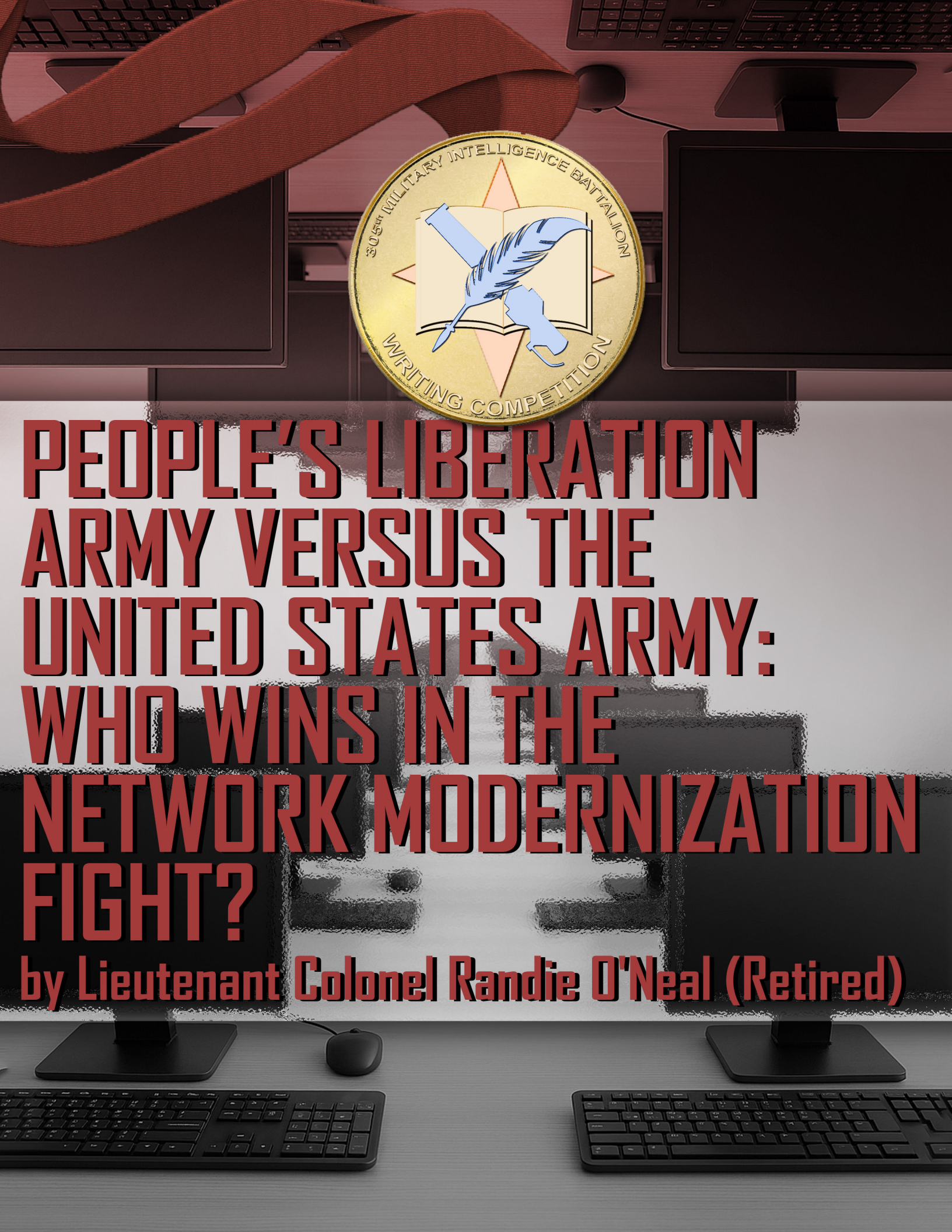
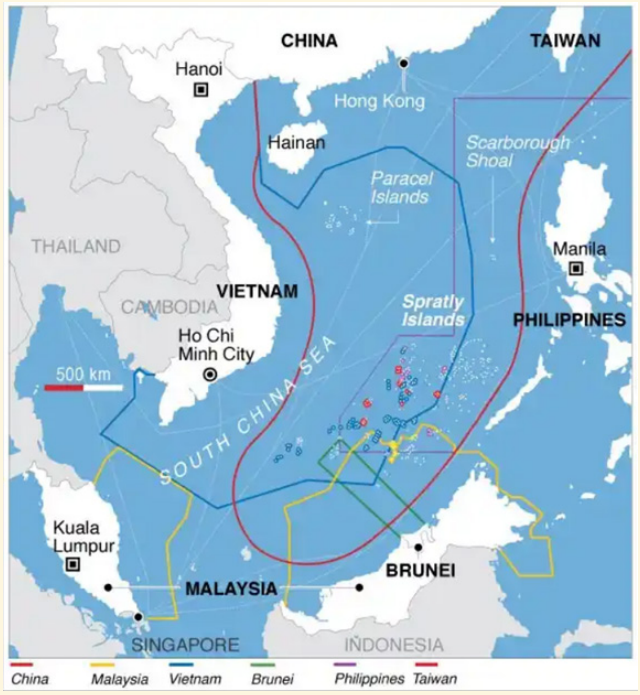


PEOPLE'S LIBERATION ARMY VERSUS THE UNITED STATES ARMY: WHO WINS IN THE NETWORK MODERNIZATION FIGHT?

by Lieutenant Colonel Randie O'Neal (Retired)

Occupation of the Scarborough Shoal

In a possible near future, the People's Republic of China (PRC), after an increase of tensions with the United States and coalition forces in the Indo-Pacific Theater, commences the occupation of Scarborough Shoal in the South China Sea, some 220 kilometers from the Philippines. The PRC has stated that this shoal is necessary for the defense of the People's Republic of China and critical for the protection of their sovereign right to the freedom of navigation.[1]



Disputed territory in the Indo-Pacific Region (graphic public domain by Voice of America)

Elements of the People's Liberation Army Navy occupy positions within these contested waters and declare a 12-mile limit in and around the shoal–an overt violation of previous international agreements and protocols. In response, and at the request of the Philippine president, a combined joint task force (CJTF) of the United States, Philippine, Japanese, and Taiwanese forces announce a combined joint operations area extending from the Spratly Islands, including Taiwan and the Japanese islands of Taketomi, Ishigaki, Tarama, and Miyakojima.

The United States deploys three U.S. Pacific Air Forces air wings that include a mix of strike, bomber, intelligence, surveillance, and reconnaissance, and support aircraft to the former Clark Air Base, Luzon. The U.S. Army's 25th Infantry Division from Hawaii, bolstered with U.S. Army maritime elements, moves to forward bases in the Philippines to provide sustainment and mobility for the forces in and around the combined joint operational area and the CJTF. A U.S. Marine expeditionary brigade deploys to the western coast of the island of Luzon, with some elements forward based on the island of Palawan. From the start, the CJTF experiences communications interoperability problems with coalition members and host nation elements. Tactical communications between the United States and Philippine forces are hampered as jamming and cyberspace attacks shut down key infrastructure, delay the deployment of forces, and render host nation utilities and telecommunications inoperable. Unknown entities on social media who notice Japanese participation in the CJTF announce, "The Japanese reoccupation of Luzon has begun." This announcement prompts public demonstrations and Japanese flag burnings across the Philippine islands.

Demonstrations and protests in Manila bring the city to a standstill as the government struggles to maintain order. The local press and social media call for the expulsion of "foreign occupiers" and an ouster of the sitting president. The PRC offers the Philippines $50 million of immediate aid, with another $50 million in Dragon's Gift[2] conditional assistance and loans over 10 years. The Dragon's Gift mandates the deployment of Chinese specialists in the country to remediate and rebuild infrastructure and assist in developing agriculture and other projects. The sole condition for providing this assistance is that the Philippines must cede the Scarborough Shoal to the PRC and expel any "foreign forces" currently residing in the Philippines and any territory it controls.

Editor's Note: This article was written in early 2024 as part of a professional writing competition open to the Army Soldiers and civilians of the 305th Military Intelligence Battalion, Fort Huachuca, Arizona. Competitors drew upon their operational and institutional experience as well as subject matter experts from across the Military Intelligence Corps to address challenges facing the intelligence warfighting function. For this competition, writers tailored their articles to the Indo-Pacific Command's area of responsibility.

Introduction

This work examines the People's Liberation Army's (PLA's) strategy to counter the United States Army's efforts to modernize its networks as part of the Joint All-Domain Command and Control strategy. A review of the relevant literature indicates that most of the PLA's efforts focus on replicating our strategic and doctrinal efforts, as well as our technology. The PLA's systems approach to warfare is its version of our joint multidomain operations; however, China has expanded the continuum of warfare beyond the kinetic phase into the right now. The PLA began this fight well over ten years ago, and it continues to this day.

If the PRC develops its doctrine into actionable warfighting systems capable of affecting the United States presence and forward deployment to support key Indo-Pacific allies, this or a similar scenario may become a reality.

People's Liberation Army: Modernization Across Domains

The PLA is rapidly modernizing its capabilities across all warfare domains. It is also developing its own version of the Joint All-Domain Command and Control, which is the U.S. joint force "warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed

Members of the People's Liberation Army Information Warfare Support Force browse online news on desktop computers. (Image from the National Security Archive)

of relevance."[3] This modernization is changing how the PLA defines warfare in its doctrine; it now views modern warfare as a "contest between opposing operational systems" rather than merely opposing armies.[4] Further, the PLA views conflict in terms of systems confrontation and systems destruction.

The PLA's approach to warfare separates systems into two categories:

- Large, integrated systems made up of multiple, smaller systems (an interconnected system of systems).
- Individual systems that execute specific functions, such as command and control (C2), fires support, electronic warfare, intelligence, surveillance, and reconnaissance, logistics, and sustainment.

This approach is designed to identify targets both before and during a conflict.

Underlying this doctrinal framework are two concepts that aim to transform the PLA: *informationized warfare* and *intelligentized warfare*. Informationized warfare is described as the strategic implementation of information technology in the digital age with the aim of improving C2 and operations across the warfighting functions and the spectrum of conflict.[5] Intelligentized warfare "seeks to increase the pace of future combat by effectively fusing information and streamlining decision making, even in ambiguous or highly dynamic operating environments.... It also amplifies the nascent concepts embodied by the Military-Civil Fusion effort."[6] This strategy focuses on acquiring technologies such as quantum computing, semiconductors, fifth-generation mobile network/long-term evolution (5G/LTE) data, nuclear and aerospace technology, gene editing, and artificial intelligence to achieve Chinese military dominance. These technologies are the backbone of an informationized and intelligentized PLA. "Careful alignment of military and civilian efforts enables the synchronization of efforts and streamlines the fielding process for the PLA."[7]

For the PLA, the final steps in its efforts to counter peer and near-peer threats are to enable its operational and tactical forces through the informationization and intelligentization of its integrated joint service capabilities and the use of emerging and disruptive technologies and techniques, which are described as—

- Attrition warfare through intelligent swarms of unmanned aircraft systems or other platforms to overwhelm the adversary's ability to respond.
- Cross-domain (joint) warfare that will integrate capabilities across land, sea, air, space, and cyberspace, as well as the emerging cognitive domain.
- Artificial intelligence-based space confrontations that will deny and destroy the adversary's use of space-based C2, global positioning systems (GPSs), and intelligence, surveillance, and reconnaissance capabilities.
- Cognitive control operations that will improve information processing in support of situational awareness and decision making at the operational and tactical levels.[8]

These capabilities currently appear aspirational, even for Western militaries. However, given the assets and resources the PLA is devoting to the effort, it is likely the PLA may achieve some breakthroughs, providing China with a significant advantage, as demonstrated by its cyberspace capabilities in recent years.

What works against China is its lack of operational military experience in modern warfare, its other significant efforts, such as the Belt and Road Initiative's international infrastructure projects, and its declining population.[9] All three hamper

China's ability to field an effective military and a technological and industrial workforce competent enough to actualize this great leap forward. Nevertheless, it is likely the PLA may see some significant improvements to their C2 and intelligence within 8 to 10 years, as well as advancements in cross-domain operations that they could leverage against peers, near peers, and other adversaries in the Indo-Pacific region. Given China's aspirations for informationized warfare and intelligentized warfare in the near future, what does this all mean?

The PLA has methodically analyzed the strategy, doctrine, tactics, and wars that the United States (China's primary adversary) and other adversaries in the Indo-Pacific region have fought since the early 1990s. This analysis has resulted in a review of China's warfighting capabilities across the five military domains—land, maritime, air, space, and cyberspace—to which they have added a sixth: the cognitive domain. Even in Western military science, the cognitive domain materializes as a distinct domain that molds how an adversary perceives information to gain knowledge and understanding. Using this analysis in combination with the concepts of informationized warfare and intelligentized warfare, the PLA has determined that warfare will further fall into two distinct realms: systems confrontation and systems destruction.

Systems Confrontation: The War Before the War

Systems confrontation is defined as "a contest among adversarial systems"[10] waged not only in the traditional domains of land, air, and sea but also in space, cyberspace, and even the psychological domain. This emerging domain encompasses the PLA's concept of *cognitive domain operations*, which expands on traditional psychological warfare using information to influence the adversary's thought processes, ranging from peacetime public opinion to wartime decision making,[11] as well as the Western notion of *cognitive warfare*, which expands the accepted continuum of warfare into how individuals perceive information to gain knowledge and understanding.[12]

Cognitive Warfare

While cognitive warfare lacks a widely accepted definition, initial proposals contain at least one of three common themes:

- The intent to influence specific individuals and groups on political matters, understanding that war is a continuation of politics by other means.[13]
- The explicit targeting of human cognition—how people perceive and interpret information to gain knowledge and understanding.[14]
- The use of psychology and advanced technologies to target individuals or groups precisely.[15]

Systems confrontation is a duel between opposing military operating systems, with the center of gravity being the information architecture. The destruction of key technological capabilities, weapons, and organized personnel can paralyze an enemy's operating system. An approach integrating land, sea, air, cyberspace, and space domains can render opposing information systems inoperable, thus achieving information dominance. Systems confrontation gives the PLA a better understanding of its adversaries, allowing it to find their weaknesses and counter their strengths. The PLA wants to infiltrate and probe its adversaries' human and technical systems for weaknesses.[16]

One example of these targeted intrusion activities is Operation Shady Rat (2006–2011), which targeted systems around the world, identified key information, and exfiltrated hundreds of terabytes of research data (technical, defense, infrastructure, and organizational) back to the PRC for exploitation and use.[17] Many experts believe the operation is still ongoing today.[18] Another example is the U.S. Office of Personnel Management data breach between 2013 and 2015. This data breach targeted security clearance records and compromised the personal information of over 21 million cleared U.S. federal employees and contractors.[19] The information acquired through such active cyberspace operations has furthered the PRC's technical capability to develop better weapons, disrupt or destroy key information technology infrastructure, and further develop human intelligence sources through influence and coercion using compromised personal data. Systems confrontation is "the war before the war," pervasive and ongoing. It strikes at the adversary's human, physical, and technical systems to develop them as targets in the event of a conflict.

Systems Destruction: Target and Destroy the Systems

Systems destruction intends to "disrupt, paralyze, or destroy the operational capability of the enemy's operational systems."[20] This goal is achieved through a mix of "kinetic and non-kinetic strikes against key points and nodes."[21] Systems destruction begins at the onset of open conflict with an adversary, taking advantage of the groundwork laid through systems confrontation. Systems destruction specifically targets four key areas:

- Information flow of the adversary's operational systems.
- Essential elements of the adversary's operational system (e.g., C2, reconnaissance, intelligence, and firepower assets).
- Operational architecture of the adversary's operational system (e.g., C2 network, reconnaissance network, intelligence network, or firepower network).
- "Time sequence and/or tempo of the adversary's operational architecture."[22]

Systems destruction targets these four areas with the intent to "undermine the operation system's own

'reconnaissance-control-attack-evaluation' process."[23]

Having described the PLA's possible future capabilities, let's examine its key target: the U.S. Army and its network modernization efforts.

U.S. Army Network Modernization

One of the most important (and targetable) of the U.S. Army's six modernization priorities is the modernization of its networks. These networks include command post mobility, secure wireless communications, cybersecurity, and edge computing.[24] The improvement and expansion of network capabilities will enable the U.S. Army to fight and win in a multidomain environment by maintaining peer and near-peer adversary communications and information technology overmatch in the next 5 to 10 years. This nests within the U.S. Army's intent to be "capable of conducting Multi-Domain Operations (MDO) as part of an integrated Joint Force in a single theater by 2028, and ready to conduct MDO across an array of scenarios in multiple theaters by 2035."[25]

Network Modernization Initiatives

- *Command post mobility* is the ability for a command post to quickly displace, move, and operate on the move, with the idea that the fight doesn't stop because the command post is moving. Ground forces need ruggedized, hardened, on-the-move equipment and ability networking. This means that the command post is small, adapts to any terrain, and is reliable in the face of unanticipated weather, power, and cyberspace conditions.[26]
- *Secure wireless communications* is a newer class of deployable, small wireless access systems that bring the benefits of classified wireless access to warfighters in the field. It allows warfighters to use commercial smartphones, tablets, and laptops to access classified information over Wi-Fi and 5G.[27]
- *Cybersecurity* is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. As an emerging warfighting domain, cyberspace has gained significance because it transcends and touches all other domains. The Department of Defense considers cyberspace to be at the same level as traditional land, sea, and air warfighting domains. With our ever-increasing use of the cyberspace domain and the expansion of connectivity and devices available to tactical forces, the requirement to secure and defend these networks from disruption and destruction is a top priority.[28]
- *Edge Computing* involves bringing computing capabilities to where the mission is in the field. It means that data does not have to travel back to a data center to be processed or analyzed. With the expectation that communications will be degraded from the start of large-scale combat operations, the Army wants to decentralize communications and make tactical networks function like forward data centers that will host situational awareness, mission command, and command and control applications and databases.[29]

People's Liberation Army: Countering U.S. Modernization

The PLA's demonstrated pervasive capabilities in technical collection, offensive and defensive cyberspace operations, open-source intelligence, and human intelligence make the U.S. Army's network modernization the most important and most targetable of its modernization priorities.[30] The PLA's doctrinal shift and its concentration on systems confrontation and warfare are direct challenges to our network modernization efforts, affecting all aspects of how the U.S. Army will conduct multidomain operations.

These efforts will directly affect how intelligence is collaborated, coordinated, and disseminated throughout the operational environment. The network is connected to every warfighting function, including intelligence; if it is degraded, disrupted, or compromised, our ability to provide situational awareness and timely intelligence to the commander in support of multidomain operations will be significantly degraded.

Avoiding Disruption and Countering People's Liberation Army Actions

Fortunately, Army network modernization is still in the early stages, and we know what the PLA is planning. At the operational and tactical levels, the Army must emphasize training on analog procedures for the military decision-making process and other intelligence warfighting function tasks, particularly during intelligence preparation of the operational environment, to ensure continuity in the event of disruption and as backups to our digital systems. Also, our tactical and operational forces should exercise and practice these analog tactics, techniques, and procedures at home stations, and they should be evaluated regularly at combat training centers on their use of analog methods across all warfighting functions.

While our systems are still in the developmental and early operational phases, we must emphasize cybersecurity for networked systems. We must also develop built-in, standalone, unplugged capabilities that allow systems to continue operations when the network is disrupted, compromised, or out of service.

Other remedies across the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy spectrum might include an aggressive mix of—

- Heightened operations security on developmental efforts (doctrine, organization, personnel, training, and policy).
- Expanded research into low bandwidth and stand-alone solutions that could relay content through proximity connects while disconnected (materiel).

- ✦ Low-signature communications systems that would allow connectivity to the network using high-frequency, wired, mesh, or other connectivity options (facilities and materiel).

Other actions could involve assisting host nations with cybersecurity for critical infrastructure such as networks, telecommunications, utilities, etc., as well as assisting in developing and refining analog tactics, techniques, and procedures. Providing this assistance will help avoid operational disruptions and maintain continuity of operations in the coalition environments.

Impact on the Warfighter

Operating in an environment where digital networks are vulnerable to disruption may limit the ability to communicate. Therefore, warfighters must train to fight across all warfighting functions in analog methods. Emphasize analog intelligence procedures to support the commander, learn to operate without connectivity, and understand that regular training with the analog options is necessary.

We need to explore and expand on the importance of the cognitive domain in relation to networks. We must broaden our awareness of the use of social media and other perception-generating systems and their influence on operations by both the PLA and the U.S. Army in the Indo-Pacific Region. As the cognitive domain becomes more significant, Army intelligence professionals must consider how perception influences operations before forward deployments.

Conclusion

Although the PLA seems to have a head start in its efforts to modernize and counter U.S. Army network modernization efforts, we must realize that much of what they have done is a product of replication and mimicry, with little or no a priori experience, effort, or research. The PRC's advanced persistent threat operations,[31] like Operation Shady Rat, might provide technical details, specifications, and other information about our network modernization activity, but their methods were compromised. However, we should not be complacent—we must recognize that our networks, however modernized they are, are under constant, advanced, persistent attack. Further research into low-bandwidth, stand-alone solutions and minimal signature communications that could serve as a survivable fallback must be developed. We also must plan for the disruption and denial of our networks and train on analog procedures as a contingency solution, allowing us to continue the multidomain fight. So, who wins the network modernization fight? The United States can by reinforcing analog procedures and working closely with coalition partners on communications, operations, and cyberspace security.

Now, let's review our notional scenario again, but this time, we'll incorporate the countermeasures we've discussed.

Coalition Forces Prevent Occupation of the Scarborough Shoal

Upon the commencement of the PLA's actions to take the Scarborough Shoal, the United States Army deploys training elements to work with the Philippine Army tactical and operational units to provide training on staff procedures and interoperability. At the same time, the United States sends cyber-focused advise and assist teams to review the Philippine national cyberspace infrastructure and local network surety. At their home stations, the U.S. Army and Marines emphasize using analog tactics, techniques, and procedures while working in digitally austere environments. As the PLA Navy's actions become more provocative, the GPS and radio communications of coalition forces on the eastern coast of Luzon are increasingly inaccurate and periodically disrupted. However, because the coalition forces have trained in alternative, analog methods, this is a minor inconvenience. United States military operational and tactical personnel and their Philippine counterparts work in coordination and engage the host nation's civilians, employing many of them to assist as interpreters and laborers, both skilled and unskilled. The PLA Navy's inability to intimidate the coalition forces results in an operational standdown and a pullback from the area around the Scarborough Shoal. In the aftermath, the Philippine president thanks the United States and requests the permanent basing of United States forces in the Philippines after a forty-year absence.

Endnotes

1. Andrea Chloe Wong, "The 2012 Scarborough Shoal Standoff: Analyzing China in Crisis with the Philippines," *Encounters and Escalation in the Indo-Pacific: Perspectives on China's Military and Implications for Regional Security*, NBR Special Report No. 108, ed. Oriana Skylar Mastro (Seattle, Washington: The National Bureau of Asian Research, 2024), 75.

2. Min Ye, "The Dragon's Gift: An Empirical Analysis of China's Foreign Aid in the New Century," *International Trade, Politics, and Development* 6, no. 2 (2022): 73-86, https://doi.org/10.1108/ITPD-06-2022-0010.

3. Department of Defense, JADC2 Cross-Functional Team, *Summary of the Joint All-Domain Command & Control (JADC2) Strategy* (Washington, DC, 2022), https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.

4. Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), iii, https://www.rand.org/pubs/research_reports/RR1708.html.

5. Department of the Army, Army Techniques Publication (ATP) 7-100.3, *Chinese Tactics* (Washington, DC: Government Publishing Office [GPO], 09 August 2021), 1-9–1-10. Change 1 was issued on 24 November 2021.

6. Department of the Army, ATP 7-100.3, *Chinese Tactics*, 1-10–1-11; and Department of State, *Military-Civil Fusion and the People's Republic of China* (Washington, DC, 2020), https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

7. Department of the Army, ATP 7-100.3, Chinese Tactics, 1-11.

8. Michael C. Horowitz and Lauren Kahn, "DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military," *Council on Foreign Relations* (blog), November 4, 2021, https://www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape.

9. Laura Silver and Christine Huang, "Key Facts About China's Declining Population," Pew Research Center, December 5, 2022, https://www.pewresearch.org/short-reads/2022/12/05/key-facts-about-chinas-declining-population/; and James McBride, Noah Berman, and Andrew Chatzky, "China's Massive Belt and Road Initiative," *Council on Foreign Relations* (blog), February 2, 2023, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

10. Engstrom, *Systems Confrontation and System Destruction*, ix.

11. Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief* 19, no. 16 (September 6, 2019), https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/.

12. Andrew MacDonald and Ryan Ratcliffe, "Cognitive Warfare: Maneuvering in the Human Dimension," *Proceedings* (U.S. Naval Institute) 149, no. 4 (April 2023), https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension.

13. Ibid. MacDonald and Ratcliffe's note consisted of commentary stating, "inclusion of the word 'political' distinguishes cognitive warfare from economic tools—such as targeted advertisements—that seek to influence behavior for profit."

14. Paul Ottewell, "Defining the Cognitive Domain," *Over the Horizon*, December 7, 2020, https://othjournal.com/2020/12/07/defining-the-cognitive-domain/.

15. Koichiro Takagi, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," *War on the Rocks*, July 22, 2022, https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/.

16. Engstrom, *Systems Confrontation and System Destruction*, ix.

17. Dmitri Alperovitch, *White Paper Revealed: Operation Shady Rat* (Santa Clara, CA: McAfee, 2011), http://graphics8.nytimes.com/packages/pdf/technology/mcafee_shadyrat_report.pdf.

18. "The Biggest Hack in History—Operation Shady Rat," Hacked.com, https://hacked.com/the-biggest-hack-in-history-operation-shady-rat.

19. U.S. Congress, House Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 114th Cong., 2d sess., H. Rep., https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

20. Engstrom, *Systems Confrontation and System Destruction*, iii.

21. Ibid.

22. Ibid., 18.

23. Ibid., x–xi; and Li Yousheng [李有升], Li Yin [李云], and Wang Yonghua [王永华], eds., *Lectures on the Science of Joint Campaigns*《联合战役学教程》(Beijing: Military Science Press [军事科学出版社], 2012), 74.

24. Charlie Kawasaki, "Four Future Trends in Tactical Network Modernization," Industry Insight, *Army AL&T*, (January-March 2019): 122-125, https://asc.army.mil/docs/pubs/alt/archives/2019/Jan-Mar2019_ArmyALT.pdf.

25. Department of the Army, *2019 Army Modernization Strategy: Investing in the Future* (Washington, DC: GPO, October 2019), 3, https://stratml.us/pdfs/AMS.pdf.

26. Kawasaki, "Trends in Tactical Network Modernization," 123-124.

27. Ibid., 124.

28. Ibid., 124-125.

29. Ibid., 125.

30. Department of the Army, Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations, 2028* (Fort Eustis, VA: TRADOC, 27 November 2018), https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

31. Advanced persistent threats are "stealthy cyberattack[s] in which a person or group gains unauthorized access to a network and remains undetected for an extended period. The term's definition was traditionally associated with nation-state sponsorship, but over the last few years we've seen multiple examples of non-nation state groups conducting large-scale targeted intrusions for specific goals." Sarah Maloney, "What Is an Advanced Persistent Threat (ATP)?" *Malicious Life* (blog), Cybereason, https://www.cybereason.com/blog/advanced-persistent-threat-apt.

LTC (Retired) Randie O'Neal is an intelligence professional with over 40 years of service to the U.S. Army as an officer and a contractor. After his retirement as a lieutenant colonel in 2014, he worked as a contractor for Program Manager-Saudi Arabia National Guard and U.S. Military Training Mission Saudi Arabia in support of training, modernization and transformation initiatives. He is currently a senior instructor for the Intelligence Analysis Committee at Ft. Huachuca, AZ. Notable assignments during his military career include as the all-source intelligence production section leader for Joint Task Force Panama (U.S. Army South) during Operation Promote Liberty; Commander, Company B, 104th Military Intelligence Battalion; G-2, 63rd Regional Readiness Command; Counterterrorism Mission Management Center team leader, National Security Agency; and as an advisor team leader and camp commander in support of the Headquarters, Iraqi Federal Police and the Kurdish Peshmerga Zeravani during Operations Iraqi Freedom and New Dawn.