Rocks* article, authors Rybeck, Cornwell, and Sagan argue that through Informatization, “China is attempting to overtake the

West as a global leader in technology innovation.”¹¹ 5G under PRC leadership of the Chinese IT industry expanding globally at a rapid pace and the United States is attempting to catch up. General Spalding in *Stealth War* described how a PRC built 5G network could “weaponize the technology within entire cities—or countries...and hold that city or state at its mercy.”¹² China’s drive to lead in 5G implementation aligns with their core national interests as well as their traditional active defense strategy.

China’s Informatization Strategy fuses all of the instruments of power in an active defense manner. In 1999’s *Unrestricted Warfare*, two senior PLA colonels described the overarching goals of China’s new strategy.

“The new principles of war are no longer ‘using armed forces to compel the enemy to submit to one’s will,’ but rather are ‘using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one’s interests.”¹³

The PRC has a long history of employing simultaneous offensive and defensive operations intended to weaken, paralyze, or confuse, and they named this strategy active defense.¹⁴ The military Informatization component, utilizing an active defense strategy, assumes simultaneous offensive and defensive operations are needed to improve “combat capabilities under informationized conditions and safeguard the sovereignty, security, and development interests of China.”¹⁵

Informatization and Informationized warfare are often inappropriately equated with Cyberspace Operations. Technologists, engineers, and even hackers are essential components of information instrument of power. However, an understanding of the laws of physics, or computer languages are useless in determining the socioeconomic impacts of a deadly virus or the election of a pro-democracy regime in Hong Kong. Success in the cognitive domain requires

anthropologists, economists, diplomats, and more to predict impacts accurately. According to the author of *Cyber Dragon*, Dean Cheng, the Chinese view information dominance as exploiting information with greater precision and speed than their adversary. More importantly, Informationized warfare includes “political warfare, which shapes and influences friendly, adversary, and third-party views and assessments.”¹⁶ Step one of safeguarding China’s core national interests is internal information control.

2. Internal Information Control

The stability of the PRC regime is China’s #1 national interest, and it relies on strategic messaging, technology, and the party’s military arms (People’s Armed Police and PLA) to control information.¹⁷ The PRC relies on a broad surveillance state, linked to a social credit system to rapidly update narratives, assess compliance by the entire population, and then discipline deviant behavior. According to General Spalding, the CCP is building a social credit system to turn every citizen (at home or abroad) into a spy.¹⁸ The future of the social credit system will enable a broad surveillance state. The system will fuse and decipher a dizzying array of social data, ranging from social data from cameras and bicycle/vehicle tracking to party alignment data from political commissars embedded into private industry. The Center for Strategic and Budgetary Assessments (CSBA) authors Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara in “Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare,” offer a glimpse into the PRC’s “political warfare system” intended to “suppress dissent, humiliate opponents and doubters, and instill unquestioning loyalty to the Party.”¹⁹ This description of the social credit system aligns with General Spalding’s view in providing an effective mechanism for ensuring the party’s stability. However,

the system would be ineffective if not for the CCP's delicate management of strategic messaging that serves as the baseline for the entire system.

The PRC utilizes the political component of its informatization strategy to control information through strategic messaging that leverages their “faithfully propagandistic media” and by censoring damaging information.²⁰ From the beginning of the CCP, the party has tightly controlled the media. President Xi Jinping has further consolidated power to manage strategic messaging by actively managing party leaders and broad diplomatic, information, military, and economic (DIME) experts through the legacy “Central Leading Groups.”²¹ Moreover, in the name of informatization, President Xi presides over Xinhua News Agency and China Central Television while allowing the party to serve as the “ultimate arbiter of media content.”²² On October 1, 2019, the PLA demonstrated the effectiveness of its strategic narrative with an immense parade of PLA capabilities celebrating the 70th anniversary of the PRC. In the lead up to the parade, PLA Major General Cai Zhijun summarized the strategic message of the parade. General Zhijun said, “The message is to uphold the absolute command of the party and to show unwavering loyalty and willingness to defend the leadership.”²³ According to Los Angeles Times Reporter Yaqia Wang, “Controlling information has always been central to Chinese Communist Party rule, and as the 70th anniversary of that rule approaches on Oct. 1, the propaganda machine is in overdrive.”²⁴ The CCP's technological advances in monitoring compliance have greatly enhanced their vice-like grip of strategic messaging.

“Strategic messages are easily undermined when the public receives effective and available counter-arguments.”²⁵ The PRC's investment in artificial intelligence and information technology has automated its ability to “maintain social harmony.”²⁶ The CCP's technical mechanisms actively promote information that is favorable to the regime, while obliterating

information that is deemed contrary to the stability of the party. According to multiple sources, the PRC employs censors and influencers to manage public opinion via social media while at the same time, blocks external information using the Great Cyber Wall.²⁷ In 2013, China employed two million public opinion analysts with ten million student volunteers ensuring “the Party’s ideas always become the strongest voice in cyberspace.”²⁸ “[T]he government is using China’s Xinjiang province as a surveillance laboratory to experiment with ‘social credit’ that will allow the government to monitor every aspect of people’s lives.”²⁹ The CCP views the social credit system as a “multidimensional, all-weather and foolproof prevention and control grid.”³⁰ On June 5, 1989, the CCP’s armed forces drove tanks over students protesting the regime in Beijing’s Tiananmen Square, and images of the thousands murdered by the CCP spread around the globe. According to General Spalding in *Stealth War*, most Chinese citizens have no recollection of the disaster. Utilizing long-standing social pressure, the CCP has effectively eradicated the incident from the collective Chinese memory. However, globalism and the intrusion of information technology threatened to reintroduce documentation and discourse of the massacre back into the Chinese culture. In response, any photographs or literature of the incident are “actively hunted down by sophisticated algorithm-powered censors and thousands of social media monitors.”³¹ President Xi Jinping recently professed the social credit system, internet monitoring, and other associated technology will enable “mega national security.” Furthermore, these systems brand Chinese citizens who challenge social harmony as deviants ready for punishment.³²

The PLA and the People Armed Police (PAP) are the CCP; they are the armed wings of the CCP responsible for enforcing party policies. The Mission of the PLA and the PAP, as described by the 2019 *Chinese Defense in the New Era*, states “As mandated by law, China’s armed forces

participate in operations for maintaining *social order*, prevent and combat violence and terrorism, safeguard political security and *social stability*, and secure the public's right to live and work in peace.”³³ The PRC's 70th-anniversary festivities provide a recent example of strategic messaging and censorship. The PAP utilizes offensive informatization tools to promote domestic stability. The PLA and the PAP retain a significant role in quelling uprisings and ensuring domestic stability. Performing this mission requires significant political training and highly trained political commissars who are responsible for advising party goals at all echelons of command. Indoctrination in the PLA can result in up to 30% of soldiers training being party-focused political training.³⁴ With the PAP and the PLA enforcing internal compliance, the CCP can focus on managing external influences.

3. External Influence Operations

China views influence as the most critical commodity in securing its national objectives. Over the last thirty years, the CCP has employed concepts from Sun Tzu's *The Art of War*, and *Unrestricted Warfare* to develop economic, social, and political influence campaigns to compete globally below the level of armed combat.³⁵ China's Central Military Committee, in 2005, approved official guidelines for “public opinion warfare, psychological warfare, and legal warfare” to compete for influence utilizing the “Three Warfares” concept.³⁶ According to General Spalding, “China's strategic culture is intertwined with Confucian ideas of hierarchy, harmony, and responsibility...Economic relationships, financial competition, and the use of information help create influence. And influence is the next best thing to actual power.”³⁷ Through the United Front, Thousand Talents program, Confucius Institutes, media control, and other party influence mechanism, the CCP is manipulating influence in the economic, political, and social sectors on a massive scale.³⁸ Perhaps this quote from *Unrestricted Warfare* best

explains CCP tactics: “We [the PLA] are not going to use our armed forces at all. Instead, we’ll use our cyber warriors as destabilizing agents to undermine rival economies and political systems.”³⁹

The United Front is the principal program for executing the command and control of China’s global influence campaign. Predating the PRC, the United Front is not a young organization and has adapted several times over its long history.⁴⁰ Mahnken et al. state the United Front’s purpose is to befriend, entice, influence, monitor, infiltrate, and, most importantly, co-opt various elements of Chinese society that do not belong to the Party.”⁴¹ Western influence near China’s borders and especially in Hong Kong and Taiwan has inspired United Front to focus on the requirement of “winning the people’s hearts” to expand China’s influence and protect its national objectives.⁴² In this light, the United Front prioritizes influencing Chinese nationals around the globe to “love the motherland,” while actively engaging in opportunities to employ offensive economic, social, and political warfare to “oppose separatism” and engender “the great rejuvenation of the Chinese nation.”⁴³ Cultivating talent in scientific and economic sectors via Chinese students studying abroad is a priority effort of the CCP influence campaign.

Publicly the United Front is tasked with creating domestic stability by finding “political work after the students return home.”⁴⁴ However, CCP literature calls for the United Front to study life situations for Chinese students studying abroad. Then the United Front will coerce students to “undertake cooperative investments, academic exchanges, cooperative research, technical development, consulting services, and many other activities to serve the nation.”⁴⁵ The CCP utilizes organizations like the United Front and the Confucius Institutes at major universities to “foster pro-Chinese worldviews” and control Chinese students. According to multiple sources, “there are now more than 100 Confucius Institutes in the United States and more than 500 in

universities globally.”⁴⁶ The most obvious return on the CCP’s investment in the United Front has been the number of Chinese students who return to China after completing their studies. In 2002, according to the U.S. Department of Energy, 92% of U.S. educated Chinese Ph.D. STEM graduates remained in the United States.⁴⁷ PRC figures published in 2011 state that approximately 340 thousand Chinese students studied abroad, with only 55% returning to China, but only five years later (2016), more than 62% returned home.⁴⁸ According to Arthur Herman, in his article “America’s STEM Crisis threatens our National Security,” “Today China is the world leader in number of STEM graduates,” producing 4.7 million graduates in 2016.⁴⁹ The United Front has proven very successful at retaining Chinese talent, but achieving President Xi Jinping’s vision of making China into a “science and technology superpower” under his “Made in China 2025” strategy requires another step: the Thousand Talents plan (TTP).⁵⁰

The CCP’s plan to build economic influence relies heavily on the Thousand Talents plan to develop a highly skilled and highly educated cadre called “*rencai*.” The Thousand Talents plan, also known as China’s “*National Medium- and Long-term Talent Development Plan*,” is the first CCP comprehensive human resources plan. The benign published national plan focuses on the strategic importance of developing and retaining Chinese talent.⁵¹ The U.S. government has a significantly different view of the plan. According to the Permanent Subcommittee on Investigation Report to the U.S. Senate in November 2019, the Thousand Talents program conducts espionage by incentivizing Americans, regardless of ethnicity, in research and development arenas for illegal information exchanges. “China unfairly uses the American research and expertise it obtains for its own economic and military gain.”⁵² The plan, launched in 2008, was designed to recruit 2000 overseas experts by 2018. However, some reports indicate the number of “higher-end” experts alone approached 7,000 by 2017.⁵³ An example case of the

Thousand Talents program is Harvard University's Dean of Chemistry and Bio-Chemistry Department, Dr. Charles Lieber. Multiple sources indicate he was recruited as a "Strategic Scientist" under the Thousand Talents program and worked with the Wuhan University of Technology. Furthermore, a New York Times article from November 2019 indicates 200 plus FBI cases investigating the depth of the TTP penetration into U.S. technological academia.⁵⁴ A significant portion of the "higher-end" talent targeted by the United Front and the Thousand Talents plan focuses on cyberspace and artificial intelligence capabilities.

Cyberspace capabilities and artificial intelligence have become the lynchpin of the CCP's Informatization strategy. Extensive analysis of Chinese writings conducted by a panel of Chinese experts orchestrated by a 2019 United States Air Force Air Command and Staff College student indicates the importance of AI to the CCP. They view "the race for AI in the same lens as the Apollo program" as a program to "leapfrog the United States in technological development."⁵⁵ According to the expert panel, "Chinese AI would serve three distinct purposes: gain economic competitive advantage, gain geo-political advantage, and maintain social harmony."⁵⁶ The CCP development of a National Data Strategy aligns its AI strategy with the protection of its core national interests.⁵⁷ The CCP uses AI to hunt down information it deems threatening (e.g., Tiananmen Square images) and then uses cyberspace capabilities to remove the information. The CCP is actively using these same capabilities to influence global public opinion.

The CCP expertly wields the information instrument of power by influencing international public opinion through government-controlled media (e.g., Chinese Global Television Network), the United Front, and Confucius institutes. In the fall of 2019, an executive from the National Basketball Association's (NBA) Houston Rockets tweeted "Fight for Freedom, Stand with Kong."⁵⁸ A dramatic example of the CCP tight control of their narrative pushed the NBA to fire

Morey, blocked all Rockets merchandise inside China and banned all Rockets games from Chinese television severely impacting the NBA economy.⁵⁹ The CCP recently used diplomatic power to cancel the credentials of journalists covering the Coronavirus outbreak as well as researching President Xi Jinping's family ties. The CCP media claimed the reporters were expelled for "racially discriminatory language and maliciously slandering and attacking China."⁶⁰ While state-controlled media shapes public opinion overtly, the CCP has covertly undermined the credibility of western media by planting Chinese propaganda in periodicals ranging from the *Wall Street Journal* to the *Des Moines Register*. Furthermore, "private" Chinese companies' investments in western media have further destroyed any media credibility.⁶¹ In addition to manipulating the media, the CCP utilizes Confucius institutes to influence western scholars to align with Chinese interests. For example, scuttling the Dalai Lama's scheduled visit to North Carolina State University in 2009. The Confucius Institute's director pressured the school stating the visit could undermine "some of the strong relationships we [NC State] were developing with China." Ultimately the school canceled the visit due to the pressure.⁶² The CCP's manipulation of media has not gone unnoticed on the international stage. Recently, the State Department identified CCP owned Chinese news outlets as "foreign missions akin to embassies."⁶³ In the competition for influence, the CCP clearly wields the diplomatic, informational, and economic IOPs with greater dexterity than the United States, but what does it all mean?

4. Putting it all together

The CCP is dramatically expanding its influence by weaponizing information. Through informatization, internal information control, and external information manipulation, the CCP is executing influence operations across the DIME. President Xi Jinping and the CCP ensure the

Party controls “all aspects of life...the party, government, military, society, education,” inside China but also extending influence on a global scale.⁶⁴ China’s influence strategy is a social (united front), military (informatization), and economic (Thousand Talents program) strategy that focuses on competing below the level of armed conflict. China aims to garner the necessary influence to protect its three core national interests. Inwardly focused influence levers eliminate the Tiananmen Square tragedy and continue to hide pro-democracy elections in Hong Kong. Outward targeted capabilities twist a united, independent Taiwanese narrative and present it as disinformation and actively minimize Muslim re-acculturation camps, unfair labor practices, human rights violations, and more to the rest of the world. With their eyes laser-focused on Taiwan reunification, Chinese influence tools enable competition while remaining below the level of armed conflict.

China’s National Defense in a New Era white paper regards the Taiwan separatists’ threat as “the gravest immediate threat to peace and stability.”⁶⁵ Recently a PLA officer stated, “[t]he Taiwan issue involves the territorial integrity and national sovereignty of China. It is our [China’s] vital security interest to prevent Taiwan from drifting toward independence.”⁶⁶ Chinese sovereignty and reunification with Taiwan are directly linked. The PRC relies upon offensive and defensive measures of the military component of its Informatization strategy when dealing with the Taiwan dilemma. The PRC has made significant preparations based upon an assumption of conflict with the United States over Taiwan.⁶⁷

If the CCP’s global influence campaign fails and the United States intervenes over Taiwan, the South China Sea, or elsewhere, American weapons will face perhaps an insurmountable challenge. China’s Thousand Talents Program, informatization strategy, and intellectual property theft have provided a springboard to build an additional defensive layer with the premier anti-

access, area-denial (A2/AD) system in the world.⁶⁸ According to John Wilson Lewis and Xue Litai in their book *Imagined Enemies*, in 1990, PRC strategists analyzed all threats to Chinese sovereignty, including U.S. intervention on behalf of Taiwan. Their analysis demonstrated China's air defenses vulnerability to "lightning or surgical strike" against Chinese targets in "the nation's heartland."⁶⁹ The study illuminated Chinese deficiencies in fighting under informationized conditions and "prompted an accelerated buildup" to close the gap.⁷⁰ In response, China has rapidly modernized its military and invested heavily in space and cyberspace capabilities to counter America's military might.⁷¹ If the United Front and the Thousand Talents plan were not able to co-opt the needed technology back to China, then perhaps Cyber would be a method for stealing it. The former top intelligence officer in the United States Air Force, Lieutenant General VeraLinn Jamison alluded to China's intellectual property theft when she said: "Potential rivals have also conducted cyberattacks against the Defense Department as well as defense contractor databases and social media networks — and use these methods to counter our advances."⁷² Intellectual property theft has identified opportunities for China to implant cyber munitions inside American technology, eliminating any U.S. technological advantage.⁷³

The PLA's development of Air, Land, Sea, Space, Cyber, and Psychological technology is useless without the ability to integrate these capabilities. PLA leadership has openly stated the strategic necessity of integrating these various capabilities into a system of systems. The information technology byproduct of creating this system of systems is 5G cellular. China's leadership in 5G cellular technologies has come under scrutiny out of concerns the technology will direct global information into "China's military, intelligence, and internal security apparatus."⁷⁴ Retired Army Brigadier General John Adams stated, "Our almost complete dependence on China...for telecommunications equipment presents potentially catastrophic

battlefield vulnerabilities.”⁷⁵ 5G indeed provides the CCP with a mechanism for extending its penetrating influence around the globe. Often missed is the multitude of access points that 5G opens up to external competition. Imagine, broadcasting Hong Kong’s election of a democratic leaning leadership into Tibet over 5G, or pushing China’s treatment of the Muslim Uyghur in Xinjiang to Indonesia Muslims during a referendum on China’s trade imbalance and maritime territory concerns. It is now time for the United States to counter China’s broad influence campaign by utilizing China’s unrestricted warfare tactics against them.



Recommendations

Unrestricted Warfare mentions 24 different methods of warfare that can be combined to form a completely new method of warfare. These methods range across all of the instruments of power and include:

“Atomic warfare, Diplomatic warfare, Financial warfare, Conventional warfare, Network warfare, Trade warfare, Bio-chemical warfare, Intelligence warfare, Resources warfare, Ecological warfare, Psychological warfare, Economic aid warfare, Space warfare, Tactical warfare, Regulatory warfare, Electronic warfare, Smuggling warfare, Sanction warfare, Guerrilla warfare, Drug warfare, Media warfare, Terrorist warfare, Virtual warfare (deterrence) Ideological warfare.”⁷⁶

Successful competition with China requires creating multiple dilemmas across all domains, including the psychological domain. In the “Battle of Cognition,” the PRC wields the Information IOP with greater dexterity than the United States. The United States must close the gap by first creating an interagency process to monitor and challenge China’s influence domestically and on a global scale. Second, they must develop the capabilities to determine where China is vulnerable to external influence, causing multiple dilemmas below the level of armed conflict. Third, and finally, if armed conflict is unavoidable, the United States must prepare to fight the battle within its weapon systems.

1. Challenge Chinese Influence – An inter-agency approach

The first recommendation is to create an inter-agency group that monitors, assesses, and challenges China’s influence operations. In 2018, the Center for Strategic Studies published a report entitled “Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare.” In it, authors Mahnken et al., argue the PRC has committed to comprehensively coercing the United States and its allies. Combating coercion requires

intelligence professionals, scholars, and journalists capable of detecting foreign influence and separating the benign from the malignant.⁷⁷

To compete across all 24 warfighting methods, this new organization will require cultural anthropologists, psychologists, economists, technologists, military strategists, intelligence professionals, and more. In *Stealth Warfare* General Spalding offers 11 recommendations for “confronting the Chinese Communist Party’s unrestricted war.” These range from banning American citizens and corporations from investing in CCP sponsored private companies to investigate PRC influence into politicians.⁷⁸ General Spalding’s approach is likely too invasive, but it highlights a significant gap in competing with China. Thankfully, there is a historical precedent for the type of organization needed to counter Chinese comprehensive coercion and address the 24 warfighting methods mentioned in *Unrestricted Warfare*.

“By operating in those shadowy seams, comprehensive coercion does not easily lend itself to traditional diplomatic, military, and other government solutions. Conventional diplomatic, military, and counter-espionage capabilities remain critically important but, on their own, are inadequate to the security challenges that comprehensive coercion brings to bear. Since no one institution or body is solely responsible for combating or even monitoring these operations, comprehensive coercion measures can appear discrete and tactical rather than part of a concerted, overarching strategy to undermine the West.”⁷⁹

In the 1980s, President Ronald Reagan temporarily established the inter-agency “Active Measures Working Group” (AMWG) to counter Soviet Disinformation.⁸⁰ In “Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference,” authors Fletcher Schoen and Christopher Lamb studied the AMWG. AMWG was the definition of interagency. Chaired by the State Department, the group included representatives from the CIA, FBI, DoD, and the now-defunct U.S. Information Agency (USIA).⁸¹ (USIA included Voice of America (VOA) but was closed in 1999 with VOA moving to the State Department).⁸² They concluded that “American history illustrates the importance of

three basic building blocks for national security: strong U.S. capabilities, good intentions, and the effective communication of both to diverse audiences.”⁸³ Moreover, the study identified the need for a full-time dedicated team with diverse expertise. “Although strategic communications are costly and challenging, the United States must be engaged for the long haul in order to have an impact.”⁸⁴

Recommendation #1: invigorate a counter-influence organization, similar to USIA and the AMWG but separate from the State Department, with cross-cutting representation across the National Security apparatus for the implicit purpose of monitoring and countering Chinese influence.

2. Untangling influence and create multiple dilemmas

In “Countering Comprehensive Coercion,” Mahnken et al. posit that defensive measures alone are not sufficient. Instead, the United States must create multiple dilemmas for the adversary, the adversary must believe the cost “in money spent, effort expended, or risk incurred—exceeds what they are willing to pay.”⁸⁵ Through the United Front, information control and manipulation via cyberspace, and social and economic strong-arm tactics, China is unintentionally broadcasting their vulnerabilities. China’s worldwide implementation of 5G technologies has the potential to provide the opportunity to push strategic communications to previously unreachable audiences.

U.S. educated PRC students are the CCP’s center of gravity in their unrestricted warfare campaign. The students acting as recruiters for the Thousand Talents program and social influencers for the United Front are also the CCP’s most critical vulnerability. The United States must compete with China’s United Front, Confucius Institutes, and the Thousand Talents plan

for China's American educated youth. Mahnken et al. provide an excellent summary of this competition.

“CCP-affiliated bodies operating in host communities enjoy access to local networks and intelligence conducive to United Front work. They are tasked to conduct strategic communications with their counterparts to voice China's positions and to influence the discourse on topics as wider-ranging as Taiwan's independence, Tibet, Falun Gong, democracy movements, and the Belt and Road Initiative. Unofficial organizations are assigned to engage in cultural and social exchanges with local communities at the grassroots level, youth groups, and the professional class. United Front writings express a particular interest in the youth of Greater China and beyond to shape the opinion of the next generation.”⁸⁶

The United States must equip these students by challenging Chinese influences while they are in the United States. Moreover, the propaganda these students receive is likely the same information China is manipulating internally.

Information warfare, per *Unrestricted Warfare*, “refers to war in which information technology is used to obtain or suppress information.” Social media influencers, the Great Cyber Wall, and cyberspace operations control information from getting to vulnerable populations.⁸⁷

Leveraging the new counter-influence organization the United States must provide targeted strategic communications to counter false information. Former USIA directed Charles Wick stated it best when he said: “In responding to disinformation, the United States has the tremendous advantage that the truth is inherently more powerful than lies, but if the lies go unchallenged, they can have a damaging effect.”⁸⁸

To challenge a lie, the offended must be aware of the lie. Competing with Chinese influence requires awareness first and then competition. Unfortunately, many American's believe operations utilizing propaganda and counterpropaganda are antithetical to their values. In this light, the United States must develop the mechanisms to generate awareness of CCP influence operations and then modify policy to allow information-based competition. Information based

competition must leverage China's information control and global influence operations to create a counter-message. The United States must synchronize a coherent counter-message across the national security apparatus to compete for influence in the cognitive domain. America's influence warriors must utilize 5G Cellular vulnerabilities, information gleaned from returning students, U.S. cyber capabilities, economic pressures, strategic messaging to allies, partners, and China's regional competitors to create multiple dilemmas.

Recommendation #2: Leverage a reinvigorated American counter-influence organization and utilizing emerging opportunities (students, 5G cellular) to provide strategic communication to previously unreachable audiences.



Conclusion

In conclusion, as author Robert Pape surmised, successful strategy “requires defeating the enemy’s particular strategy, not merely stopping its conventional military operations.”⁸⁹ The United States’ 2018 National Defense Strategy emphasizes competition below the level of armed conflict. Unfortunately, China has a significant head start and has been actively competing for influence on a global scale, ensuring their social, economic, and territorial security. The influence they have already garnered will make it next to impossible for the United States or its allies to prevent Taiwan from becoming an eventual fait accompli to a reunified China. To compete with China, the United States and its allies must rebalance to challenge the CCP’s integrated political, economic, and military strategy. Deterring China from invading Taiwan requires creating multiple dilemmas targeting China’s core national interests.

“Although the boundaries between soldiers and non-soldiers have now been broken down, and the chasm between warfare and non-warfare nearly filled up, globalization has made all the tough problems interconnected and interlocking, and we must find a key for that. The key should be able to open all the locks, if these locks are on the front door of war. And this key must be suited to all the levels and dimensions, from war policy, strategy, and operational techniques to tactics; and it must also fit the hands of individuals, from politicians and generals to the common soldiers. We can think of no other more appropriate key than ‘unrestricted warfare.’”⁹⁰

The multiple dilemma construct described in the Joint Concept describes developing dilemmas across five domains (Air, Land, Sea, Space, Cyber) but does not account for the cognitive domain. China’s informatization strategy seeks asymmetries within all five domains by leveraging the psychological (cognitive) domain. To be effective in competing with China, the United States must create multiple dilemmas within the minds of the CCP leadership. The CCP must fear a digital social invasion via its technology (e.g., 5G Cellular) that threatens the stability of the party by publicizing the information CCP has hidden from its people. The CCP must fear the price for Taiwan being an independent Tibet, a democratic resurgence in Hong Kong, and a

Uighur uprising, and other challenges to Chinese national interests.⁹¹ The CCP must fear, a global campaign to eject Chinese investments and products that ravages their economy following the dismantling of China's high-octane propaganda machine. The information instrument of power has a devastating effect on the cognitive domain, specifically of decision-makers. The United States strategy today is woefully inadequate to compete with the Information IOP vis a vis China. The United States lacks the people, strategy, and organization to challenge China, and sophomoric competition may raise the level of competition into the level of armed conflict where the United States military is even more vulnerable.

“Should deterrence fail...” Military planners have historically used this phrase as the kickoff of campaign planning. If counter-influence operations trigger a military response from China, it forces the United States to leverage the Military instrument of power. Unfortunately, it is likely American technology will not work, either turning an F-35 into a target a la *Ghost Fleet*, or worst case, disinformation deceives American leaders into making a strategic mistake.⁹² General Spalding correctly stated America must reinvent its military, moving away from “spending too much on bombs and bullets” instead they must focus on “manufacturing, STEM and research and design...on 5G, artificial intelligence, and quantum computing.”⁹³ The United States must innovate, adapt, and reorganize to ensure they are not following the historical tendency to fight the last fight instead of the next unrestricted war.⁹⁴

Bibliography

- Air Combat Command (ACC), *Combat Cloud 1.0 Operating Concept*, 1 July 2015.
- Airpower Vista Research Task Force Student #5191, "A Grounded Theory on the Battle of Cognition and Offensive Counter Data as a New Mission for the U.S. Air Force," *Air University*, Maxwell Air Force Base, Alabama: Air University, 15 May 2018.
- Barry, Ellen, "US Accuses Harvard Scientist of Concealing Chinese Funding," *New York Times*, 28 January, 2020.
- Bernstein, Richard, and Ross H. Munro. *The Coming Conflict with China*. New York: Alfred A. Knopf, Inc, 1997.
- Blasko, Dennis J. *Chinese Army Today : Tradition and Transformation for the 21st Century*. 2nd ed. Asian Security Studies. New York: Routledge, 2012.
- Byman, Daniel L., and Matthew C., Waxman, "Kosovo and the Great Air Power Debate," *International Security*, Vol 24, No. 4, Spring 2000.
- Cheng, Dean, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Santa Barbara, CA: Praeger Security International, 2017.
- Victor Cha & Andy Lim, "Flagrant Foul: China's Predatory Liberalism and the NBA," *The Washington Quarterly* (2019), 42:4, 23-42.
- Chairman of the Joint Chiefs of Staff, *Joint Operating Environment (JOE) 2035: The Joint Force in a Contested and Disordered World*. Washington, DC: Pentagon, 2016.
- Cheung, Tai Ming, ed. *Forging China's Military Might: A New Framework for Assessing Innovation*. Baltimore, MD: Johns Hopkins University Press, 2014.
- Cliff, Roger. *China's Military Power: Assessing Current and Future Capabilities*. New York: Cambridge University Press, 2015.
- Cohen, Warren I. *America's Response to China: A History of Sino-American Relations*. 5th ed. New York: Columbia University Press, 2010.
- Crane, Conrad, "Avoiding Vietnam: The US Army's response to defeat in Vietnam," *Strategic Studies Institute*, Carlisle, PA, 2002.
- Davis, Richard, *The 31 Initiatives: A Study of Air Force-Army Cooperation*, Washington, D.C: Office of Air Force History, 1987.

Department of Defense, *Joint Publication 3-13, Information Operations*. 27 November 2012, Change 1, 20 November, 2014.

Department of Defense, *Joint Publication 5-0 Joint Planning*. 16 June 2017

Defense Intelligence Agency. *China Military Power: Modernizing A Force to Fight and Win*, November 2018.

Diamond, Larry and Orville Schell, "Chinese Influence & American Interests: Promoting Constructive Vigilance: Report of the Working Group on Chinese Influence Activities in the United States," *The Hoover Institution*, Stanford, CA: The Hoover Institute, 2018.

Dixon, Robin, "China going big with military parade for its 70th anniversary," *Los Angeles Times*, 25 September, 2019.

Freeman, Chas W. "China's Strategic Caution," *the Globalist*, August 12 2017.

Flournoy, Michele, and Michael Sulmeyer. "Battlefield Internet: A Plan for Securing Cyberspace," *Foreign Affairs*, Vol 97, No. 5, September/October 2018.

Gamer, Robert E., and Stanley W. Toops. *Understanding Contemporary China*, 5th ed. Boulder CO: Lynne Rienner Publishers, 2017.

Gungwu, Wang. *China Reconnects : Joining a Deep-rooted Past to a New World Order*. Singapore: World Scientific Publishing, 2019.

Hallion, Richard P., Roger Cliff, and Phillip C. Saunders. *The Chinese Air Force: Evolving Concepts, Roles and Capabilities*. Washington DC: NDU Press, 2012.

Herman, Arthur, "America's STEM Crisis Threatens Our National Security," *American Foreign Affairs Journal*, Spring 2019, Vol III, Number 1.

Huang, Yanzhong "The Sick Man of Asia," *Foreign Affairs*, Volume 90 No 6, 2011

Jamieson, VeraLinn, and Maurizio Calabrese. "An ISR Perspective in Fusion Warfare," *The Mitchell Forum*, October 2015.

Ji, You. *China's Military Transformation : Politics and War Preparation*. Malden Mass.: Polity Press, 2016.

Kaku, Michio., and Chin, Feodor. *The Physics of the Future: How science will shape human destiny and our daily lives by the year 2100*. New York: Random House, 2011.

Kania, Elsa, "The PLA's Latest Strategic Thinking on the Three Warfares," *Center for International Maritime Security*, August 25, 2016.

- Kelly, Luke. "How China Is Winning Back More Graduates from Foreign Universities Than Ever Before," *Forbes*, January 25, 2018.
- Lewis, John Wilson., and Xue Litai. *Imagined Enemies: China Prepares for Uncertain War*. Stanford, Calif.: Stanford University Press, 2006.
- Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.
- Mahnken, Thomas G., Ross Babbage, and Yoshihara Toshi. "Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare," *Center for Strategic and Budgetary Assessments*, 2018.
- McGregor, Richard. *The Party: The Secret World of China's Communist Rulers*. New York: Harper Collins Publishers, 2010.
- Mitter, Rana. *Modern China : A Very Short Introduction*. Second ed. Very Short Introductions. 2016.
- Walter Russell Mead, "China is the Real Sick Man of Asia," *Wall Street Journal*, 3 Feb, 2020,
- Miller, Mary J, "Principal Deputy, Assistant Secretary of Defense for Research and Engineering, Statement Testimony before the U.S. House of Representatives Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities," *115th Congress*, March 14, 2018.
- Murray, Williamson, "History, War and the Future," *Orbis*, Vol 52, Issue 4, Fall 2008.
- Reed, Kevin, "Renowned Harvard chemistry professor charged with lying about ties to China," *World Socialist Web Site*, 3 February, 2020.
- Ross, Robert S., and Jo Inge Bekkevold, ed. *China in the Era of Xi Jinping: Domestic and Foreign Policy Challenges*. Washington, DC: Georgetown University Press, 2016.
- Ryan, Mark A., David M. Finkelstein, and Michael A. McDevitt. Eds. *Chinese Warfighting: The PLA Experience since 1949*. Armonk, NY: M.E. Sharpe, 2003.
- Rybeck, Charles, Lanny Cornwell, and Philip Sagan. "Applying America's Superpowers: How the U.S. should respond to China's Informatization Strategy," *War on the Rocks*, September 19, 2018.
- Schoen, Fletcher, and Christopher J Lamb. "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference." *Institute for National Strategic Studies*, Strategic Perspectives Number 11, Washington DC: National Defense University Press, June 2012.

- Scobell, Andrew. *China's Use of Military Force: Beyond the Great Wall and the Long March*. Cambridge, UK: Cambridge University Press, 2003.
- Scowcroft, Brent, Paul D Wolfowitz, Richard N. Haass, David E Jeremiah, and Richard Kerr. "The Gulf War: Twenty Years Later," *Council on Foreign Relations*, 15 February, 2011.
- Shambaugh, David, ed., *China & The World*. New York: Oxford University Press, 2020.
- Singer, P.W., and August Cole. *Ghost Fleet: A Novel of the Next World*. New York, NY: First Mariner Books, 2015.
- Singer, P.W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.
- Singer, P.W., *Wired for War: The Robotic revolution and conflict in the 21st century*, New York, NY: Penguin Press, 2009.
- Spalding, Robert Brigadier General Retired, *Stealth War: How China took over while America's elite slept*. United States: Penguin Books, 2019.
- The State Council Information Office of the People's Republic of China. *China's National Defense in the New Era*. Beijing: Foreign Languages Press Co. Ltd, 2019.
- Townshend, Ashley, Brendan Thomas-Noone, and Matilda Steward. "Averting Crisis: American Strategy, Military Spending and Collective Defence in the Indo-Pacific," The United States Studies Centre at the University of Sydney, 19 August, 2019.
- Trauschweizer, Ingo, *The Cold War U.S. Army: Building Deterrence for Limited War*, Lawrence, KS: University Press of Kansas, 2008.
- Twardowski, Adam, "Order from Chaos: General David Goldfein on Building the Air Force of the future." *The Brookings Institute* 22 February 2019.
- United States Air Force, *USAF Multi-Domain C2 Operating Concept (Draft)*, 4 Jan 2017.
- United States Army, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century," Version 1.0, *U.S. Army Training and Education Commander*, Leavenworth, KS: TRADOC Press, December 2017.
- United States Senate, *Permanent Subcommittee on Investigation report to the U.S. Senate: Threats to the U.S. Research Enterprise : China's Talent Recruitment Plan*, Washington, DC: The United States Senate, 18 November, 2019.
- Wall Street Journal, no author, "China Expels Three Wall Street Journal Reporters," *The Wall Street Journal*, 19 February 2020.

- Wang, Haiyan, and Colin Sparks, "Chinese Newspaper Groups in the Digital Era: The Resurgence of the Party Press," *Journal of Communication*, Volume 69, Issue 1, February 2019, Pages 94–119.
- Wang, Huiyao, China's National Talent Plan: Key Measures and Objectives, *Brookings.edu*, May 1, 2011 retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1828162
- Wang, Yaqia, "Opinion: China's Communist Party is as shadowy and repressive as when it took power 70 years ago," *Los Angeles Times*, 30 September 2018.
- Weinbaum, Cortney, and John N. T Shanahan. "Intelligence in a Data-Driven Age," *Joint Force Quarterly* 90, 3rd Quarter 2018.
- Williams, Brett T. Major General, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Issue 73, 2nd Quarter, 2014.
- Zhang, Xiaoming, "Building a World-Class Military." EL6741: Lecture, Chinese Military, Airpower and Implications, Air War College, Maxwell Air Force Base, AL, August 12, 2019.
- Zhang, Xiaoming. "China : The Quest for a Modern Air Force," Chapter 2 in *Air Forces: The Next Generation*. Edited by Amit Gupta. Hampshire, UK; Howgate Publishing Limited, 2020.
- Zhang, Xiaoming, "Chinese Air Power," in *Global Air Power*. Edited by John A. Olsen. Washington, DC: Potomac Books, 2011.
- Zhang, Xiaoming. *Deng Xiaoping's Long War : The Military Conflict between China and Vietnam, 1979-1991*. Chapel Hill, NC: University of North Carolina Press, 2015.
- Zhang, Xiaoming. *Red Wings over the Yalu : China, the Soviet Union, and the Air War in Korea*. 1st ed. Texas A & M University Military History Series ; No. 80. College Station: Texas A&M University Press, 2002.
- Zhen, Liu, "Why 5G, a battleground for the US and China, is also a fight for military supremacy," *South China Morning Post*, September 19, 2019.

Notes

¹ P.W. Singer, and August Cole, *Ghost Fleet: A Novel of the Next World*, (New York, NY: First Mariner Books, 2015).

² Robert Spalding Brigadier General retired, *Stealth War: How China took over while America's elite slept*, (USA, Penguin Books, 2019), xii.

³ The State Council Information Office of the People's Republic of China, "China's National Defense in the New Era", (2019), 7.

⁴ PRC Information Office, "China's National Defense in the New Era," 7, 32.

⁵ Charles Rybeck, Lanny Cornwell, and Philip Sagan, "Applying America's Superpowers: How the U.S. should respond to China's Informatization Strategy," *War on the Rocks*, September 19, 2018. Accessed 3 September, 2019 from <https://warontherocks.com/2018/09/applying-americas-superpowers-how-the-u-s-should-respond-to-chinas-informatization-strategy/>

⁶ Thomas G. Mahnken, Ross Babbage, and Toshi Yoshihara, "Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare," *Center for Strategic and Budgetary Assessments*, 2018. retrieved 23 January 2020 from <https://csbaonline.org/research/publications/countering-comprehensive-coercion-competitive-strategies-against-authoritar/publication/1>, 31; Xiaoming Zhang, "Building a World-Class Military." EL6741: Chinese Military, Airpower and Implications (class lecture, Air War College, Maxwell AFB, AL, August 12, 2019).

⁷ Qiao Liang, and Wang Xiangsui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts publishing House, 1999), 11.

⁸ Roger Cliff. *China's Military Power: Assessing Current and Future Capabilities*. (New York, NY: Cambridge University Press, 2015), 129.

⁹ Liu Zhen, "Why 5G, a battleground for the US and China, is also a fight for military supremacy" *South China Morning Post*, 31 January 2019. Accessed 10 September, 2019 from <https://www.scmp.com/news/china/military/article/2184493/why-5g-battleground-us-and-china-also-fight-military-supremacy>

¹⁰ You Ji, *China's Military Transformation: Politics and War Preparation*. (Malden, MA: Polity Press, 2016), 130; Rybeck, et al "Applying America's Superpowers", September 19, 2018.; Tai Ming Cheung, ed, *Forging China's Military Might: A New Framework for Assessing Innovation*, (Baltimore, MD: Johns Hopkins University Press, 2014), 1.

¹¹ Rybeck, et al "Applying America's Superpowers", September 19, 2018.

¹² Robert Spalding, *Stealth War*, 115.

¹³ Qiao Liang, and Wang Xiangsui, *Unrestricted Warfare*, 7.

¹⁴ Defense Intelligence Agency. *China Military Power: Modernizing A Force to Fight and Win*, November 2018. Accessed 13 August 2019 from https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf, 24; Richard R. Hallion, et al., *The Chinese Air Force*, 145; You Ji, *China's Military Transformation*, 119.

* Information Enabled Operations, Informationized Warfare, Informatization and other similar terms are used interchangeably under the concept of Informatization throughout all cited works.

¹⁵ Tai Ming Cheung, *Forging China's Military Might*, 276.

¹⁶ Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, (Santa Barbara, CA: Praeger Security International, 2017), 15-16.

-
- ¹⁷ You Ji, *China's Military Transformation*, 74.
- ¹⁸ Robert Spalding, *Stealth War*, 148, 208.
- ¹⁹ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 28.
- ²⁰ Andrew Scobell, *China's Use of Military Force: Beyond the Great Wall and the Long March*, (Cambridge, UK: Cambridge University Press, 2003), 66-73; DIA, *China Military Power*, 24; Richard R. Hallion, et al, *The Chinese Air Force*, 18; Rybeck, et al "Applying America's Superpowers", September 19, 2018.
- ²¹ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 45.
- ²² Haiyan Wang, Colin Sparks, "Chinese Newspaper Groups in the Digital Era: The Resurgence of the Party Press", *Journal of Communication*, Volume 69, Issue 1, February 2019, Pages 94–119, <https://doi.org/10.1093/joc/jqy061>; Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 45.
- ²³ Yaqia Wang, "Opinion: China's Communist Party is as shadowy and repressive as when it took power 70 years ago," *Los Angeles Times*, 30 September 2019, Accessed 1 October, 2019 from <https://www.latimes.com/opinion/story/2019-09-30/china-repression-communist-party-70th-anniversary>
- ²⁴ Yaqia Wang, "Opinion: China's Communist Party is as shadowy and repressive as when it took power 70 years ago."
- ²⁵ Robyn Dixon, "China going big with military parade for its 70th anniversary," *Los Angeles Times*, 25 September 2019, Accessed 27 September 2019 from <https://www.latimes.com/world-nation/story/2019-09-24/chinas-70th-anniversary-military-parade-scare>
- ²⁶ Student #5191, Air Power Research Task Force, A Grounded Theory on the Battle of Cognition and Offensive Counter Data as a New Mission for the U.S. Air Force," *Air Power Vistas*, (Maxwell Air Force Base, AL: Air University, 15 May 2018), 27.
- ²⁷ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 33; Robert Spalding, *Stealth War*, 93.
- ²⁸ Robert Spalding, *Stealth War*, 94, 104.
- ²⁹ Rybeck, et al "Applying America's Superpowers", September 19, 2018.
- ³⁰ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 33-34.
- ³¹ Robert Spalding, *Stealth War*, 29.
- ³² Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 33-34.
- ³³ PRC Information Office, "China's National Defense in the New Era," 14.
- ³⁴ You Ji, *China's Military Transformation*, 34-35.
- ³⁵ Robert Spalding, *Stealth War*, 122.
- ³⁶ Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *Center for International Maritime Security*, August 25, 2016, retrieved 25 February from <http://cimsec.org/plas-latest-strategic-thinking-three-warfares/27468>
- ³⁷ Robert Spalding, *Stealth War*, 21.
- ³⁸ Robert Spalding, *Stealth War*, 205-206.
- ³⁹ Robert Spalding, *Stealth War*, 94.
- ⁴⁰ Larry Diamond, and Orville Schell, "Chinese Influence & American Interests: Promoting Constructive Vigilance: Report of the Working Group on Chinese Influence Activities in the United States," *The Hoover Institution*, (Stanford, CA, 2018), 3,103.
- ⁴¹ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 45-46.
- ⁴² Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 48.
- ⁴³ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 27, 45-46.

-
- ⁴⁴ Thomas G. Mahnken, et al., “Countering Comprehensive Coercion, 50.
- ⁴⁵ Thomas G. Mahnken, et al., “Countering Comprehensive Coercion, 50; Larry Diamond, and Orville Schell, “Chinese Influence & American Interests,” 4.
- ⁴⁶ Thomas G. Mahnken, et al., “Countering Comprehensive Coercion, 36; Robert Spalding, *Stealth War*, 139.
- ⁴⁷ Wang, Huiyao, “China’s National Talent Plan: Key Measures and Objectives,” *Brookings.edu*, May 1, 2011 retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1828162
- ⁴⁸ Luke Kelly, “How China Is Winning Back More Graduates From Foreign Universities Than Ever Before,” *Forbes*, January 25, 2018, retrieved 22 February, 2020 from <https://www.forbes.com/sites/ljkelly/2018/01/25/how-china-is-winning-back-more-graduates-from-foreign-universities-than-ever-before/#758256175c1e>
- ⁴⁹ Arthur Herman, “America’s STEM Crisis Threatens Our National Security,” *American Foreign Affairs Journal*, Spring 2019, Vol III, Number 1, retrieved 22 February, 2020 from <https://americanaffairsjournal.org/2019/02/americas-stem-crisis-threatens-our-national-security/>
- ⁵⁰ Arthur Herman, “America’s STEM Crisis Threatens Our National Security.”
- ⁵¹ Wang, Huiyao, “China’s National Talent Plan,” 2.
- ⁵² Permanent Subcommittee on Investigation report to the U.S. Senate, *Threats to the U.S. Research Enterprise: China’s Talent Recruitment Plans*, November 18, 2019, 1,7.
- ⁵³ Investigation report to the U.S. Senate, *China’s Talent Recruitment Plans*, November 18, 2019, 20.
- ⁵⁴ Kevin Reed, “Renowned Harvard chemistry professor charged with lying about ties to China,” *World Socialist Web Site*, 3 February, 2020 retrieved from <https://www.wsws.org/en/articles/2020/02/03/harv-f03.html>; Ellen Barry, “US Accuses Harvard Scientist of Concealing Chinese Funding,” *New York Times*, 28 January, 2020, retrieved from <https://www.nytimes.com/2020/01/28/us/charles-lieber-harvard.html>; As a note the Coronavirus global epidemic from Winter/Spring 2020 originated from Wuhan China.
- ⁵⁵ Student #5191, “A Grounded Theory on the Battle of Cognition,” 27.
- ⁵⁶ Student #5191, “A Grounded Theory on the Battle of Cognition,” 27.
- ⁵⁷ Student #5191, “A Grounded Theory on the Battle of Cognition,” 27.
- ⁵⁸ Victor Cha & Andy Lim, “Flagrant Foul: China’s Predatory Liberalism and the NBA”, *The Washington Quarterly* (2019) , 42:4, 23-42.
- ⁵⁹ Victor Cha & Andy Lim, “Flagrant Foul: China’s Predatory Liberalism and the NBA”, 23-42.
- ⁶⁰ Yanzhong Huang, “The Sick Man of Asia,” *Foreign Affairs*, Volume 90 No 6, 2011 from <https://www.bths.edu/ourpages/auto/2011/9/14/65205157/FOREIGN%20AFFAIRS%20ARTICLE%20ON%20CHINA.pdf>; Walter Russell Mead, “China is the Real Sick Man of Asia,” *Wall Street Journal*, 3 Feb, 2020, <https://www.wsj.com/articles/china-is-the-real-sick-man-of-asia-11580773677>; Wall Street Journal no author, “China Expels Three Wall Street Journal Reporters,” *The Wall Street Journal*, 19 February 2020, from <https://www.wsj.com/articles/china-expels-three-wall-street-journal-reporters-11582100355>
- ⁶¹ Larry Diamond, and Orville Schell, “Chinese Influence & American Interests,” 2, 83-84.
- ⁶² Robert Spalding, *Stealth War*, 50.
- ⁶³ Wall Street Journal no author, “China Expels Three Wall Street Journal Reporters,” *The Wall Street Journal*, 19 February 2020, from <https://www.wsj.com/articles/china-expels-three-wall-street-journal-reporters-11582100355>
- ⁶⁴ Thomas G. Mahnken, et al., “Countering Comprehensive Coercion, 28.
- ⁶⁵ PRC Information Office, “China’s National Defense in the New Era,” 5.

-
- ⁶⁶ John W. Lewis, and Xue Litai, *Imagined Enemies: China Prepares for Uncertain War*. Stanford, CA: Stanford University Press, 2006. 243
- ⁶⁷ John W. Lewis, and Xue Litai, *Imagined Enemies*, 215.
- ⁶⁸ You Ji, *China's Military Transformation*, 142. * You Ji utilizes the acronym 2A/AD to described Anti-Access & Aerial Denial but the other authors and US military literature utilize the A2/AD acronym that this author will use in this paper.
- ⁶⁹ John W. Lewis, and Xue Litai, *Imagined Enemies*, 225, 227.
- ⁷⁰ John W. Lewis, and Xue Litai, *Imagined Enemies*, 214
- ⁷¹ Xiaoming Zhang, "Chinese Air Power," in *Global Air Power*, edited by John A. Olsen, (Potomac Books, 2011), 306; John W. Lewis, and Xue Litai, *Imagined Enemies*, 1; Michael S. Chase, "Defense and Deterrence in China's Military Space Strategy," *China Brief*, (Volume XI, Issue 5, March 25, 2011) 12.
- ⁷² VeraLinn Jamieson and Maurizio Calabrese, "An ISR Perspective on Fusion Warfare," *The Mitchell Forum*, October 2015, 6.
- ⁷³ VeraLinn Jamieson and Maurizio Calabrese, "An ISR Perspective on Fusion Warfare," 35.
- ⁷⁴ Rybeck, et al "Applying America's Superpowers", September 19, 2018.
- ⁷⁵ Robert Spalding, *Stealth War*, 83.
- ⁷⁶ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, 146.
- ⁷⁷ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 61-64
- ⁷⁸ Robert Spalding, *Stealth War*, 215-217.
- ⁷⁹ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 7-8, 55-56.
- ⁸⁰ Fletcher Schoen, and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *National Defense University*, Washington, DC: National Defense University Press, June 2012, retrieved 23 Jan 2020 from <https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf> , 3.
- ⁸¹ Fletcher Schoen, and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications," 35, 76.
- ⁸² Robert Spalding, *Stealth War*, 206.
- ⁸³ Fletcher Schoen, and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications," 120.
- ⁸⁴ Fletcher Schoen, and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications," 120.
- ⁸⁵ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 60.
- ⁸⁶ Thomas G. Mahnken, et al., "Countering Comprehensive Coercion, 49.
- ⁸⁷ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, 18.
- ⁸⁸ Fletcher Schoen, and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications," 115.
- ⁸⁹ Daniel L. Byman and Matthew C. Waxman, "Kosovo and the Great Air Power Debate," *International Security*, Vol. 24, No. 4 (Spring 2000), 23; Robert Pape, *Bombing to Win*, 30.
- ⁹⁰ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, 222.
- ⁹¹ PRC Information Office, "China's National Defense in the New Era," 5.
- ⁹² P.W. Singer, and August Cole, *Ghost Fleet*, 78.
- ⁹³ Robert Spalding, *Stealth War*, 217.
- ⁹⁴ Conrad Crane, "Avoiding Vietnam: The US Army's response to defeat in Vietnam," *Strategic Studies Institute*, (Carlisle, PA, 2002)

https://www.files.ethz.ch/isn/47370/Avoiding_Vietnam_US.pdf (Accessed September 12, 2019), 18.

