

Thoughts on Information Advantage

Information is fast becoming the dominant factor in all levels of Great Power competition, crisis, and conflict. Maintaining an information advantage over our potential adversaries, across the Diplomatic, Information, Military, and Economic (DIME) spheres, and then, in terms of military operations, at all echelons in a Joint and Combined way, will be the most critical factor in determining success in all operations now and in the future. As the Army contemplates its role in this process, it is coalescing its

Figure 1: Decision Dominance and Information Advantage

Decision Dominance: a desired state in which a commander can sense, understand, decide, act, and assess faster more efficiently than an adversary.

Information Advantage: A condition where a force holds the initiative in terms of relevant actor behavior, situational understanding, and decision-making through the use of all military capabilities.

thoughts around the idea of seeking **Decision Dominance** by maintaining an **Information Advantage** over our adversaries (see figure 1). However, our pacing threat (China) and our near-peer threat (Russia) also have sophisticated approaches to the use of information, and in some ways maintain unique advantages in this realm.

China: Political Warfare for an Intelligentized Age

China is best known in the U.S Intelligence Community for advancing its strategic goals through intellectual property theft. That said, China is the most **methodical** competitor in the information dimension. In fact, The FBI Director, Christopher Wray, stated, “No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China.”¹ China has developed a unique approach to operations in the ID, which converges

traditional Marxist-Leninist notions surrounding political warfare², and advances them to take advantage of the opportunities that Beijing’s whole-of-nation power brings to the high-tech, intelligentized age. Political warfare first came to the forefront in the late 1940s and early 1950s as part of the Cold War. No less astute an observer as George Kennan, writing in 1948 about the Soviet efforts to employ political warfare in a now-declassified State Department position paper defined it as:

The logical application of Clausewitz’s doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation’s command, short of war, to achieve its national objectives, *to further its influence and authority and to weaken those of its adversaries* (struck in the original, but a key thought, nonetheless). Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures, and “white” propaganda to such covert operations as clandestine support of “friendly” foreign elements, “black” psychological warfare and even encouragement of underground resistance in hostile states.³

China’s political warfare activities also are guided by traditional Chinese thought, including the writings of Sun Tzu:

¹ Department of Justice, “Attorney General Jeff Session’s China Initiative Fact Sheet,” 1 November 2018.

² Peter Mattis, “China’s ‘Three Warfares’ In Perspective,” *War on the Rocks*, 30 January 2018.

³ George F. Kennan, “The Inauguration of Organized Political Warfare,” [Redacted Version of a National Security Council Document], Wilson Center Digital Archive, 30 April 1948

“The supreme art of war is to subdue the enemy without fighting.”

“All warfare is based on Deception”

“If you *know* the *enemy* and *know* yourself, you need not fear the result of a hundred battles.”

China has built on these ideas, and is in a much better position than the Soviet Union was to carry them out due to their economic clout, their rapid acquisition of advanced technology (both stolen and indigenously developed), and their highly integrated power center, which can effectively harmonize activities across the DIME, while also drawing on the Chinese pseudo-private sector in what is termed “civil-military fusion.” The ideas surrounding political warfare that Kennan expressed above are found throughout Chinese ID activities.

Because it operates on a broad, whole-of-nation spectrum, Chinese information operations generally operate around a unified theme pushing well developed narratives designed to gain influence across the globe where it can, and to effectively deter and undermine the efforts of nations it views as hostile to its inevitable (through the eyes of Beijing) rise. The narratives generally center on the idea that China is rapidly becoming a global power and that their approach to international relations/discourse is superior to that of the West. The Chinese Communist Party has been building what it calls “discourse power” by shaping a narrative that its model of government is superior to democratic government structures.⁴ They argue that China, who suffered generations of humiliation in a global system dominated by others (especially Westerners), is the future. And unlike US/Western efforts in the information arena, Beijing works to match words and actions, in an integrated fashion. The Belt and Road Initiative is such an integrated effort designed to boldly demonstrate across the DIME, that China is the up and coming power with global reach and impact.

It also is increasingly clear that China’s information efforts are aimed squarely at the United States and its Allies and Partners as its arch rival/foil. A telling example was the “Wolf Warrior” campaign, undertaken by the Chinese Ministry of Foreign Affairs. This effort drew upon the very popular series of movies in China “Wolf Warrior,” which in many ways are akin to the Rambo movies in the 1980s, that push a pro-China message of toughness in the face of their adversaries⁵. The Wolf Warrior diplomats represented a fundamental change for Chinese diplomacy, which was traditionally bland and stale. These new diplomats were instructed to be fiery and bold, and to push back repeated at perceived insults of China wherever they were in the world, and they integrated this effort with social media platforms both internal to China, but also on Western platforms like Twitter and Facebook. This effort has come to the forefront with the onset of the COVID-19 pandemic and China’s “mask diplomacy,” where they gave out PPE, masks, and eventually vaccines around the globe and used both white and black propaganda to show the impact of their efforts. The Wolf Warrior as a narrative was very useful as it targeted China’s internal and external audiences simultaneously. Internally, it showed that China was being aggressive on the world stage, and was pushing against the West. This narrative played on the views of a significant portion of China’s youth who are highly supportive of an aggressive, world-

⁴ Edwin S. Cochran, “China’s ‘Three Warfares’: People’s Liberation Army Influence Operations,” *International Bulletin of Political Psychology*, Volume 20, Issue 3, 7 September 2020, 3-4.

⁵ Jessica Brandt and Bret Schafer, “How China’s ‘Wolf Warrior’ Diplomats Use and Abuse Twitter,” *Brookings Tech Stream*, 28 October 2020; and Yaoyo Dai and Luwei Rose Luquiu, “China’s ‘Wolf Warrior’ Diplomats Like to Talk Tough,” *The Washington Post*, 12 May 2021.

leading power known as the “Young Pinks.” At the same time, it demonstrates to the international community that China is a leader and that its activities and system are superior to the West.

Until recently, China had not employed offensive social media capabilities akin to Russia’s main information efforts. However, COVID-19 shifted that dynamic. China, in seeking to protect its international image, employed a comprehensive information campaign to counter the narrative that COVID-19 originated within its borders. Chinese agents also created fake social media accounts to push out false messages on Twitter and in texts that the US government was planning COVID-related lockdowns. A further example of this type of activity occurred during the VPOTUS’ recent visit to Asia. VPOTUS was slated to travel to Vietnam, where as part of her visit, she was announcing that the US was donating one million doses of COVID vaccine to Hanoi, which is hard pressed by the virus. When the VPOTUS’ flight to Vietnam was delayed, China quickly stepped to the forefront, and arranged a press conference with its ambassador in Hanoi where it pledged to donate **2 million doses** of its own indigenous vaccine to Vietnam in a show of well-orchestrated one-upmanship.⁶

The PLA is an active component of China’s broader Political Warfare efforts, and it works to help achieve China’s national-level information goals, as well as to establish its own form of Decision Dominance and Information Advantage for its own military operations. Indeed, the PLA’s active participation in these efforts, along with the key role it plays within the civil-military fusion construct transforms the original Political Warfare definition into something akin to **confrontational competition**, which provides a more operationalized form of Political Warfare, broadens it, and gives it other avenues of advance against an adversary. The key element of this approach for the PLA is the “Three Warfares Doctrine.”

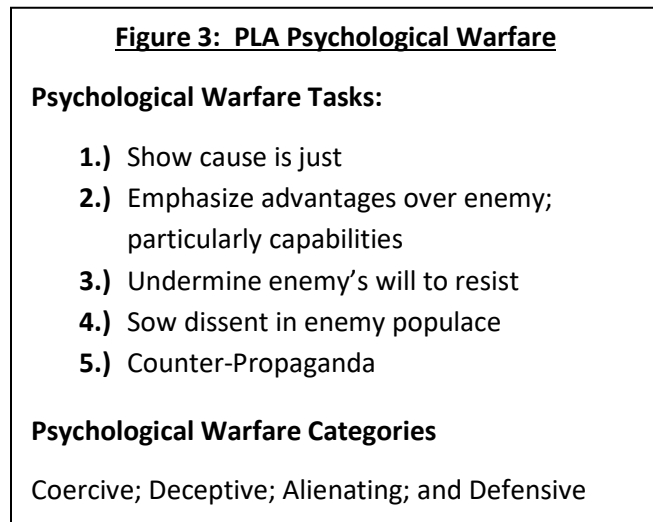
Based on principles dating back to the 1960s, but refined in the early 1990s and also throughout the 2000s, the Three Warfares Doctrine is the PLA’s effort to frame its operations within the information environment. These ideas were codified and approved by the CCP Central Commission and the Central Military Commission, and were written into the PLA’s Political Works Regulations. The Three Warfares offers the PLA a dynamic, nuanced approach to information operations that allows them to influence a target audience and to complicate an adversary’s decision-making cycle. It operates along three interrelated lines of effort: 1.) Media Warfare; 2.) Psychological Warfare; and 3.) Legal Warfare (sometimes called “lawfare.”) When taken together, these provide the PLA with a capability to control perceptions and shape the narrative, while undermining those of an opponent. This likely is designed for use in competition, but becomes essential in crisis as they work to set conditions for a transition to conflict in their favor. It also may provide them with a way to maintain a narrative edge in conflict and perhaps even allow for off-ramps in China’s favor.⁷

Media Warfare focuses on the control and exploitation of means of communications to influence public opinions and attitudes that build support, or “buy-in” to PLA military actions and deter an adversary from pursuing actions that counter them. These type of operations focus not just on traditional media, but also on films, television programs, music, global media, and increasingly, in social media/cyberspace. It relies on all activities to manipulate public attitudes (foreign and domestic). The use of propaganda narratives is essential to this effort, and the PLA will rely on white, gray, and black propaganda to

⁶ Shibani Mahtani, “Harris, in Vietnam, Gets a Dose of China’s Challenge to the U.S.,” *The Washington Post*, 25 August 2021.

⁷ Cochran, 2-9.

achieve its goals. It is the cornerstone of the Three Warfares Doctrine, and sets the conditions for the other two elements.⁸



The PLA considers Psychological Warfare to be the method by which they can influence, constrain, and/or alter an enemy's thoughts, emotions, and habits, while simultaneously buttressing their own⁹. It is designed to get inside the enemy's decision-making cycle and to slow or suppress their ability to conduct military operations by shocking and demoralizing their enemy's military personal and civilian population. It is designed to sow doubts and to create a sentiment in a targeted population that undermines their enemy's leadership. The PLA has spent a great deal of effort at thinking about these type of operations, and it has five psychological

warfare tasks and five psychological warfare categories (see Figure 3).¹⁰

Legal Warfare relies on the use of Chinese domestic and international law, as well as the adversary's own domestic laws against them to demonstrate the "rightness" of Beijing's position. It offers a stilted, but legalistic justification for any PLA/Chinese action, while illustrating the illegality of an adversary's activities. It generally is designed to attain a particular objective, while allowing China, the CCP and the PLA to retain the political initiative and international top cover for their efforts. When matched with Media Warfare, it is a useful tool to help set key narratives.¹¹

While the PLA plays a critical role in China's whole of nation confrontational competition effort, it also recognizes the centrality of information in terms of military operations. More accurately, it understands the imperative for transitioning from informationized warfare to intelligentized warfare, where the PLA can augment its already formidable understanding of how to use information and merge it with new technologies, such as artificial intelligence, quantum computing, big-data analytics, cloud computing, and unmanned systems.¹² Where "informationized" warfare focused on ways to weaken an adversary's ability to acquire, transmit, process, and use information during warfare, and seek their capitulation prior to the start of conflict, "intelligentized" takes it to another level. Information superiority is essential the PLA's views of modern conflict, and the newly developing "intelligentized" warfare concept will target the enemy's information itself; targeting its AI, its big data, all in an effort to shape the cognitive realm, which in the PLA's thought's on intelligentization, becomes **a separate warfighting domain**. A strand of thinking within the PLA calls for it be able to seize "war control," or the ability to precisely control and adjust warfighting intensity and scope to achieve the objectives for which the war

⁸ Ibid., 4-5.

⁹ Ibid., 5-6.

¹⁰ Ibid; and Mattis.

¹¹ Cochran, 9-10 and Mattis.

¹² Mark Pomerleau, "China Moves Toward New 'Intelligentized' Approach to Warfare, Says Pentagon," *C4ISRNet*, 1 September 2020.

is fought.¹³ When taken together, the idea of intelligentized warfare is all about war control, and information is at its heart.

The PLA is doing more, however, than simply talking about how to carry out information-related operations. In 2015, they created the PLASSF as a separate branch of its Armed Forces. The creation of this entity signaled the importance of informationized operations, and its continued development and successes place it at the very forefront of the shift to intelligentized warfare and as the PLA's operational arm of its information-related activities. It brings together under one command space, cyber, electronic warfare, and information operations capabilities. It is considered a "new-type combat force," and its creation demonstrates the importance of information dominance to China's way of war. The PLASSF inherits both offensive and defensive information operations, and it will play a central role in carrying out the PLA's efforts to secure information dominance and target its enemy's decision-making cycle.

Russia: Information Confrontation [Informatsionnoe provivoborstvo, or IPb] Turns Weakness into Strength

Russia is the most **capable** actor in the information dimension – its ability to synchronize information effects across all mediums is unmatched. Russia, and its Soviet predecessors, have a long history at using information as a means of advancing its national interests and objectives. Kennan's discussion on political warfare was designed specifically for the Soviet model. Although it shares history and culture, today's Russia is not the Soviet Union, and its use of information is not simply a reprisal of Cold War activities. Russia's current approach to information operations, known to them as Information Confrontation, takes advantage of three contemporary Operational Environment characteristics of which the old Soviet approach could only have dreamed: 1.) the character of modern warfare; 2.) the global interconnectedness of the information domain, and; 3.) the prominence of non-governmental organizations in the international order who can serve as witting partners or unwitting pawns for Moscow's information activities.¹⁴ Russia's current approach to information confrontation is aimed directly at the United States and its NATO Allies and European partners, and it targets the key vulnerabilities Moscow perceives in their open, democratic societies. At its core, Information Confrontation is designed to create confusion and sow doubt in the existence of truth, thereby complicating an adversary's decision-making and also undermine their will to engage in conflict. If done correctly, Information Confrontation keeps the Kremlin at a threshold below armed conflict, and allows it to "win without fighting."

Figure 4. Russian Information Warfare

"A new type of war had emerged, in which armed warfare has given up its decisive place in the achievement of military and political objectives of war to another kind of warfare – information warfare." Vladimir Kvachkov, Russian GRU

¹³ John Dotson and Howard Wang, "The 'Algorithm Game' and Its Implications for Chinese War Control," *The Jamestown Foundation*, China Brief Volume 19, Issue 7, 9 April 2019.

¹⁴ Lesley Kucharski, "Russian Multi-Domain Strategy Against NATO: Information Confrontation and US Forward-Deployed Nuclear Weapons in Europe," Lawrence Livermore National Laboratory, 2018, 3.

Information Confrontation offers a two-pronged pathway to secure a form of Decision Dominance over its adversaries. The first form is termed information technical operations, and these are designed to target, disrupt, exploit, manipulate, or destroy an adversary's C4ISR and other systems a society needs to function. This involves a combination of cyber operations, space and counter-space efforts, and electronic warfare at all echelons. The second type is information psychological operations, and these are designed to exploit and exacerbate pre-existing societal divisions, and affect the cognitive realm and emotions of targeted audiences and individuals.¹⁵ In the Russian concept of information confrontation, there is no distinction between where information resides, be it on a system or in the human mind, just like there is no distinction between how information is transferred between those two repositories.¹⁶

It must be noted that Russia's use of information is to them, a defensive response to an overly aggressive United States (and NATO), but also as a response to its own perceived military weakness when compared to its main adversaries.¹⁷ Nevertheless, while Russia may consider information operations a defensive response, their approach and doctrine to these operations states that they are "always at war" in the information space.¹⁸ Operating with information confrontation activities allows Moscow to control escalation and stay under the threshold of war, while still directly competing with its main adversary on a global level. It also considers information confrontation to be a form of deterrence it can employ against an adversary in a place where Moscow may believe it has a form of dominance.

Like China, Russia's information activities reflect a whole of nation approach, which involve all elements of Russian national power. Russian strategic documents, including its National Security Strategy and its Foreign Policy Concept all make references to the importance of information as a means to influence international opinion on Russia and to secure Russia's position as one of the world's leading nations. Moscow's international efforts focus on developing effective ways to influence foreign audiences and deliver what it terms "unbiased" views of Russia and its actions. They seek to use new ways of communicating (social media) and also to engage with thought leaders in the academic world and with NGOs to help set the international security dialogue. In short, Russia's information confrontation approach is all about setting the narratives it wishes to convey and countering those it wishes to suppress.¹⁹

The Defense Intelligence Agency defines information confrontation as Russia's term for conflict in the information sphere. They assess it includes diplomatic, economic, military, political, cultural, social, and religious arenas across both the information technical and information psychological lines of effort.²⁰ The fundamental differences noted above between how the Soviets once conducted political warfare and how Russia undertakes information confrontation allows Moscow to wage a more focused effort against a broader series of targets, and often with a degree of plausible deniability that it makes it very

¹⁵ Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspiration," 2017, 38.

¹⁶ Kucharski, 4; and Keir Giles, *Handbook of Russian Information Warfare*, NATO Defense College Fellowship Monograph, November 2016, 6-7.

¹⁷ Kucharski, 4-5; and Michel Duclos, "Russia's National Security Strategy 2021: The Era of 'Information Confrontation'", Institute Montaigne, 2 August 2021.

¹⁸ US Department of State Global Engagement Center, "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem," August 2020, 6.

¹⁹ Ibid., 5.

²⁰ DIA, 37-39.

difficult to determine Moscow's role in the effort. Where Soviet efforts once focused on individuals and on groups – the anti-nuclear movement in Western Europe, for example – Moscow's ability to effectively use social media content (white, gray, and black) to shape opinions means that they can with very little effort, and often using private entities and cut-outs, impact whole populations vice a handful of targets.²¹ This has been on display across the United States and Europe as Moscow conducted operations aimed at influence a variety of political elections and to sow broader societal dissent on hot-button issues. Furthermore, as the Russians consider this struggle to be perpetual, it also is dynamic. Russia can change positions as needed, and even can play both sides of the fence by taking one position publicly, but using deniable assets (witting or unwitting) to perpetuate another.

Russian Information operators are experts in understanding and leveraging key fault lines in the U.S. domestic base. They excel at sowing political discord in domestic audiences and target audiences. They are on a continuous campaign to spread misinformation and disinformation to create internal strife, change attitudes and behaviors, and cause polarization in domestic U.S. audiences. Their operators are given free rein to post on social media, hack and post stolen information, and build online support against political enemies. For example, during the 2016 U.S. Elections, Russia's Internet Research Agency (IRA) used gray and black information operations on social media to organize rallies, promote their preferred candidate with gray and black tropes, and discredit the candidate they did not prefer. Russia also has interfered with the UK BREXIT proceedings, with elections in France, Montenegro, and the Netherlands, as well as with voting issues in the European Union and the United Nations.

And like China, there also is a military component to Russia's information confrontation efforts. It may not be the main effort, as the intent of Moscow approach to information is stay below the conflict threshold, but these operations clearly are linked to military operations. Chief of the General Staff of the Armed Forces of the Russian Federation, GEN Valery Gerasimov famously wrote that the ratio of non-military means to military means in contemporary Great Power military conflict is 4:1. Furthermore, while the military has significant capabilities that can come to bear in the IE – including some cyber capabilities, intelligence capabilities, space and counter-space capabilities, and a great deal of EW capabilities – the vast majority of Moscow's ability to influence opinion resides outside of the military, and sometimes outside of the government.²²

The military can, however, benefit from the broader elements of Russia's whole-of-nation information operations. Significant information confrontation activities surrounded Russia's invasion of Georgia in 2008 and Russia's annexation of the Crimea from Ukraine in 2014. These activities caused confusion, particularly the infamous "little green men" who spearheaded the military move into Crimea who could not directly be attributed to Russia. Even military exercises, like the recently-concluded ZAPAD in the Western Military District had a significant information theme, as do ongoing Russian operations in Ukraine, while Russia's recent large-scale deployments to the Ukrainian border clearly was intended as an information confrontation activity designed to undermine Ukrainian resolve, NATO willpower, and to set the agenda of Russia as a world leader.

Both China and Russia have well-developed approaches to information operations, and in their own ways, seek to achieve what we term **Decision Dominance** and **Information Advantage** (see Figure 1.)

²¹ Kucharski, 3-6.

²² Blagovest Tashev, Michael Purcell, and Brian McLaughlin, "Russia's Information Warfare: Exploring the Cognitive Dimension," *Marine Corps University Journal*, Volume 10, No. 2, Fall 2019, 129-131.

Their approaches seek to achieve some of the same advantages the U.S. Army considers when discussion these terms. When we talk about China and Russia in terms of competition, crisis, and conflict, we often note that they both attempt to: 1.) win without fighting; and 2.) use standoff capabilities to separate the United States internally, from our allies and partners, and in an operational/tactical sense, separate the constituent elements of the Joint Force. These objectives make information a central element of their Great Power competition, which they use it to help dominate in crisis and conflict, while at the same time attempting to control escalation and quickly achieve their objectives. Their respective weaponized approach to information may be the most effective “standoff” weapon that our adversaries wield.

*Sincere thanks go to **Mr. David May (DISL)**, the Senior Cyber Intelligence Advisor at the Cyber Center of Excellence and to **COL Justine Krumm**, the G-2 of Army Cyber Command for their thoughtful insights, additions, and commentary on this paper.*