

Red Diamond

Operational Environment & Threat Analysis



Volume 10, Issue 3

July - September 2019



Focus on

CHINA



Bits in the Wire:
Advancing Threats in
the Cyber Domain

**China's
Maritime
Militia**

Also:
Worldwide Equipment Guide (WEG)
Showcase and Updates

INSIDE THIS ISSUE



Competition in 2035: Training for Multi-Domain Operations in Competition with China 3



China's Belt and Road Initiative and Its Infamous Debt: More of a Threat than a Trap 8



China's Maritime Militia 11



Bits in the Wire: Advancing Threats in the Cyber Domain 20



The Combined Arms Battalion and Combined Arms Brigade: The New Backbone of the Chinese Army .. 27



Interview: Dennis J. Blasko, LTC, USA (Ret) 42



Film Review: Operation Red Sea 47



WEG Showcase 49



WEG Updates 51

ON THE COVER: Tiananmen Square

Source: Morio [CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>); https://commons.wikimedia.org/wiki/File:Tiananmen_Square_2016_April.jpg]

The *Red Diamond* newsletter presents professional information but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official US Army position and does not change or supersede any information in other official US Army publications. Authors are responsible for the accuracy and source documentation of the material that they reference. The *Red Diamond* staff reserves the right to edit material. Appearance of external hyperlinks does not constitute endorsement by the US Army for information contained therein.

Red Diamond access via:



<https://community.apan.org/wg/tradoc-g2/ace-threats-integration/>

OEE *Red Diamond* published by TRADOC G-2 Operational Environment & Threat Analysis Directorate, Fort Leavenworth, KS



Topic Inquiries:

Angela Williams (DAC), Branch Chief, Training & Support
Jennifer Dunn (DAC), Branch Chief, Analysis & Production

OE&TA Staff:

Penny Mellies (DAC) penny.l.mellies.civ@mail.mil	Director, OE&TA 913-684-7920
MAJ Megan Williams megan.r.williams.mil@mail.mil	MP LO
WO2 Rob Whalley Robert.Whalley297@mod.gov.uk	UK LO 913-684-7994
SGT Rodney Knox rodney.knox@defence.gov.au	AU LO 913-684-7928
Laura Deatrick (CTR) laura.m.deatrick.ctr@mail.mil	Editor 913-684-7925
Keith French (CTR) keith.a.french.ctr@mail.mil	Geospatial Analyst 913-684-7953

Angela Williams (DAC) angela.m.williams298.civ@mail.mil	Branch Chief, T&S 913-684-7929
John Dalbey (CTR) john.d.dalbey.ctr@mail.mil	Military Analyst 913-684-7939
Jerry England (DAC) jerry.j.england.civ@mail.mil	Intelligence Specialist 913-684-7934
Rick Garcia (CTR) richard.l.garcia.ctr@mail.mil	Military Analyst 913-684-7991
Jay Hunt (CTR) james.d.hunt50.ctr@mail.mil	Military Analyst 913-684-7960
Kris Lechowicz (DAC) kristin.d.lechowicz.civ@mail.mil	Intelligence Specialist 913-684-7922
Craig Love (CTR) craig.r.love4.ctr@mail.mil	Military Analyst 913-684-7974
Pat Madden (CTR) patrick.m.madden16.ctr@mail.mil	Military Analyst 913-684-7997
Jamie Stevenson (CTR) james.e.stevenson3.ctr@mail.mil	Military Analyst 913-684-7995
Marc Williams (CTR) james.m.williams257.ctr@mail.mil	Military Analyst 913-684-7943
Walt Williams (DAC) walter.l.williams112.civ@mail.mil	Intelligence Specialist 913-684-7923

Jennifer Dunn (DAC) jennifer.v.dunn.civ@mail.mil	Branch Chief, A&P 913-684-7962
Rick Burns (CTR) richard.b.burns4.ctr@mail.mil	Military Analyst 913-684-7987
Kevin Freese (DAC) kevin.m.freese.civ@mail.mil	Intelligence Specialist 913-684-7938
William Hardy (CTR) william.c.hardy26.ctr@mail.mil	Social Science Research Analyst 913-684-7901
Andrew Johnson (CTR) andrew.m.johnson7.ctr@mail.mil	Social Science Research Analyst 913-684-7956
Nicole Laster, PhD (CTR) nicole.m.laster.ctr@mail.mil	Social Scientist 913-684-7839
Anthony Mack (CTR) anthony.e.mack2.ctr@mail.mil	Military Analyst 913-684-7761
Brad Marvel (CTR) bradley.a.marvel.ctr@mail.mil	Military Analyst 913-684-7914
Dave Pendleton (CTR) henry.d.pendleton.ctr@mail.mil	Military Analyst 913-684-7946
Wayne Sylvester (CTR) vernon.w.sylvester.ctr@mail.mil	Military Analyst 913-684-7941

Competition in 2035:

Training for Multi-Domain Operations in Competition with China

By Andrew M. Johnson, OE&TA

This article is adapted from the TRADOC G-2 Operational Environment & Threat Analysis Directorate report *Competition in 2035: Anticipating Chinese Exploitation of Operational Environments*

Competition in 2035 Study

TRADOC G-2 Operational Environment and Threats Analysis Directorate (OE&TA) conducted a study to assess how China could exploit OEs during competition through 2035 to gain strategic advantage, especially in relation to the US. To achieve the study purpose, the following research questions were explored:

- *What conditions will likely shape the strategic environment in 2035?*
- *Of the conditions identified, which are conducive to exploitation by China?*
- *Based on our understanding of Chinese strategy, how and where might China exploit the identified conditions in 2035?*
- *What are the implications of the predicted Chinese exploitation for the US Army?*

The answers OE&TA developed to these research questions provided insight into how Soldiers, leaders, and units can and should shape training to best prepare to operate during competition with China.

Exploitable conditions across the strategic environment in 2035

The Army Multi-Domain Operations (MDO) concept introduces the idea of exploitation of conditions by adversaries across the competition continuum but stops short of identifying *what* conditions are exploitable.¹ OE&TA began its study by identifying pervasive conditions across the contemporary strategic environment. OE&TA then assessed which of the conditions that could be exploited would likely continue through 2035. Ultimately, OE&TA identified 24 strategic environment conditions that actors will likely exploit through 2035:ⁱ

- Persistent State of Competition
- Erosion of the Liberal World Order
- Multi-Polar World
- Fragile and Failing States
- New International Cooperation Models
- Use of Proxies

- Diverse Technology Actors
- Information Communication Technology Ubiquity
- Technology Access Gaps
- Technology-Reliant Societies
- Crypto-Technology Use
- Contested Spaces
- Competing Narratives
- Factionalized and Polarized Societies
- Effects of Urbanization
- Dominance of Cities
- Demographic Pressures
- Resource Competition
- Economic Inequalities
- Specialized Economies
- Interconnected Economies
- Infrastructure Capacity Challenges
- Climate Change
- Disease Evolution

The study excluded conditions that were less operationally relevant or were geographically limited.

At first glance, many of these conditions appear to have few or no tactical (or even operational) applications. However, ground manifestations of these conditions are familiar to Soldiers and leaders. Tactical and operational aspects of these conditions can be replicated in training scenarios and have been for nearly two decades. Although the US Army is transitioning focus from violent extremist organizations (VEOs) to “Great Power” or “near-peer” adversaries, the conditions have not changed. Regardless of the adversary (or adversaries), training and exercises should continue to replicate these conditions.

The key to replication is the scale of the condition in the scenario. For example, the condition “Economic Inequalities” should apply to a class or group of people, such as a minority group, a patron-peasant society/economy, or the divide between the population and an affluent political and/or military class. The difference from previous VEO-focused training scenarios is *how* the different adversaries would exploit these conditions. The US Army must understand multiple conditions and potential actions by multiple actors, decide how to deal with them, act/react to the conditions/actions, and then continue to do so in a continuous loop.

i. Conditions are listed here in loose groupings, and not in any order of importance. For definitions of all 24 conditions, please see page 7. For additional information, please consult the TRADOC G-2 OE&TA report *Competition in 2035: Anticipating Chinese Exploitation of Operational Environments*.

OE conditions consistently exploited by China for competitive advantage

OE&TA examined the future strategic environment conditions in the context of current and forecasted trends as well as Chinese strategy, interests, and capabilities.ⁱⁱ While China would likely exploit any of the 24 conditions if it can gain advantage, OE&TA identified four conditions that China consistently exploits, as well as examples of methods that China frequently employs in exploiting each of these conditions. Understanding this and training in scenarios replicating these conditions and methods reduces uncertainty and provides Soldiers, leaders, and units with insight into further potential Chinese actions.

Infrastructure Capacity Challenges are inadequacies of current systems to meet the needs/challenges of the population. China targets undeveloped and fragile environments where its capital investments, technology, and human capital can produce financial gains and generate political influence. *Example: China is funding major infrastructure projects under OBOR, which can give China access to, and in some cases control over, the systems it is developing.*

Interconnected Economies are economic systems that are linked to other economic systems. China seeks partners and opportunities to become a significant stakeholder in a wide variety of economies in order to capitalize on its investments as well as generate political influence. *Example: China produces electronics that become the base equipment for larger technology markets, and can provide access to associated data and technology.*

Specialized Economies are focused on a limited (niche) scope of goods and services within the global market. China looks for opportunities to partner with specialized markets and leverage their vulnerabilities for gain. *Example: China has employed predatory lending practices to exploit hydrocarbon-based economies for preferential access and continued influence.*

Technology Access Gaps exist as technological advancements and access vary globally and are primarily available to those with control of technology distribution and use. China gains partners, influence, and access to data and technology by targeting technologically underdeveloped areas. Its investments in technology and development of technology infrastructure provide partners with key resources and competitive advantages by filling technology gaps. *Example: OEs around the world benefit by having China-based companies establish operations internationally and improve their communications systems to 5G, which can provide China access to all data on those networks.*

Chinese application of the instruments of national powerⁱⁱⁱ during competition

China employs a whole-of-nation approach to competition and conflict, employing all instruments of national power. OE&TA case studies revealed several of China's preferred methods. Replicating these methods in training and exercises provides Soldiers, leaders, and units with practical experience of situations similar to those they will likely face in an OE with a Chinese competitive presence.

China's Strategic Objectives

Perpetuate CPC rule
Maintain internal security and stability
Sustain economic growth and development
Defend national sovereignty and territorial integrity
Maintain regional stability
Secure China's status as a great power
Safeguard interests abroad

Diplomatic

China employs a charm offensive with potential partners to gain economic influence by portraying itself as the "partner of choice." By 2035, China will have expanded its diplomatic influence through increasingly outward policies, making significant inroads with partners that are disillusioned or frustrated with the US. Diplomatic efforts are supported by, or supporting, the Information, Economic, and Financial instruments of power (see below).

Information

China will continue to employ the Information instrument of power in support of all actions and objectives in competition and conflict. Psychological Warfare and Public Opinion Warfare are two of China's "three warfares" (along with Legal Warfare, outlined below) which it uses to support all objectives and actions employing other instruments of power. Psychological Warfare uses propaganda, deception, threats, and coercion to affect the adversary's decision-making capability. Public Opinion Warfare disseminates information for public consumption to guide and influence public opinion and gain support from domestic and international audiences. Additionally, by 2035, China will make tremendous advances in innovative and disruptive capabilities, including cyber, artificial intelligence (AI), and machine learning. China will be a world leader in global information technology, despite protestations from the US and other Western countries over concerns of Chinese data access through its systems and equipment.²

ii. For case study analyses, please see the TRADOC G-2 OE&TA report *Competition in 2035: Anticipating Chinese Exploitation of Operational Environments*.

iii. Diplomatic, Information, Military, Economic, Financial, Intelligence, and Law Enforcement/Legal (DIMEFIL)

While deployed to areas of competition between the US, its partners, and China, Soldiers and leaders will likely experience aspects of China's "three warfares;"³ and therefore training and exercises should replicate aspects of each. While the Army has troops and units specializing in these methods and how to counter them, ALL Soldiers and leaders must understand and be able to recognize how China employs these measures. Army forces will likely deploy to areas saturated, if not dominated, by Chinese technology. INFOSEC, OPSEC, and other safeguards and countermeasures must be known, practiced, and implemented routinely to maintain integrity of US information and communications systems. Bare base /austere environment training will enable units to operate independent of host nation or partner systems, providing insulation from systemic Chinese access. Counter-Intelligence (CI) and cyber defense training is critical for all Soldiers, leaders and units in addition to integrating with those capabilities while training for and deployed in OEs with pervasive Chinese personnel and technology presence.

China's Three Warfares

Psychological Warfare uses propaganda, deception, threats, and coercion to affect the adversary's decision-making capability.

Public Opinion Warfare disseminates information for public consumption to guide and influence public opinion and gain support from domestic and international audiences.

Legal Warfare uses international and domestic laws to gain international support, manage political repercussions, and sway target audiences.

Military

China will use direct military power as a last resort, but is more likely to employ the PLA in a coercive and/or supporting role to other instruments of power. Beyond its primary role ensuring domestic security and stability throughout Chinese territory, China will continue to employ its military as a deterrent, to support promotion of China's global image, and to facilitate its economic and political objectives overseas. The military means China will use, and that US Army forces may likely encounter, include continuing to be a leading contributor of peacekeeping forces to the United Nations in areas of Chinese economic interests, providing non-uniformed security forces at investment/project sites in unstable areas, and conducting train, advise, and assist activities with potential partners of economic interest to China.

These forces and activities are easily replicated in training. Scenarios can be developed to present Soldiers, leaders, and units with dilemmas involving both overt and covert PLA presence. ROE must be developed and exercised to cover a Chinese presence of both military and "civilian" personnel and formations.

Economic

China will continue to rely primarily on the economic instrument of power to gain influence. By 2035, the "One Belt, One Road" (OBOR) initiative will have increased China's access and economic influence globally. China will have reduced its dependence on foreign energy by pursuing renewable and nuclear power, with most of its remaining energy imports originating in unstable areas such as Venezuela and central, eastern, and southern Africa. Chinese infrastructure development and trade transactions could result in Chinese personnel presence and access to—if not control of—infrastructure, systems, and materials. This is most likely in transportation and information infrastructure and energy and natural resources transactions. China's relationships and presence will likely influence partners and services, which could impact Army operations. Additionally, forced technology transfers and industrial espionage by Chinese companies and intelligence services will pose threats to partners and US entities alike.

As mentioned above, Army forces must train to expect and mitigate Chinese access and influence across many aspects of OEs where China is competing for advantage.

Financial

China uses the financial instrument of power in conjunction with the economic instrument of power to gain influence through loans and leveraging host nation debt. Financial pressure may be applied to host nation civilians, business, government, and security forces that can affect Army operations.

Intelligence

Chinese intelligence services are involved in military and industrial espionage to gain information as well as to clone and modify technology for the PLA and Chinese industry.

INFOSEC, OPSEC, and CI training for ALL Soldiers and leaders, along with integration of CI capabilities with deployed units, are necessary to mitigate the threat posed by foreign intelligence activities.

Law Enforcement/Legal

Legal Warfare is one of China's "three warfares." It uses international and domestic laws to gain international support, manage political repercussions, and sway target audiences. China employs legal warfare to manipulate

international institutions and conventions for its own benefit while in turn using them to hinder its adversaries.

Implications for the US Army

China will continue to gain global influence through the application of economic and financial power and exploitation of the information environment using its three warfares approach. It will leverage and shape the existing international system to advance its own interests while attempting to constrain others, including the US. Four specific implications apply to the US Army:

Traditional threat paradigms may not be sufficient for competition.

The US Army's threat paradigm emphasizes the *military* capabilities of state and non-state adversaries, but the US Army is likely to be confronted with adversaries executing a whole-of-nation approach during both competition and conflict. Generating an understanding of an adversary based on its military capabilities and capacity creates a critical gap in understanding the holistic threat from an adversary's intent and the full breadth of its capabilities. China demonstrates that adversaries of the future are not likely to engage in competition or conflict by relying on their military capabilities. They will seek to achieve competition objectives mainly through other instruments of national power.

The US Army's threat paradigm must account for this phenomenon in training, exercises, and operations. Army units should not assume that there are other USG elements capable of dealing with adversary actions. The Army must train to handle non-military actions that affect US interests, operations, and partners.

The US could be drawn into unanticipated escalation.

Persistent competition in 2035 will challenge how competitors observe, understand, act, and react to the actions of others. China is unrestrained by the same legal and ethical limitations as the US. Its actions in competition will skirt the threshold between competition and conflict, pushing boundaries in order to gain advantage. This creates the potential for unanticipated escalation due to miscalculation or misunderstanding. If China acts in the guise of competition but violates US Rules of Engagement (ROE) or law, it may invoke a response from US forces that crosses into conflict. Similarly, China may perceive or claim that US actions exceed those expected under competition, increasing the risk of conflict.

This potentially thin or opaque line between competition and conflict can be replicated through ROE and rule of law training. Scenarios can be

developed based on Chinese strategy, interests, and observed actions that will violate US ROE and/or US or international law.

China will likely undermine US Army military partnerships.

Undermining the partnerships of competitors is fundamental to Chinese strategy. China's economic and financial power in 2035 will enable it to limit or prevent partner involvement with the US through coercion or incentives. US partners may suddenly cancel or scale down scheduled training, logistics support, or operations based on pressures brought by China.

While US forces will not be dealing with China directly in this case, training on interaction dynamics with partner forces is critical.

The pervasiveness of Chinese goods, technology, infrastructure, and systems will increasingly impact US Army operations and engagements.

























By 2035, the US Army will increasingly have to work with partners and in OEs that are reliant on Chinese-supplied and/or controlled equipment, infrastructure, and systems. This may challenge compatibility with US systems and US sustainment of these systems. Some systems, particularly electronic and communications, are accessible to the PRC by design according to Chinese law. This will represent a threat to the availability, integrity, and confidentiality of US systems. US forces and partners could also encounter delays, disruptions, or denials of use of facilities and systems that are directly or indirectly controlled by Chinese entities.

INFOSEC and OPSEC scenarios can be woven into any training event, as can denial of service or facilities. Additionally, training to operate in bare base or austere environments prepares Soldiers, leaders and units for OEs with incompatible, unsecure, or otherwise unreliable infrastructure and technology.

Enduring Competition, Enduring Concern

The US Army will operate in a persistent state of competition with the "2+3" adversaries as well as countless other actors across OEs worldwide for decades to come. The Chinese ends, ways, and means and the implications for competition with China described above merit concern by Army leaders today and through 2035. However, these are only the most significant implications that resulted from the OE&TA study on Chinese competition. Simply learning about Chinese ways and means to achieve influence in competition and their implications is not sufficient. Soldiers, leaders, and units must incorporate these mostly non-military adversary actions into training and exercises to be able to deal with the variable aspects of a whole-of-nation approach to competition. Only then can the Army safeguard US interests in competition or conflict now and into the future. ♦

Table of strategic environment conditions and definitions.

ICON	CONDITION	DEFINITION
	Climate Change	Change in global or regional climate patterns resultant from the cumulative effects of global mean surface temperature increase.
	Competing Narratives	Explanations or interpretations of events/ideas originating from a particular perspective and presented to a target audience in order to gain influence.
	Contested Spaces	The physical, cognitive, or heterotopic spheres of competition.
	Crypto-technology Use	The utilization of encryption technology that enables increased security for the transmission and storage of data.
	Demographic Pressures	Factors within a population that reduce the ability of an environment to support that population.
	Disease Evolution	The emergence of new and/or evolved pathogens that impact the way people live.
	Diverse Technology Actors	Non-traditional technology leaders are emerging to compete with traditional technology leaders as new technologies emerge and are implemented globally.
	Dominance of Cities	Concentration of regional/global power in Census Metropolitan Areas (CMA), for example, CMAs may generate a majority of the GDP of a state.
	Economic Inequalities	Unequal distribution of income, wealth, and economic opportunity.
	Effects of Urbanization	Consequences associated with increasingly urbanized populations, for example, pollution, poverty, resource scarcity, etc.
	Erosion of the Liberal World Order	The shift of state and non-state actors from 20th century liberalism to a realist pursuit of self-interests ahead of collective interests, while ignoring or subverting existing international structures and norms.
	Factionalized and Polarized Societies	Societies characterized by increasing divisiveness as a result of conflicting or competing identities.
	Fragile and Failing States	A fragile state is characterized by weak state capacity or weak state legitimacy leaving citizens vulnerable to a range of shocks. A failing state refers to a political body disintegrating toward the point where basic conditions and responsibilities of a sovereign government no longer function properly.
	Information Communication Technology Ubiquity	Near universal access to information and communication around the globe.
	Infrastructure Capacity Challenges	Inadequacy of current systems to meet the needs/challenges of the population.
	Interconnected Economies	Economic systems that are linked to other economic systems.
	Multi-Polar World	A global environment where power is distributed among three or more significant poles (states), each with the ability to generate wealth and/or military capability that can/may threaten other interests and attract other actors into their spheres of influence.
	New International Cooperation Models	The development of new regionalized and specific cooperative agreements, relationships, and institutions that replace or challenge existing agreements, relationships, and institutions.
	Persistent State of Competition	Diverse transnational actors (states, cities, and nonstate actors including VEOs, criminal groups, MNCs, empowered individuals, etc.) compete through all instruments of power (Diplomatic, Information, Military, Economic, Financial, Intelligence, and Legal) and across all domains (Sea, Land, Air, Space, and Cyberspace).
	Resource Competition	Contest between actors to secure needed or desired resources.
	Specialized Economies	Economies focused on a limited scope of goods and services to gain an advantage within a market.
	Technology Access Gaps	Technological advancements and access will vary globally and be primarily available to those with control over its distribution and use.
	Technology-Reliant Societies	Societies are embracing and becoming increasingly reliant upon the digitalization of every aspect of their lives.
	Use of Proxies	Widespread use of surrogates by both state and nonstate actors to further their interests indirectly and with reduced direct risk.

1. TRADOC, *TRADOC Pamphlet 525-3-1: The U.S. Army in Multi-Domain Operations 2028*, Fort Eustis, VA: U.S. Army Training and Doctrine Command, 6 December 2018; Joint Staff, *Joint Doctrine Note 1-19: The Competition Continuum*, Washington, DC: Department of Defense, 03 June 2019.
2. The White House, *National Security Strategy of the United States of America*, Washington, DC, Dec 2017; James Mattis, *Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, DC: U.S. Department of Defense, January 20, 2018; Daniel Coats, *National Intelligence Strategy of the United States of America: 2019*, Washington, DC: Office of the Director of National Intelligence, 2019; Prashant Patel, *Competition Short of Armed Conflict* presentation to J39 Strategic Multilayer Assessment, 25 JAN 2019, slides 5-9, 17-18, 22; Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, Washington, DC: Defense Intelligence Agency, 2019, p. 11; Daniel Coats, "Statement for the Record, Worldwide Threats Assessment of the US Intelligence Community," Washington, DC: Senate Select Committee on Intelligence, 29 January 2019, 24; General Joseph L. Votel, "Statement of General Joseph L. Votel, Commander, U.S. Central Command, Before the Senate Armed Services Committee on the Posture of U.S. Central Command, Great Power Competition: The Current and Future Challenges in the Middle East," Washington, DC: US Senate, 5 February, 2019, p. 11; Lloyd Thrall, "China's African Interests and Strategic Perceptions," in

- China's Expanding African Relations: Implications for U.S. National Security*, Santa Monica, CA: RAND Corporation (2015); 9-20; General Thomas D. Waldhauser, "Statement of General Thomas D. Waldhauser, United States Marine Corps, Commander, United States Africa Command Before the Senate Committee on Armed Services," Washington, DC: US Senate, February 7, 2019, p. 9; Admiral Craig S. Fuller, "Posture Statement of Admiral Craig S. Fuller, Commander, United States Southern Command, Before the 116th Congress Senate Armed Services Committee," Washington, DC: US Senate, February 7, 2019, p. 1; Admiral Philip S. Davidson, "Statement of Admiral Philip S. Davidson, U.S. Navy Commander, U.S. INDO-PACIFIC Command Before the Senate Armed Services Committee on U.S. INDO-PACIFIC Command Posture," Washington, DC: US Senate, 12 February, 2019, p. 8.
3. "Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies," Report to Congressional Committees, Washington, DC: U.S. Government Accountability Office, December 2018, p. 13; Robert D. Kaplan, *The Return of Marco Polo's World and the U.S. Military Response*, Washington, DC: Center for a New American Security, May 2017, pp. 18, 24; Michael Fabey, *Relentless: China's Quest for Control* presentation to the J39 Strategic Multilayer Assessment, 31 JAN 2019; Michael J. Mazarr, et al, "Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives," *RAND Project AIR FORCE* Report, Santa Monica, CA: RAND Corporation, 2018, p. 18

China's Belt and Road Initiative and Its Infamous Debt: More of a Threat than a Trap

By **Jessica C. Liao**, Department of Political Science, North Carolina State University

The Belt and Road Initiative (BRI) has morphed into China's premier policy framework, both domestically and internationally, since its launch in 2013. China's top economic planning agency, the National Development and Reform Commission, released its first BRI action plan in 2015, and it has since updated and expanded BRI's geographic and financial scope. In 2017, during the 19th National Party Congress, BRI promotion was formally adopted into the Chinese Communist Party's (CCP) constitution. On these official documents, BRI is envisioned as an overarching infrastructure plan that links China with over sixty countries in Europe, Africa, and Asia at a cost of nearly \$8 trillion. Unsurprisingly, BRI has provoked a wave of China-threat sentiments due to its strategic

implications, with some comparing BRI to the Marshall Plan, others calling it Beijing's game changer, and many more urging Washington to aggressively counter BRI-engendered strategic and security challenges.

While the strategic threat is difficult to gauge given BRI's short life, this article discusses a different type of threat that is more immediate and affects not only BRI-participating countries, but also China itself, with potential consequences for the entire global economy: the debt threat. It is important to note that the debt threat described in this article is distinct from, if not in direct contradiction to, a common assumption of BRI as 'debt trap' diplomacy. Namely, Beijing extends credits at a level beyond debtor countries' ability to repay with the "malign" intent of extracting economic and political concessions. While this "debt trap" discourse provides useful propaganda points for China's

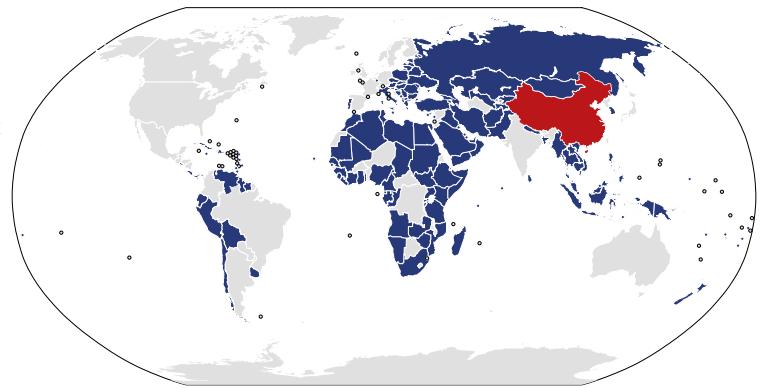
critics, it obscures reality by omitting two important facts: 1) Debtor countries must consent to Chinese loans, and Beijing cannot force Chinese money on other countries; and 2) loan defaults affect not just debtor countries, but China's fiscal health. This leads to the question, if pushing Chinese finance in developing countries is a risky foreign policy move, why does Beijing choose to do so?

To answer this question, one needs to understand China's system of statist capitalism. If infrastructure is an engine of growth and industrialization, debt financing fuels that engine. Nowhere in the world is public spending on infrastructure more important to economic development than in China. Infrastructure spending has been a centerpiece of China's public budget as well as a growth area for its state-owned enterprises (SOEs). Over the past three decades, China has been the world's largest infrastructure spender with rates of public investment to GDP of 15-20 percent, more than double developing countries' average and triple that of developed countries'. Until recently, China's infrastructure investment has supported high rates of economic growth. However, economic and social returns on infrastructure investment diminish sharply, if not go negative, when haphazard investment leads to overcapacity. This happened in China in the late 2000s when Beijing pushed through a \$590-billion stimulus package in response to the 2008 financial crisis. While creating a short-term boost, it caused severe overcapacity, particularly amongst Chinese SOEs. Beijing's response to this problem—coupled with shrinking global export markets, falling returns of China's holdings of US Treasuries, and strategic concerns driven by increased rivalry with the United States—were all important factors in Xi's decision to launch the BRI. In many ways, BRI is an outward extension of China's domestic infrastructure-led growth model, which Beijing hopes to replicate elsewhere while also reaping strategic and foreign policy dividends.

BRI may have appeared to Beijing as a clever, multi-functional strategy in 2013, but in 2019, it has become increasingly clear that BRI, in spite of its goal of promoting China's infrastructure export, has also spread China's overcapacity problems and other problems inherent in Chinese statist capitalism. BRI has generated significant growth in Chinese overseas lending for a wide range of infrastructure projects. At the first BRI Summit in mid-2017, two major policy banks, Export and Import Bank of China and China Development Bank reportedly extended \$200 billion of lending to BRI projects. In a recent interview, a Chinese central bank governor noted Chinese financial institutions have provided more than \$440 billion for BRI construction

projects.¹ Morgan Stanley has estimated China's overall BRI expenditures could reach \$1.2–1.3 trillion by 2027, though this number is subject to wide variation.² The majority of BRI projects are located in developing countries, with the China-Pakistan Economic Corridor being the largest one for an estimated cost of \$68 billion, covering various construction projects linking Southwest China to Pakistan's Gwadar Port.

It is true that BRI has helped some developing countries to reduce poverty and, to a certain extent, replicate China's infrastructure-driven growth. Ethiopia is an often-cited example as Addis Ababa over the past decade has spent about 15 percent of its GDP on public infrastructure, and in return, it has achieved annual growth rates around 9 percent. However, not all countries grow fast enough to service the incurred debt. Rather, rapid accumulation of foreign debt in certain BRI-participating countries has heightened their financial stress and sovereign default risks. According to a 2018 Center for Global Development (CGD)



Countries shown in blue have signed BRI cooperation documents.

Source: Owennson [CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>)], https://commons.wikimedia.org/wiki/File:Belt_and_Road_Initiative_participant_map.svg

study, debt-to-GDP ratios of 10-15 countries recently climbed above 50-60 percent—a common indicator of debt distress for developing countries—because of increased borrowing for BRI-related projects.³ Among these countries, eight are of particular concern because of the high ratio of Chinese debts to their total external debts. These countries are Djibouti, Kyrgyzstan, Laos, the Maldives, Mongolia, Montenegro, Pakistan, and Tajikistan. Some Chinese loans to these countries are at concessional rates, but others are close to prevailing market rates, which means higher default risk for borrowers. While some of these countries' BRI projects are complete, others, particularly big-ticket ones, are delayed or disrupted for various reasons. In short, massive capital injection to infrastructure sectors did not generate sufficient growth for these countries and instead pushed them towards increasing levels of fiscal distress.

Yet, to say Beijing actively seeks to exploit these countries in a long-term effort to gain strategic ground is somehow misleading. Rather, perverse incentives, moral hazard problems and the related “bailout culture,” and crony capitalism—problems fundamental to China’s statist capitalism—are reasons that are more evident for BRI-incurred debt problems. To start, many developing countries, prior to signing on to BRI, were already debt prone for reasons stemming from poor finance and macroeconomic management to political instability and bad governance. Being high-risk investment markets limited their access to international capital and was the reason they turned to China as a lending alternative in the first place. They were also drawn to China for its less stringent lending rules compared with western donors/lenders, i.e. lower feasibility threshold, lax social/environmental impact assessments, and little demand to reform their domestic political and economic systems. BRI, with its campaign-style loan expansion, added fuel to a simmering fire in many debt-prone developing countries, increasing their tendencies toward bad borrowing, and perpetuating the problem of unproductive investment.

Additionally, managers at Chinese SOEs often have political goals, rather than profitability, in mind when they make investment decisions. In this world of perverse incentives, Chinese SOEs have a tendency to compete through ‘outgrowing’ each other rather than being profit-oriented and are thus prone to excess growth, a key factor contributing to China’s domestic overcapacity. BRI in turn extends China’s overcapacity problems overseas as Chinese SOEs take their domestic incentives to compete for foreign markets. The repercussion of unproductive investments was on full display in Sri Lanka, where its government had to hand a Chinese developer the Hambantota port under a debt-for-equity swap because the port generated too little revenue to service its debt. Similar repayment stress has also appeared in Pakistan and Djibouti. As losses from international lending soared, coupled with China’s continued economic slowdown (due in part to the ongoing US-China trade dispute), Beijing is increasingly finding itself under financial stress. BRI-related lending fell sharply in 2018, compared to previous years. Similarly, Chinese President Xi, at the 2nd BRI Summit in May 2019, cautioned a prudent approach to BRI

and emphasized the importance of debt sustainability. While Xi likely recognized that China’s overzealous lending has led to public diplomacy blunders—as was the case in Sri Lanka—he also likely came to realize the heightening financial problem facing China since BRI’s launch. For both China and BRI borrowing countries, the 80s debt crisis in Latin America is a good reminder of how cheap and easy credit fueled a wave of infrastructure spending that not only harmed many countries’ fiscal condition, but also caused political and social turmoil so serious that it damaged the region’s long-term competitiveness.

BRI’s debt threat has important implications for US policymakers. First, it is important to understand the complex relationship between China and BRI borrowing countries. When the United States tells developing countries that Chinese money and BRI projects are not in their interest it comes off as patronizing. Developing countries are perfectly capable of calculating their interests, but often have minimal means to achieve desired ends. Second, viewing all Chinese investments as steps in Beijing’s long-range plan for world domination masks the real risks and vulnerabilities China has exposed itself to under Xi’s “go big” foreign policy. It also fails to account for the relative independence with which Chinese SOEs go abroad in search of profit and “political glory.” Although Xi has consolidated power, the old Chinese proverb that “heaven is high and the emperor is far away” remains true. This means Chinese firms, in pursuit of their own self-interest, will find ways to skirt Beijing’s rules, even at the cost of its overarching diplomatic and strategic goals. Finally, given the opaque nature of China’s domestic economy and its BRI projects, it is difficult, if not impossible, to fully comprehend the scale of Beijing’s BRI-incurred debt problems, and whether, or to what extent, debt loads might affect BRI borrowing countries, as well as China. Nonetheless, sovereign debt defaults spread contagion, often resulting in a rapidly unfolding financial crisis that affects the entire global economy. In this sense, rather than coming across as patronizing, the United States could focus resources on helping borrowing countries better understand and negotiate the terms of foreign financing deals and “too good to be true” Chinese loans. ♦

About the Author:

Jessica C. Liao is Assistant Professor of Political Science at North Carolina State University. Previously, she taught at George Washington University and was a Visiting Fellow at Monash University, Kuala Lumpur campus. She received her PhD in international relations from the University of Southern California and MA in Asia-Pacific and China Studies from National Sun Yat-Sen University in Taiwan. Her research focuses on Chinese foreign policy and East Asian politics. Her current project addresses China and Japan’s economic statecraft competition and infrastructure development in Southeast Asia.

1. Chen Jia, “Leveraging private funds prioritized in BRI projects,” *China Daily*, April 26, 2019. Link: <http://www.chinadaily.com.cn/a/201904/26/WS5cc20b24a3104842260b868c.html>
2. Morgan Stanley Research, Inside China’s Plan to Create a Modern Silk Road. March 14, 2018. Link: <https://www.morganstanley.com/deas/china-belt-and-road>
3. John Hurley, Scott Morris, and Gailyn Portelance, Examining the Debt Implications of the Belt and Road Initiative from a Policy Perspective, CGD Policy Paper 121, Center for Global Development, March 2018. Link: <https://www.cgdev.org/sites/default/files/examining-debt-implications-belt-and-road-initiative-policy-perspective.pdf>



China's Maritime Militia

By Richard L. Garcia, OE&TA

Introduction

It is no secret that China has been undertaking an unprecedented series of construction and land reclamation projects in the East China Sea and South China Sea, but what is notable is how China's Maritime Militia is used to protect its territorial ambitions. While there is no conclusive definition of the Chinese Maritime Militia (CMM)¹, in 2012 the Zhoushan garrison commander, Zeng Pengxiang, and the Mobilization Office described it concisely: "The Maritime Militia is an irreplaceable mass armed organization not released from production and a component of China's ocean defense armed forces [that enjoys] low sensitivity and great leeway in maritime rights protection actions."² One of the world's premier experts on China's Maritime Militia, Dr. Andrew Erickson, a Professor of Strategy at the US Naval War College China Maritime Studies says, "China's armed forces comprise of three major organizations, each with a maritime subcomponent that is already the world's largest such sea force by number of ships."³ These three separate organizations that make up China's Maritime force include the People's Liberation Army Navy (PLAN), China's Coast Guard (CCG) and the People's Armed Forces Maritime Militia (PAFMM). While the United States has the world's most powerful Navy—in that their vessels are larger, more technically advanced, and have superior weapon systems—the US and China's maritime fleets are largely the same size in terms of number of vessels. Combined, the People's Liberation Army Navy, China's Coast Guard, and China's Maritime Militia possess over 650 large vessels with military capabilities, whereas the US Navy, US Coast Guard, and US Military Sealift Command (MSC) combine for over 645 ships.⁴ What balances out the US advantage is the fact that a large majority of the US fleet (Navy and MCS ships) operates globally, whereas China's fleet operates regionally.

With a military strength of over 2,183,000⁵ personnel on active duty and 510,000⁶ serving as military reservists, China has the world's largest military and is quickly becoming one of the world's strongest maritime powers. China is not attempting to compete with the United States in terms of having a global maritime footprint, instead their maritime intentions are more along the lines of being able to deter outsiders from incursions into Chinese territorial waters, which they

consider the East China Sea, South China Sea, and the Yellow Sea. While China views these three seas as Chinese territory, in truth territorial waters only extend 12 nautical miles past land. Anything outside of 12 nautical miles is considered international waters; however, by claiming sovereignty on islands located in international waters, they can claim a 12 nautical mile buffer around those islands as Chinese territory. According to a recent 2019 study conducted by GlobalFirepower.com, the PLAN's Naval assets total 714 (1 aircraft carrier, 52 frigates, 33 destroyers, 42 corvettes, 76 submarines, 192 patrol vessels, and 33 mine warfare ships).⁷ This number will continue to increase due to China's drive to become the world's largest and most powerful naval force by 2030. Growing alongside the PLAN, China has the world's largest Coast Guard with, "more ships than those of all its regional neighbors combined: 225 ships over 500 tons capable of operating offshore and another 1,050-plus confined to closer waters, for a total of 1,275."⁸ When you consider the sheer size of the PLAN and the CCG, coupled with a Maritime Militia fleet that has over 200,000⁹ vessels, it is easy to see why China's maritime force has become an increasing threat to its regional neighbors.

Outside of China, very little is known about the Maritime Militia, but through Chinese open source documents, people like Dr. Andrew S. Erickson are shedding light on China's Maritime Militia and how it fits into China's strategic goals. The CMM can be summarized as a "state-organized, developed, and controlled force operating under a direct military chain of command to conduct Chinese state-sponsored activities."¹⁰ Along with Vietnam, China is one of the very few countries to have a Maritime Militia, which comprises of civilian fishing vessels that execute a variety of missions ranging from emergency response to protecting China's sovereignty claims. The CMM are an inexpensive force multiplier that plays a paramilitary role for the PLAN during peacetime and armed conflict. Blurring the lines between civilian ships and military ships, the maritime militia raises legal and political challenges in the law of naval warfare. While warships may engage civilian fishing vessels that assist enemy forces, the law of naval warfare protects coastal fishing vessels from capture or attack during armed conflict so long as they are not supporting the enemy.¹¹ Having the world's largest fishing fleet, China's

Maritime Militia not only complicates the battlespace, but it also obscures the decision making process of military leaders operating in the area. During the 2019 US and China Diplomatic and Security Dialogue press conference, Defense Secretary James Mattis stated, “We...discussed the importance of all military, law enforcement, and civilian vessels and aircraft-including those in the PLA Navy, the Chinese Coast Guard, and the PRC Maritime Militia to operate in a safe and professional manner in accordance with international law as we seek peaceful resolution of all disputes in the South China Sea.”¹² This was the first public statement by the Trump Administration or anyone in the higher echelons of the US Government that acknowledged that the Chinese Maritime Militia operating in disputed areas is problematic and will erode US and allied interest in the area.

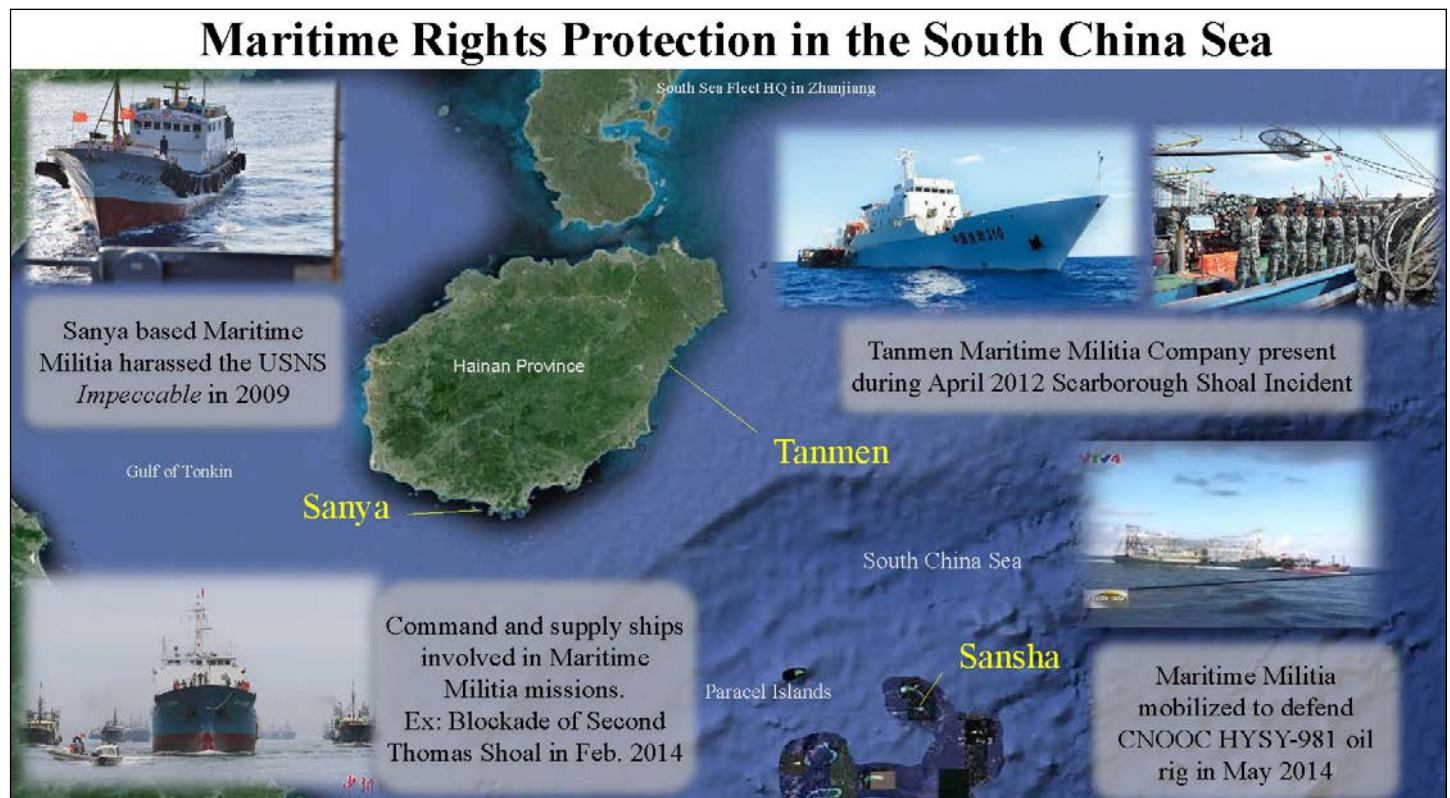
History

For hundreds of years, the law of naval warfare has always protected fishing vessels during armed conflict. During the Spanish-American War (21 April, 1898 – 13 August, 1898), a US Navy vessel captured two Cuban fishing vessels named the *Paquete Habana* and *Lola* which were attempting to return to Havana, Cuba. Both fishing vessels were stopped at the US blockade and were found to have no weapons or ammunition on board. Even though both vessels were nothing more than simple fishing vessels that were trying to return to port after a few days of fishing, the US

Navy seized both vessels. It took two years and the US Supreme Court to finally release the two vessels back to their rightful owners. During the US Supreme Court case of the *Paquete Habana* (175 U.S. 677) in 1900, the court’s ruling held that, “by ancient usage among civilized nations, beginning centuries ago, and gradually ripening into a rule of international law, coast fishing vessels, pursuing their vocation of catching and bringing in fresh fish, have been recognized as exempt, with their cargoes and crew, from capture as prize of war.”¹³ The International Humanitarian Law (IHL), which includes the Geneva Conventions, Hague Conventions, and Customary International Law, states that during times of war, civilians and civilian property should be protected at all cost. The purpose of the IHL is to define conduct and responsibilities between nations engaged in warfare, neutral nations, and non-combatants. In 1996, the International Court of Justice identified this rule as one of the two “cardinal principles” constituting the “fabric of humanitarian law.”¹⁴

“The first (principle) is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; states must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets.”¹⁵

Prior to the Chinese Communist Party (CCP) coming to power in 1949¹⁶, China had a militia system, but it wasn’t until the 1950s that China began to organize



Source: Conor Kennedy, "Maritime Militia: The Unofficial Maritime Agency," Maritime Security Challenges 2018 Conference, 2018, accessed June 4, 2019, <https://msconference.com/wp-content/uploads/2016/10/Kennedy-Maritime-Militia.pdf>, pg.8.

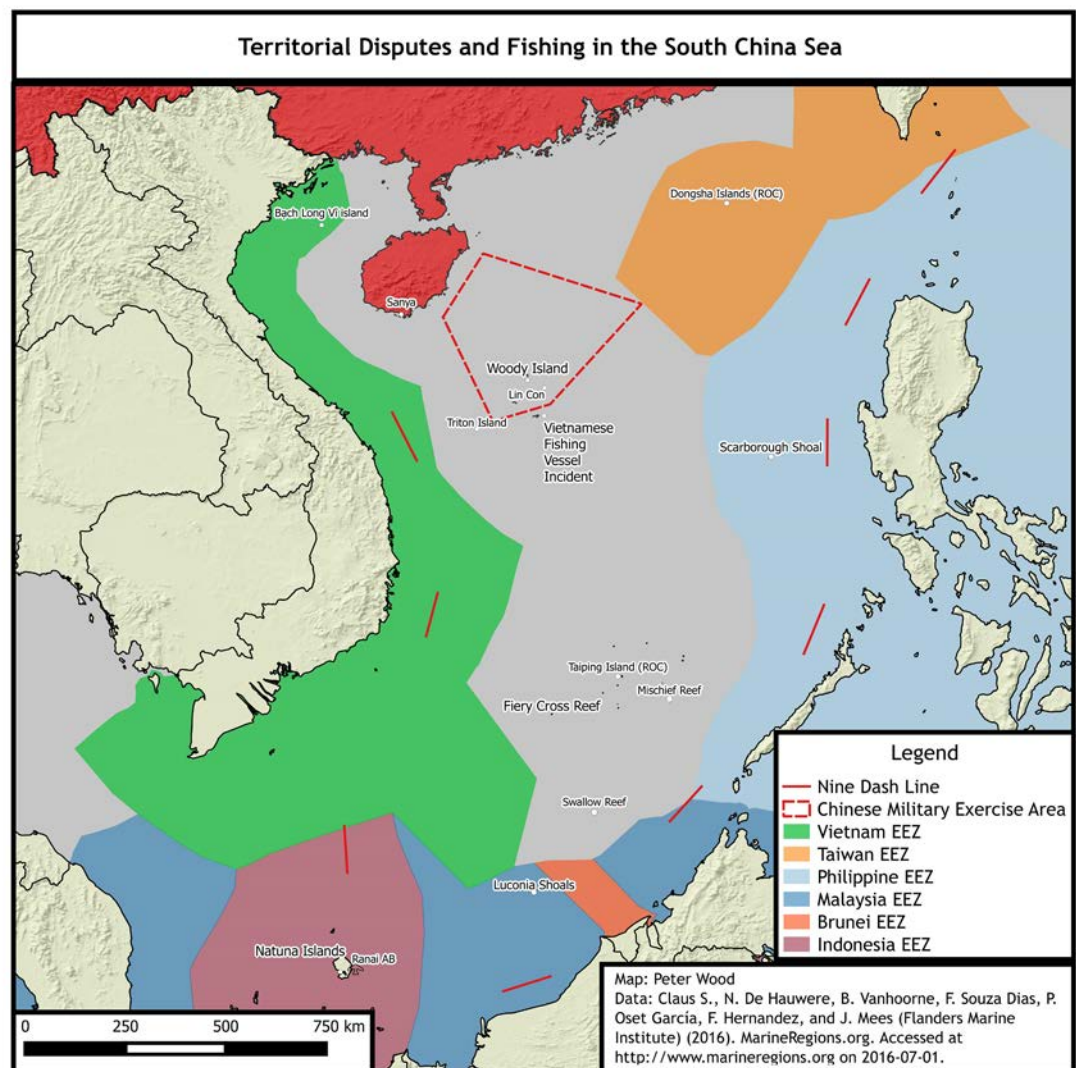
the maritime militias and establish individual units along the coastline. The CCP Maritime Militia initiative focused on establishing the CMM within the fishing communities, creating fishing collectives and work units, conducting political education, and enacting strict organizational control.¹⁷ While not all CMM missions are initiated by the PLAN, all missions require PLAN approval and once mobilized leadership falls to the local governments/military. Throughout their history, the Chinese Maritime Militia has played significant roles in a number of coercive incidents and military campaigns, including the 1950s support of the PLA's island seizure campaigns, the 1974 seizure of the western portion of the Paracels, the 2009 *Impeccable* incident, the 2011 harassment of Vietnam's survey vessels (*Viking II* and *Binh Minh*), the 2012 Scarborough Shoal standoff (Tanmen Militia present), and the 2014 *Haiyang Shiyou-981* oil rig standoff.¹⁸ Additionally, CMM was used in the South China Sea during the search for the missing Malaysia Airlines Flight 370 in 2014.

One of the most famous examples of how advantageous having a Maritime Militia can be for a nation, was seen during the 1964 Gulf of Tonkin (or U.S.S. *Maddox*) incident. During the second Indo-China War, the United States Seventh Fleet was patrolling the Gulf of Tonkin, an area located off the coast of southern China and northern Vietnam. During their patrol, the United States Navy's U.S.S. *Maddox* came across a few Vietnamese fishing vessels. Unbeknownst to the US Navy, the North Vietnam Maritime Militia was directed to report the position of any US warships operating in the area. Shortly after being seen by the Vietnamese fishing vessels, the U.S.S. *Maddox* was engaged by three North Vietnamese gunboats. After the incident, which led to the United States' entry into the Vietnam War, "a declassified National Security Agency study was

conducted and noted that a message was sent from an unidentified vessel to an unidentified shore-based shipping net control station,"¹⁹ shortly before the U.S.S. *Maddox* was attacked. While they lacked the technology the United States had during the time, North Vietnam understood the importance of the Maritime Militia and how they could be used as a force multiplier.

Role in Maritime Power

The US Navy has ships deployed throughout the world and the US Coast Guard primarily focuses on patrolling territorial waters (within 12 nautical miles of land), whereas China's maritime fleet has a much different mission set. By contrast, all three major Chinese maritime forces remain focused, first and foremost, on the contested near seas and their immediate approaches, close to China's homeland, land-based air and missile coverage and supply lines.²⁰ Since becoming the General Secretary of the Communist Party of China (CPC) in 2012²¹ and the President of the People's Republic of China (PRC) in 2013²², one of President's Xi Jinping's primary strategic goals has been for China to become a



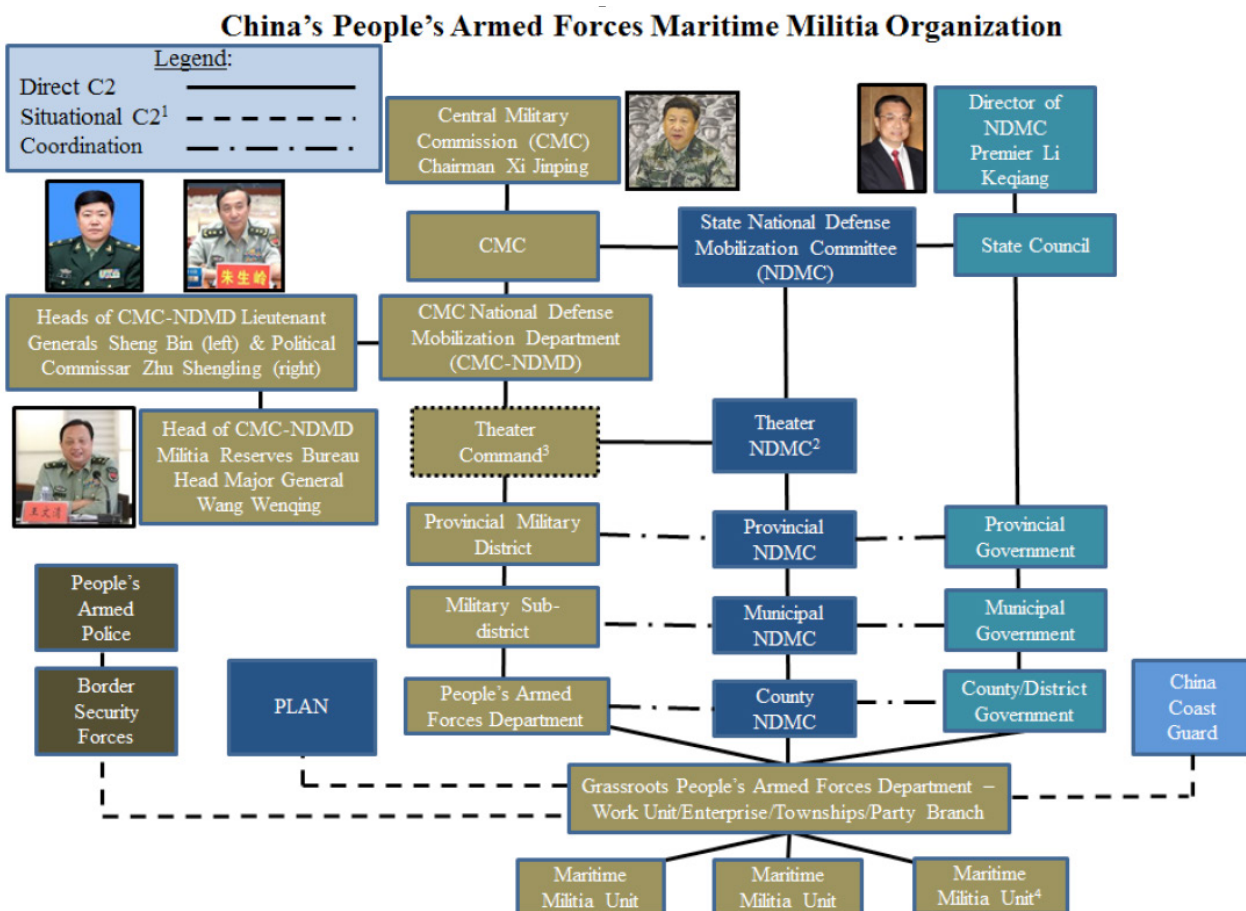
Source: Peter Wood, "China's Great Fishnet," The Jamestown Foundation, July 06, 2016, accessed June 4, 2019, <https://jamestown.org/program/chinas-great-fishnet/>, pg.1.

great maritime power. In order to meet this goal, China must not only look to modernizing and increase the size of the PLAN and CCG fleet, but also the Maritime Militia. This modernization strategy is upgrading and outfitting PLAN, CCG and CMM ships with state of the art radars; global positioning systems; lethal and non-lethal weapons systems; interceptor boats; helicopters; and Command, Control, Communications Computers, and Intelligence (C4I) suites.

The primary role of China's Maritime Militia is to act as an additional reserve force that supports China's military forces as needed, and acts as an independent force capable of performing a variety of conventional and unconventional missions. CMM missions include, but are not limited to: emergency and medical response, blockade operations, sovereignty claims, logistical support, navigational assistance, emergency repairs, fuel and material replenishment at sea, and surveillance and reconnaissance operations.²³ The CMM's secondary role is to provide domestic security forces by supporting the Chinese Coast Guard, assisting the Maritime Law Enforcement (MLE), and acting as a rapid rescue response.

Command and Control

The PLAN has operational control over the Maritime Militia. Through the CMM, China is expanding its operational control and influence without using conventional naval forces. The Command and Control (C2) of China's Maritime Militia falls under a dual military-civilian structure, with both Government/Party officials and military leaders having overall responsibility over the CMM. In fact, some of these leaders hold dual positions in both the military and government. This dual-leadership system starts at the Provincial Military District (MD) level and goes down to the township/country People's Armed Forces Department (PAFD) level.²⁴ What brings together the military and government into one decision-making body is the National Defense Mobilization Committee (NDMC), which organizes, issues orders, and coordinates mobilization of the maritime militia. At the national level, the State NDMC is led by the Central Military Commission (CMC) and State Council, and an NDMC is formed at each corresponding military and government leadership level from the province down.²⁵ Within this system is the authorization by the National People's Congress Standing Committee and general secretary to activate national or local mobilization, with



Source: Conor M. Kennedy and Andrew S. Erickson, *China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA*, report no. 3-2017, China Maritime Studies Institute Center for Naval Warfare Studies US Naval War College, US Naval War College, March 2017, accessed May 21, 2019, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1000&context=cmssi-maritime-reports>, pg.6.

the State Council and CMC submitting mobilization policies and plans for approval by the Standing Committee.²⁶ The chairman of that level's NDMC is the local government leader, with the local party secretary ensuring party control and serving as the first chairman. Serving as the executive chairman is the local military commander, with other government deputy leaders serving in vice chairman positions.

The NDMC system allows military-civilian joint command structures, such as the one operated by Nigde City, which is a “one-committee, two-headquarters” command structure, with the NDMC as the committee overseeing a “support the front” mobilization headquarters and a people's air defense headquarters.²⁷ Mobilization orders are initiated at the CMC or State Council level, with the General Staff Department's Mobilization Department responsible for supervising the maritime military work and establishing policies and regulations. Funding for the militia comes from both central and provincial governments. Because of this, local governments can activate the Maritime Militia for maritime rescues, natural disasters, or any other local emergency. Training and overall management of the militia falls to the local command structure consisting of government and military officials. Due to the fact that the CMM works with non-military forces and they are widely dispersed, the command and control structure is much more complex than a land based militia.

Xu Haifeng, the Provincial Military District Mobilization Division Chief, explains the command relationship of the Maritime Militia as the following:

- Units independently conducting intelligence gathering and reconnaissance at sea are commanded directly by the MD system.
- Emergency response units are organized by the local government or search and rescue agencies with MD participation.
- Rights protection units report to a command organized by their MD and relevant agencies, under the unified leadership of local government and party officials.
- Units involved in law enforcement missions are commanded by the CCG with the cooperation of their MD, under the unified leadership of local government and party officials.
- Units involved in supporting naval missions will be under the unified command of the PLAN with cooperation by the MD.²⁸

Training & Organization

Since 2002, President Xi Jinping and other Chinese leaders have made a concerted effort to not only increase the size of the PLAN, but increase the size of the CCG and the CMM. With a fishing fleet that employs more than 14 million people—25 percent of the world's total fishing population²⁹—what makes China's Maritime Militia unique is that it is state funded, locally organized and trains alongside the military. While most militias are seen as land based fighting units, China began to shift their militia towards the non-ground force services in 2007 when the “Militia Military Training and Evaluation Outline” was released by the General Staff Department. This regulated the CMM's possible evolution into a reserve force for the PLA, PLAN, PLA Air Force (PLAAF), Second Artillery Force (SAF)-renamed the PLA Rocket Force (PLARF), and the Strategic Support Force (PLASSF), and elevated the CMM into the status as a sixth military organization on 1 January 2016.³⁰ With this shift in supporting all of China's military services, as opposed to just the PLAN,



Sansha Maritime Militia receiving weapons training from the Hainan Provincial Military District

Source: Conor M. Kennedy and Andrew S. Erickson, “Hainan's Maritime Militia: A Standing Vanguard,” *The Maritime Executive*, March 30, 2017, accessed June 04, 2019, <https://www.maritime-executive.com/features/hainans-maritime-militia-a-standing-vanguard.pg.1>.

the CMM units were better organized, more flexible, and trained to carry out specific missions that support the needs of China's national defense. In an effort to promote China's strategic interest in the oceans, the Maritime Militia are assigned to collectives or attached to civilian companies and receive military and political training throughout the year.³¹ The building of a militia unit falls to the local civilian government and the local PAFD, together they are responsible for providing equipment, weapons, training, and political education to the militia members. Some of this training includes, but is not limited to: navigation, ship identification, firefighting, medic training, military customs and

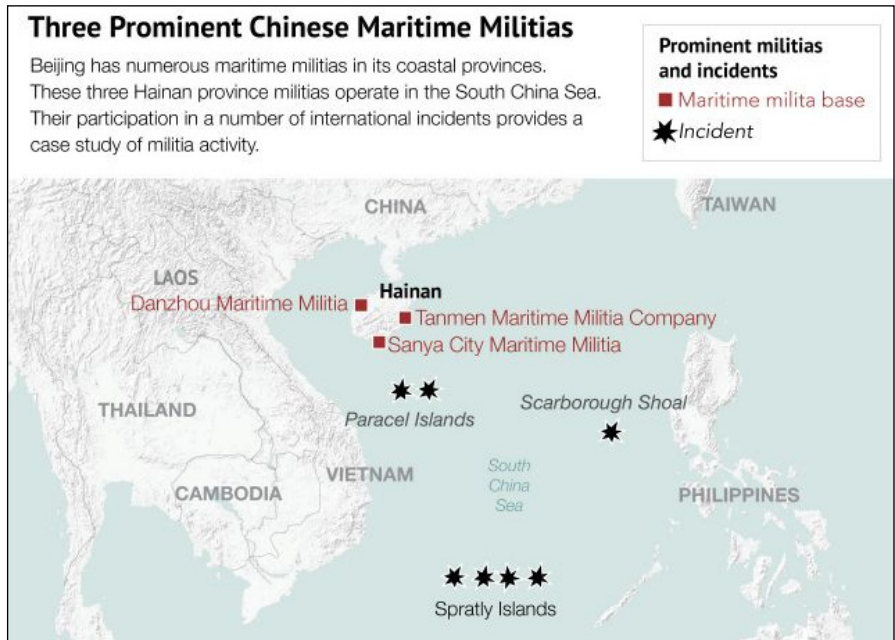
courtesy, civil defense, political indoctrination, and military weapons training. The Maritime Militia is funded by both the local city government for normal day-to-day operations and the provincial government for large exercises or specific missions. As per the mobilization rules, any cost associated with a militia mission or damage that occurs to a ship is compensated and repaired by the government. In an effort to convince the Maritime Militia to venture further out to sea in order to protect China's sovereignty claims and provide intelligence on foreign vessels, local governments have begun to subsidize the fuel for the vessels when they are on a sanctioned CMM mission.

Some of the more elite maritime militia units are fishermen in name only and have no fishing responsibilities. Recently, there has been a push to recruit ex-military personnel into the CMM and station them on vessels with mounted water cannons, lethal and non-lethal weapons, and reinforced hulls for ramming. Deployed to contested areas, these new elite maritime militia units expand China's influence and control over strategically important areas without resorting to war, a classic case of "winning without fighting."³² While most of the CMM men are fishermen with some military and political training, it is not uncommon to see active duty PLAN personnel on Chinese fishing vessels, especially near areas where disputed sovereignty claims exist. The Maritime Militia not only looks to ex-military when recruiting new members, but they also look to the universities when selecting CMM members who will train as reporting specialists. CMM reporting specialists are trained in collecting intelligence at sea, vessel target identification, collection methods, operation of the Maritime Militia vessel management platform and the Beidou notification terminal.³³ In recent years, this process of recruiting and training for a specific job within the Maritime Militia has reduced the uncertainty of military and political leaders ashore regarding the quality of the information they are being provided.

Implications

China has the world's largest fishing fleet and as part of their plan to become one of the world's most powerful maritime forces, they will deploy the Maritime Militia in unconventional ways and use it for intelligence gathering and a real time targeting apparatus at sea. During a visit to Qionghai City in the Hainan Province, President Xi Jinping met the local CMM and told

them, "Maritime Militia members should not only lead fishing activities, but also collect oceanic information and support the construction of islands and reefs."³⁴ President Xi Jinping went on to praise the work they were doing in protecting China's sovereignty claims in the East China Sea and South China Sea. Not only has the support for the Maritime Militia increased, so too have the annual financial resources for training, equipment, and even new state owned fishing vessels. In the past, most fishing vessels were privately owned or company owned, but after seeing how versatile the Maritime Militia is, the state began to purchase new fishing vessels for specific missions. Replacing the older



Source: Stratfor Enterprises, "Why China Is Arming Its Fishing Fleet," Stratfor, June 16, 2016, accessed June 04, 2019, <https://worldview.stratfor.com/article/why-china-arming-its-fishing-fleet>.

wooden hulled fishing ships, many of the newer ships are being built with steel hulls which not only allows them to sail in rougher seas, but also gives them the ability to ram smaller ships.

Peacetime

During peacetime, China uses the CMM as a non-military presence in contested areas such as the South China Sea and East China Sea. With overlapping maritime claims with Indonesia, Brunei, Vietnam, Malaysia, and the Philippines, China's Maritime Militia acts as a powerful non-kinetic method of coercion to dominate the seascape without the risk of open conflict.³⁵ This same Maritime Militia strategy is also being conducted near the Senkaku Islands in the East China Sea, where both China and Japan lay claim to the islands. From China's perspective, sending the Maritime Militia rather than military warships to maintain a presence near the Senkaku Islands greatly reduces the

likelihood of an international incident. While Japan would prefer to not have any Chinese vessels in the area, from their perspective it is much better to have fishing vessels operating in and around the Senkaku Islands, than military warships. In addition, due to overfishing and an increasing population, China is having to expand its fishing zones and is using the CMM as a quasi-military force that intimidates fishing vessels from other nearby foreign countries. China has already broken a number of international fishing agreements by overfishing not only their territorial waters (12 nautical miles past land), but also overfishing the Exclusive Economic Zones (EEZ), which extend out to 200 nautical miles past land. Part of the reason that China is funding the new upgraded CMM fishing vessels with steel hulls, rather than wood hulls is due to the distances their fishing fleet must now travel to fish. Not only are China's government and military leaders optimistic about the future of the CMM, so too are the leaders within the fishing industry. In June of 2012, He Jianbin, the chief of the State-run Baosha Fishing Corporation in Hainan province, encouraged the government to transform Chinese fishing vessels and their crews into a militia for the PLAN:

"If we put 5,000 Chinese fishing ships in the South China Sea, there will be 100,000 fishermen And if we make all of them militiamen, give them weapons, we will have a military force stronger than all the combined forces of all the countries in the South China Sea. Every year, between May and August, when fishing activities are in recess, we should train these fishermen/ militiamen to gain skills in fishing, production and military operations, making them a reserve force on the sea, and using them to solve our South Sea problems."³⁶

Wartime

Known as the "People's War," the integration of the military and civilian forces is the foundation of China's Maritime Militia. During wartime, China can deploy a combination of military and CMM vessels to an area, which would, "flood the zone with activity, confusing and complicating opponents' intelligence collection and targeting capacity."³⁷ China does have sophisticated satellite imagery, but there is no substitute to having a forward deployed asset that can provide up to the minute targeting data and intelligence. What appears to be an innocent civilian fishing vessel sailing around in international waters, is actually a hi-tech forward observer that can provide real-time targeting data for Anti-Ship Missiles (ASM) located thousands of miles away. Sailing in and around an area of operation, the

Major Operation Types in China's Echelon Defense Strategy			
Dispute Type	Operation Type	Primary Function(s)	Surface Fleet Action
Island sovereignty	Sovereignty patrol	Manifest China's claims; collect intelligence	Sail to waters surrounding a disputed feature
	Blockade	Enforce China's claims	Prevent foreign access to a disputed feature
Maritime rights	Tracking and monitoring	Manifest China's claims; collect intelligence	Follow foreign vessels operating "illegally" in Chinese-claimed waters; urge them to leave
	Obstruction and eviction	Enforce China's claims	Use nonlethal measures to force foreign vessels to cease "illegal" activities and depart Chinese-claimed waters
	Escort	Enforce China's claims	Use nonlethal measures to prevent foreign vessels from obstructing the "legal" operations of Chinese civilians in Chinese-claimed waters
Both	Support and cover	Discourage escalation; collect intelligence	Sail to and linger in disputed waters; signal a threat to use force to protect Chinese vessels; be prepared to act on that threat

Source: Ryan D. Martinson, *Echelon Defense: The Role of Sea Power in Chinese Maritime Dispute Strategy*, report no. 2-2018, China Maritime Studies Institute, US Naval War College, 2018, accessed June 4, 2019, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1014&context=cmsi-red-books>.

Maritime Militia would severely reduce the ability of the US and its allies to identify the enemy, and could also divert attention away from PLAN vessel movements and conceal China's true intentions on the battlefield. Dr. Erickson wrote in an Indo-Pacific Defense Forum, "Not seeking war but determined to change the status quo coercively, Beijing employs its enormous second and third sea forces in the so-called maritime gray zone operations to further its disputed sovereignty claims in the near seas (Yellow, East and South China seas)."³⁸ With a CMM fleet of over 200,000 vessels and the ability to sail not as combatants, but rather civilians, the Maritime Militia can execute wartime missions like no other force can.

China's Maritime Militia Operational Variables Implications

The foundation to developing an appropriate Operational Environment (OE) for any training exercise is the eight operational variables that exist in all OEs. Capable of replicating any OE that the United States force may encounter along the full spectrum of conflict, these operational variables are flexible and scalable.³⁹ These eight important operational variables are: Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT). When identifying any asset with unique capabilities such as China's Maritime Militia, exercise planners must take into account the implications of this new capability on all of the operational variables and how those implications affect the overall operational environment.

Political:

- A powerful non-kinetic method of coercion to dominate the seascape without the risk of open conflict in areas with overlapping maritime claims with Indonesia, Vietnam, Malaysia, Brunei, and the Philippines.⁴⁰
- Blurs the lines between civilian ships and military ships (International Humanitarian Law), raising legal and political challenges in the law of naval warfare

Military:

- A state-organized, developed, and controlled force of over 200,000 civilian vessels operating under a direct military chain of command to conduct Chinese state-sponsored activities.
- Acts as an additional reserve force that supports China's military forces as needed, and acts as an independent force capable of performing a variety of conventional and unconventional missions.

Economic:

- An inexpensive force multiplier that can provide logistical support, navigational assistance, emergency repairs, fuel and material replacements at sea, and act as a paramilitary force.
- All the nations that claim sovereignty in the contested areas do so because of the immense hydrocarbon resources, oil and natural gas, underneath the South China Sea, which is needed to satisfy the world's ever-increasing energy demands.
- The South China Sea serves as the artery that provides life to Japan and many other Asian countries, and any disruption to shipping due to CMM conflicts would cause repercussions throughout the world.
- Funded by both the local city government for normal day-to-day operations and the provincial government for large exercises or specific missions.

Social:

- Indoctrinates fishing communities with strict organizational control, military training, and political education.
- Provides domestic security forces by supporting the Chinese Coast Guard, assisting the Maritime Law Enforcement (MLE), and acting as a rapid rescue response.

Information:

- Real time intelligence gathering, reconnaissance, and vessel target identification at sea.

Infrastructure:

- Protects China's sovereignty claims and helps establish a Chinese footprint on islands and territorial waters in contested areas.

Physical Environment:

- Floods the physical environment with activity, confusing and complicating opponents' intelligence collection, decision making process, and targeting capacity.⁴¹

Time:

- The CMM offers China the ability to forward deploy civilian vessels throughout the operational environment, where they can provide up to the minute targeting data and intelligence.
- Increased energy requirements by the PRC and other Asian countries require the immediate deployment of the CMM in order to secure and protect the hydrocarbon resources found there.

Training Implications

Trainers at the CTC's and home station need to account for China's Maritime Militia and how the PRC uses it in a variety of unorthodox methods during peacetime and wartime. It is recommended that CTCs look to integrate the full spectrum of capabilities that a Maritime Militia brings to an Opposing Force (OPFOR) and how those capabilities affect the OE. China's Maritime Militia's ability to collect real-time intelligence and target data, conduct reconnaissance, safeguard sovereignty claims, and obscure the operational environment must be taken into account. Internally, the TRADOC G2 Operational Environment and Threat Analysis Directorate (OE&TA) will need to update the Decisive Action Training Environment (DATE) Worldwide Equipment Guide (WEG) to better represent China's Maritime Militia capability. Some of these updates will include the different types of CMM vessels, onboard equipment and weapons, and their support capabilities.

Conclusion

With very little risk or cost to China, the Maritime Militia will continue to expand China's control over strategically important territory and territorial waters. Professor James Kraska, a research director in the Stockton Center for the Study of International Law, US Naval War College notes, "as a force multiplier, the

maritime militia poses an operational challenge that requires an expansion in US and allied force structure, including warships, submarines and, especially, unmanned drones and unmanned subsurface vehicles, to manage the threat.”⁴² As part of an effort to counter China’s Maritime Militia threat, it is important to reveal publically who they are and what their true intentions are. Leading this charge is the U.S Naval War College’s China Maritime Studies Institute, which has published numerous reports and articles on the CMM, causing US leaders to take notice. Additionally, Dr. Erickson believes to deter the CMM’s harmful activities, the US

and its allies should: educate the Commanders and Vessel Masters operating in the contested areas; modify the Rules of Engagement (ROE); treat China’s three sea forces as one; and hold China to international standards of seamanship (Rules of the Road) and the International Humanitarian Law.⁴³ During peacetime, China’s Maritime Militia serves a valuable role in conducting reconnaissance, intelligence gathering, and protecting China’s sovereignty claims. However, it is during wartime that the CMM has its greatest effect, serving as a force multiplier for the PLAN and blurring the line between enemy combatants and civilians. ♦

1. Also called the People’s Armed Forces Maritime Militia. For this article we will refer to them as China’s Maritime Militia (CMM).
2. Andrew S. Erickson and Conor M. Kennedy, “Meet the Chinese Maritime Militia Waging a ‘People’s War at Sea,’” *The Wall Street Journal*, March 31, 2015, accessed May 21, 2019, <https://blogs.wsj.com/chinarealttime/2015/03/31/meet-the-chinese-maritime-militia-waging-a-peoples-war-at-sea/>, pg. 2.
3. David Axe, “Watch Out, U.S. Navy: China Has 650 ‘Vessels with Military Capabilities,’” *The National Interest*, May 15, 2019, accessed May 21, 2019, <https://nationalinterest.org/blog/buzz/watch-out-us-navy-china-has-650-vessels-military-capabilities-57652>, pg. 2.
4. Axe, “Watch Out, U.S. Navy,” pg. 4.
5. Global Firepower.com, “2019 China Military Strength,” *Global Firepower - World Military Strength*, 2019, accessed May 23, 2019, https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=china#navy.
6. Ibid.
7. Ibid.
8. Axe, “Watch Out,” pg. 3.
9. James Kraska, “China’s Maritime Militia Upends Rules on Naval Warfare,” *The Diplomat*, August 10, 2015, accessed May 23, 2019, <https://thediplomat.com/2015/08/chinas-maritime-militia-upends-rules-on-naval-warfare/>, pg. 2.
10. Conor M. Kennedy and Andrew S. Erickson, China’s Third Sea Force, The People’s Armed Forces Maritime Militia: Tethered to the PLA, report no. 3-2017, China Maritime Studies Institute Center for Naval Warfare Studies U.S. Naval War College, U.S. Naval War College, March 2017, , accessed May 21, 2019, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1000&context=cmsi-maritime-reports>, pg. 2.
11. Kraska, “China’s Maritime Militia,” pg. 3.
12. Andrew S. Erickson, “Shining a Spotlight: Revealing China’s Maritime Militia to Deter Its Use,” *The National Interest*, November 26, 2018, accessed May 21, 2019, <https://nationalinterest.org/feature/shining-spotlight-revealing-china-s-maritime-militia-deter-its-use-36842>, pg. 3.
13. Ibid.
14. Legality of the Threat or use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. in James Kraska and Michael Monti, The Law of Naval Warfare and China’s Maritime Militia, report no. 91 Int’l Stud. 450 (2015), International Law Studies, U.S. Naval War College, 2013, accessed May 21, 2019, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1406&context=ils>
15. Ibid.
16. The Editors of Encyclopedia Britannica, “Chinese Communist Party,” *Encyclopedia Britannica*, July 18, 2016, accessed May 24, 2019, <https://www.britannica.com/topic/Chinese-Communist-Party>.
17. Bruce Swanson, Eighth Voyage of the Dragon: A History of Chinas Quest for Sea power (Annapolis, MD: Naval Institute Press, 1982). pg.47.
18. Andrew S. Erickson and Conor M. Kennedy, “China’s Maritime Militia,” *CNA Analysis & Solutions*, 2016, accessed May 23, 2019, https://www.cna.org/cna_files/pdf/Chinas-Maritime-Militia.pdf, pg. 3
19. Kraska, “China’s Maritime Militia,” pg.1.
20. Axe, “Watch Out,” pg. 4.
21. Melissa Albert, “Xi Jinping,” *Encyclopedia Britannica*, March 19, 2018, accessed May 28, 2019, <https://www.britannica.com/biography/Xi-Jinping>.
22. Ibid.
23. Ibid. pg. 5-6.
24. Erickson and Kennedy, “China’s Maritime Militia,” pg. 8.
25. Ibid.
26. Ibid.
27. Ibid.
28. Ibid. pg. 11.
29. Kraska, “China’s Maritime Militia,” pg. 2.
30. Ibid. pg. 7.
31. Erickson & Kennedy, “Meet the Chinese,” pg. 2.
32. Erickson & Kennedy, “China’s Maritime Militia,” pg. 3.
33. Ibid. pg. 16.
34. President Pays Visit to Hainan Fishermen,” *China Daily*, 11 April 2012, http://usa.chinadaily.com.cn/2013-04/11/content_16394643.htm, pg. 3
35. James Kraska and Michael Monti, The Law of Naval Warfare and China’s Maritime Militia, report no. 91 Int’l Stud. 450 (2015), International Law Studies, U.S. Naval War College, 2013, accessed May 21, 2019, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1406&context=ils>, pg. 454.
36. Miles Yu, Inside China: Armed Fishermen, *WASHINGTON TIMES* (July 18, 2012), in James Kraska and Michael Monti, The Law of Naval Warfare and China’s Maritime Militia, report no. 91 Int’l Stud. 450 (2015), International Law Studies, U.S. Naval War College, 2013, accessed May 21, 2019, <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1406&context=ils>, pg. 453.
37. Dennis J. Blasko, Chinese Strategic Thinking: People’s War in the 21st Century, 10(6) *China Brief*, Mar. 18, 2010, at 5, http://www.jamestown.org/single/?tx_ttnews%5Bttnews%5D=36166&no_cache=1#.VTZQu2RVikp, pg. 7.
38. Axe, “Watch Out,” pg. 3.
39. Contemporary Operational Environment and Threat Integration Directorate (CTID), TRADOC G-2 Intelligence Support Activity (TRISA)-Threats., “OE Data Integration Network,” ODIN, , accessed June 18, 2019, https://odin.tradoc.army.mil/TC/TC_7-100.2_Opposing_Force_Tactics#Operational_Environments.
40. Kraska and Monti, The Law of Naval Warfare. pg. 454.
41. Dennis J. Blasko, Chinese Strategic Thinking: People’s War in the 21st Century, 10(6) *China Brief*, Mar. 18, 2010, at 5, http://www.jamestown.org/single/?tx_ttnews%5Bttnews%5D=36166&no_cache=1#.VTZQu2RVikp, pg. 7.
42. Kraska, “China’s Maritime Militia,” pg. 2.
43. Erickson, “Shining a Spotlight,” pg.4.

Bits in the Wire: Advancing Threats in the Cyber Domain

By Jerry England, OE&TA

Introduction

Today, computers and automation are central to many government, commercial, and personal activities. The automation of military command and control (C2) functions is continually adapting to the changing nature of multi-domain operations (MDO). This unprecedented level of connectivity has its own set of security challenges that includes an almost infinite attack space where anyone can be a victim of a cyberattack launched from practically anywhere in the world.¹ Overreliance on network battlefield management systems used to facilitate mission command can be particularly vulnerable to the force that fails to develop a recovery plan for critical systems. Information technology (IT) and the inherent risk of network communications is leading the United States of America and other nations to aggressively pursue information-related capabilities (IRC) to defend networks from determined, coordinated, and sophisticated adversaries in the information environment (IE).

In 2011 the Secretary of Defense declared cyberspace as an operational domain for the purposes of organizing, training, and equipping US military forces. In an address to Army Cyber Command troops, then Army Chief of Staff General Mark Milley stated that “The first shots fired in the next actual war will likely be in cyberspace, and likely [will be] with devastating effects.”² Cyberspace is defined as a global domain within the IE which consists of the interdependent network of information technology, infrastructures, and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.³ This article will address how cyber operations are becoming the weapon of choice for adversaries, describe the challenges associated with attribution, compare costs of cyberattacks to cyber investments by threat group, and present significant trends for the most significant threat actors.

Cyber the Weapon of Choice

In the last 20 years adversarial cyber activity has moved from an operational security concern to a full scope cyber threat requiring the development of doctrine, organizations, training, material, leadership, personnel, facilities and policies. “Gray Zone” confrontations and other competitive operations short of war are especially suited for cyber based capabilities.⁴ While there is a tendency to overhype the transformative capabilities of cyber operations, analysts are recognizing the relevance of cyber operations as a useful tool in recent conflicts. Academics at the Sage institute at the University of Michigan have compared present day interactions between traditional kinetic operations and cyber to those of ground operations and air power in World War I. Cyber can provide improved situational awareness as an important intelligence gathering tool but the full potential for the modern battlefield is just beginning to take shape.⁵

Threat actors can distribute malware both internally and externally via dark web networks to provide the platforms and infrastructure to perform a range of disruptive actions from the spread of propaganda to the destruction of critical information systems. Examples include social media “bots” that spread disinformation, “worms” and “sniffers” that illegally collect data, “RATs” that provide remote access to victim’s information resources, blockers that censor unwanted websites, as well as other tools and techniques that execute attacks to degrade or disrupt information systems. The networks used to deploy the malware and execute the attack lifecycle are hidden on dedicated and appropriated hosts generally outside of any network that can be traced to the attacker. The tools, when used in an adversarial attack on information systems and against media outlets are an alternative to traditional troops and equipment and can significantly transform battlefield events with relatively low risk.

The anonymity of cyberspace permits state and non-state actors to pursue broad operational and strategic goals with little chance of being discovered. By compromising sensitive government and commercial websites, forcibly transferring industrial and military

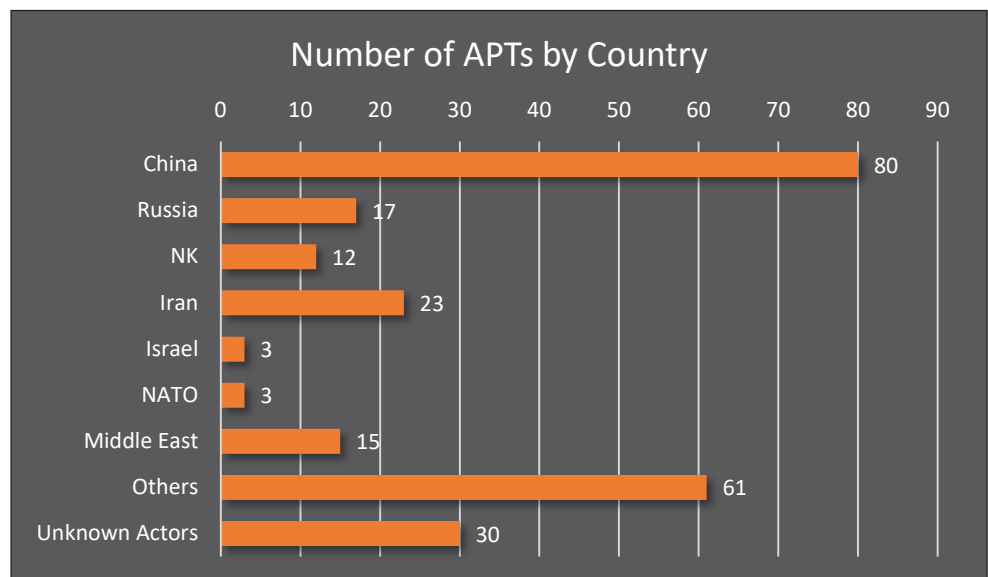
technology, and engaging in influential perception management campaigns the threat is able to potentially transform events by integrating cyber tools into their asymmetric warfare strategies.

Propagating disinformation and spying on select persons of interest appear to be the modernized information warfare techniques of former Soviet Russia. Examples of this include operationalized cyber activities in military campaigns from the Georgian war of 2008 to ongoing operations in Syria, as well as the compromise of government and non-government entities by degrading operational systems.⁶

Another cyber threat of a different nature, involves the theft of billions of dollars' worth of intellectual property and sensitive commercial information by Chinese advanced persistent threat (APT) groups operating under centralized government control.⁷ The cyber tools and expertise produced and used by these two major threat groups are spreading to other threat groups through cyber black markets on the dark web and increasing the risks associated with online interactions.⁸ Countries such as Iran and North Korea are reaping the value of cyber operations and are developing their own capabilities through observation, acquisition, research, and development.⁹

The versatility of cyber weapons and other information related capabilities make them ideal for coercive operations. Russia's version of the "whole of government" approach to the conflict continuum is a fundamentally non-military approach to political warfare that involves political alliances, economic warfare, propaganda, and psychological warfare that incites violence in an indirect way.¹⁰ Enabled by data driven activities and increasing interconnectivity, threat actors are attempting to level the playing field offset by US technology to undermine support and affect the perceptions of events on the ground.

Cyber weapons are unique because their objectives are often abstract and intangible and therefore difficult to recognize until after the fact. Cyber weapons are replicable and will regenerate more quickly than traditional weapons systems. Generally, a cyber weapon is not bound by the physical limitations of conventional direct and indirect fire weapons. Cyber weapons are designed to influence an adversary's actions and behavior by informational and



Number of APTs by country.

Source: Florian Roth. "APT Groups and Operations." <https://apt.threattracking.com/>

cognitive effects rather than through physical effects which can engender a kinetic response or stark condemnation on the world stage. For these reasons adversaries may prefer to use their cyber capabilities in pre conflict and pre kinetic situations in order to use the information environment to achieve their objective while limiting collateral damage. For example, Russia's information warfare campaign that preceded the annex of the Crimea was a relatively bloodless operation partially because ethnic Russians in the area had been reassured that annexation was more of a rescue operation than an occupation. The idea that the Russian population was under siege by extremist Ukrainians was accomplished through a mass media disinformation campaign that included a "troll army" that produced thousands of pro-Kremlin comments in online chatrooms. Other techniques involved staged military operations and influential messaging designed to increase ethnic tensions and promote the idea to Ukrainian security forces that the annexation was a fait accompli.¹¹ These operations had a significant impact and through a combination of internal and external disinformation remained well below the threshold of a traditional military response.

Network attacks as opposed to other types of IRCs are most associated with the term cyber because they are limited to the cyber portion of the information environment. These can include malicious code that mainly targets the physical and informational elements in the information environment. However, the impact of these attacks can bleed over into the cognitive element and influence the perceptions of those affected by the attack. The WannaCry ransomware attack launched in 2017 by a suspected North Korean hacking group spread to 250,000 computers in four

days and critically disrupted national services in the United Kingdom, Spain and Russia.¹² Described as the largest ransomware attack in history, WannaCry caused billions of dollars in damages in a few hours and caused many to question their government's ability to protect key cyber infrastructure. In spite of the large scale damage, the response was limited to dismantling the infrastructure that enabled the attack. The software vulnerabilities that enabled the attack were disabled and patched quickly, North Korea was publically blamed for the operation, and a part of North Korea's offensive hidden cyberattack network was shut down.¹³ Future attacks may incur stronger response as norms are established for countering cyber operations.

Maneuvering in Cyberspace

The ability to maneuver and provide command and control (C2) through cyberspace allows threat actors to potentially execute attacks from multiple physical and virtual locations thousands of kilometers away. Dispersed infrastructure along with other obfuscation techniques makes attribution difficult.¹⁴ Further, networks have the ability to change the location and the appearance of data elements through software updates, IT policies changes, and hardware upgrades. This shifting nature of cyberspace affects not only attacker's relation to the target but their relation to the information environment as well.¹⁵

Attribution Challenges

Attribution continues to be a challenge in the cyber domain; the anonymity of cyberspace is one of the main reasons for the attention cyber operations receives today. However, there are specific clues such as attack origins (in the physical and logical sense), the type of network equipment used, the identity of human and electronic personas, as well as common threat vectors, and malware that can assist in determining the origins or source of a cyberattack. Indicators such as tradecraft techniques, infrastructure and C2 relations, as well as malware signatures, objectives and intent, can support identifying a particular attack.¹⁶ Similar to how cryptologists during World War II were able to decipher messages using header messages and studying the rhythm of a threat operators typing speed, analysts today can use non-content indications like the programming styles and linguistic character to narrow the search for a cyber threat.

In the past, commercial and government entities only intermittently provided the details necessary to understand and identify cyber threat group operations. But as the frequency, size, and scope of attacks increase, the commercial and government sectors have

collaborated to help defend information systems. This partnership has created a better understanding of the signatures of offensive cyber operations and has improved defensive capabilities. For example, dwell time is a key metric developed by the cyber security industry, to assess the effect of a cyber capability. It is the time that a cyberattack has access to a targeted system and can provide signatures of a threat group. In 2011 the cyber security firm FireEye assessed that cyber threat groups had a median dwell time of 416 days to execute a cyberattack, while in 2018 it was 78 days.¹⁷ The decrease in dwell times over the last ten years is an indication of the increase in awareness individuals and organizations have of cyber risks.

Costs

Attacks are larger and more costly now than before in terms of the number of data records affected. The increasing number of affected records can translate to increased recovery costs. The estimated total of both direct and indirect costs for an average data breach is \$3.86 million. A mega data breach involving more than one million compromised records can cost hundreds of millions of dollars for an organization to fully recover.¹⁸

Massive data breaches of sensitive corporate and government networks like those at the US government's Office of Personnel Management (OPM) in 2015 and the credit consumer reporting agency Equifax in 2017 are part of an emerging trend for threat groups to compromise large datasets for intelligence and criminal purposes. Aside from the direct and indirect costs of recovery, a large scale data breach can have multiple second and third order effects.¹⁹ For instance, the ability to steal and exploit millions of files of personally identifiable information helps threat actors to validate intelligence from other collection efforts. Large amounts of personally identifiable information can be an advantage for a threat group's counter intelligence operations.

The effects of large scale data breaches on target systems are a significant return on investment for threat cyber actors. Online hacking services as well as stolen information like credit card numbers and other personally identifiable information can bring in significant revenue for a few hundred dollar investment on the dark web.²⁰ For example, a DDoS attack could cost approximately \$60 dollars per hour, while the monthly costs for a Remote Access Tool (RAT) campaign could be less than \$200 a month. The difference in prices usually indicates how much the interaction of a malware provider is required to maintain and operate the campaign.²¹

The total costs caused by cyberattacks and cybercrime in 2018 is estimated in the billions of dollars.²² Unique cyberattacks have increased by at least threefold from 2013 to 2018.²³ In 2018 the average number of breached records for an attack was 24,615 records at an average cost of \$3.86.²⁴

The global cyber market is estimated to be \$17.8 billion.²⁵ The military cyber budget for the Russian Ministry of Defence in 2013 was \$70 million.²⁶ Lack of transparency in accounting makes estimating China's defense spending difficult let alone its budget for cyber.²⁷ Between the years 2009 and 2010 one telecommunications vendor received more than \$220 million dollars in research funding from the PRC government.²⁸ Since that time, the Chinese defense budget has increased by 83 percent.²⁹ Since 2013, the Iranian government has increased its overall cyber budget to \$20 million.³⁰

China: Large Scale Initiatives

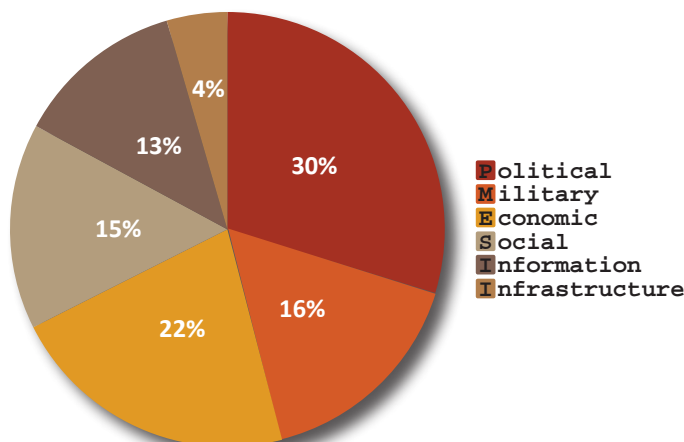
China continues to pursue large scale strategic cyber activities against the US Government, its corporations, and its allies. With twice the internet users than the entire population of the US, there are an estimated 75 unique Chinese based threat groups.³¹ These advanced persistent threats (APT) are increasing their operations and improving their techniques to avoid detection while gaining information on political, economic, and military sectors. The repurposing of commercial network security and testing tools for cyber exploitation operations and the installation of electronic vulnerabilities production process in Chinese network devices are just two of the techniques used for finding and siphoning critical data on a large scale.³²

For more than two decades China has built an ambitious program to train thousands of individuals to work within its cyber threat groups and create organizations that leverage the skillsets necessary

to penetrate industry specific networks and obtain protected technical data.³³ Some threat groups even have their own dedicated feeder schools that specialize in western languages and computer technology in order to provide trained personnel for their programs.³⁴ Chinese APTs have been associated with key industrial sectors and technological objectives in line with China's long term economic goals and development strategy. The "Made in China Action Plan" which describes the economic aspirations of China's latest five year plan, highlights ten areas of national interest in which the country intends to innovate. The areas are new energy vehicles, next-generation IT, biotechnology, new materials, aerospace, ocean engineering and high-tech ships, railway, robotics, power equipment, and agricultural machinery.³⁵ The ten areas combined with Chinese concepts of "military-civil fusion," "informatized," and "unrestricted warfare" indicate the likelihood that commercial objectives will have a significant government and military component.

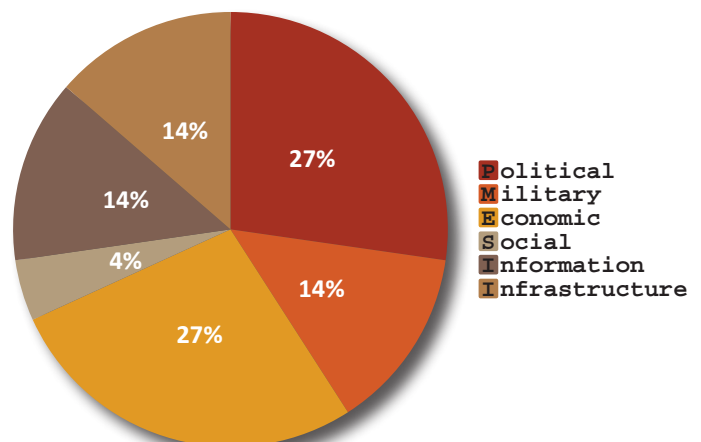
North Korea: Exploiting Opportunities

North Korea has been accused of a few high profile attacks in the last five years, in spite of very limited internet access across the country. North Korean hackers are suspected of receiving training in China and using their skills in a variety of locations. The widely publicized hack of the Sony Corporation in 2014 was described as unparalleled and well-planned for North Korean cyber groups. During the attack North Korean government cyber actors used stolen certificates as part of their plan to wipe as many corporate hard drives as possible.³⁶ Since then North Korean hackers have managed to steal an estimated \$649 million in electronic cash and cryptocurrency with a sophisticated combination of online fraud and malware.³⁷ This revenue stream is possibly being used to fund the regime's research and development for weapons of mass destruction. One of the largest heists



Sample China Based Advanced Persistent Threat Groups

Source: Florian Roth, "APT Groups and Operations," <https://apt.threattracking.com/>



Sample N. Korea Based Advanced Persistent Threat Groups

Source: Florian Roth, "APT Groups and Operations," <https://apt.threattracking.com/>

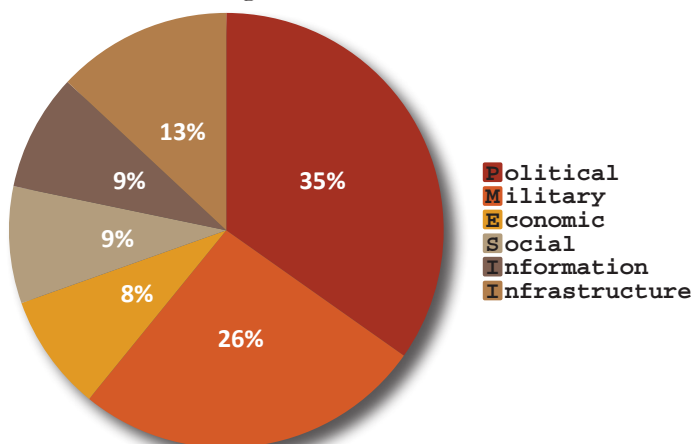
came from an attack on a US Federal Reserve Bank in which suspected North Korean operatives posing as Bangladeshi officials managed to lift \$81 million in SWIFT money transfers before being discovered.³⁸ North Korea's intelligence apparatus has made the most of opportunities with evolving cyber capabilities from espionage to large scale financial crimes.³⁹

Russia: Information Warfare

Russia's largely state owned energy firms, intelligence agencies, organized crime organizations, and embassies are using their skills in information warfare to support elements of the Russian government to achieve political warfare and information operations objectives.⁴⁰ During the opening months of the Ukraine conflict, Russia was engaged in a full scope information warfare campaign that hacked official Ukrainian government computers, physically degraded telecommunications networks, and spread disinformation.

Russia's has historically embraced information warfare as an integral part of its military and political operations. Liberal policies that protected Russian citizens who were accused of cybercrimes promoted the criminal hacker culture in Russia and created a talent pool for executing state sponsored initiatives.

The use of information resource capabilities to destabilize regional competitors and promote Russian elements of national power are contributing to the frozen conflicts affecting the regions in Russia's "near abroad."⁴¹ Russia's cyber operations are suspected as having a global reach and are not limited to European regional targets.⁴² In 2018 the United States accused Russia affiliated hackers of targeting the American electrical grid.⁴³ The technical requirements for cyberattacks against infrastructure indicate that Russia's cyber operations are far reaching and sophisticated. Other nations have taken note and have conducted similar attacks using similar methods.



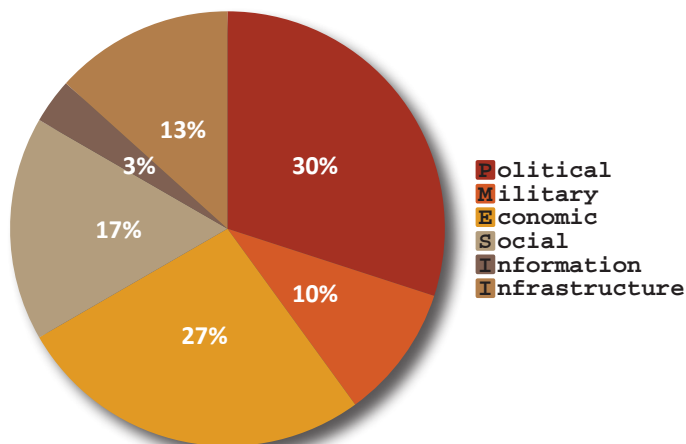
Sample Russia Based Advanced Persistent Threat Groups

Source: Florian Roth. "APT Groups and Operations." <https://apt.threattracking.com/>

Iran: Emerging Capabilities

Iranian activities in the information environment have included censorship and monitoring of Iranian internet users, blocking sites the regime found dangerous or offensive, and banning of the social media accounts of suspected dissidents.⁴⁴ Protesters using the social media platform to express their opinion about the 2009 Iranian presidential election, caused the government of Iran to acquire hardware for internet surveillance from Chinese telecommunications firm Huawei in order to monitor their communications.⁴⁵ Censorship and monitoring of social media internet traffic by Iran and its proxies are some of the techniques at Iran's disposal in other conflict areas such as Syria, Iraq, and Yemen. Since then, the Iranian Supreme Leader has authorized the establishment of a new Supreme Council of Cyberspace in 2011. In 2012 the new president of Iran announced a \$20 million budget increase for cyber operations.⁴⁶

Iran is also training "cyber warriors" drawing from its large hacker community to develop skills in attacking not just individuals but large organizations for political purposes.⁴⁷ Cyberattacks on Saudi Aramco and the Qatari RasGas and a series of distributed denial of service attacks against some large US banks by suspected Iranian hackers are noticeable indicators of the progress and scope of Iranian cyber offensive capabilities.⁴⁸ According to a US Department of Justice statement, employees of a number of Iran-based computer companies were sponsored by Iranian Revolutionary Guard Corps to conduct the campaign against the financial sector.⁴⁹ In 2012 a hacker who was suspected of acting on behalf of the Iranian government penetrated the industrial control system of a water dam in New York State using an open source tool known as Shodan.⁵⁰



Sample Iran Based Advanced Persistent Threat Groups

Source: Florian Roth. "APT Groups and Operations." <https://apt.threattracking.com/>

The use of third party individuals and proxy organizations to execute cyberattacks is an extension of the asymmetric warfare techniques refined by Iran's paramilitary Iranian Revolutionary Guard Corps. This year the US Department of Homeland Security issued a warning implicating Iran in a large scale Domain Name System (DNS) hijacking campaign against regional and European targets. Using compromised credentials, the attackers were able to change the resolved resource of a number of Middle Eastern organization's domain names. This enabled the attackers to redirect traffic to a controlled host and steal the encryption certificates enabling man-in-the-middle attacks.⁵¹ A leak by an Iranian whistleblower revealed the cyber campaign's goals and objectives as well as the software tools used by the Iranian government for the large cyberattack.⁵²

Winning in Cyberspace

Cyberspace is an important operational domain that the threat is using to establish and maintain an operational advantage against competing interests in the information environment. Cyberspace is considered an area in which future multi domain operations will be significantly influenced. The growth in cyber activity among countries with the technical abilities to leverage the information environment is increasing as well. In the last two decades, cyber enabled nation states have established increasingly sophisticated information gathering systems. Like the intelligence systems that nations and organizations have used for centuries, cyber enabled data collection efforts use a variety of overt and covert techniques to find, gather, and exploit information systems using both government and private organizations to achieve their objectives. As more users and devices go online the number of vulnerable devices and systems, known as the attack surface, will continue to increase the size and scope of cyber collection and exploitation efforts and the potential for large scale attacks. This increases the risk for further attacks. The nation, or organization that aggressively pursues a comprehensive cyber program has a significant operational advantage given these trends.

The use of artificial intelligence as an enabler of future cyberattacks may increase the capability of analytics as a toll for future military engagements. The amount of data produced by the next major conflict will significantly change the cyber capabilities as we understand them today. Facial recognition systems are generating large datasets of biometric data. Interconnected vehicles, weapons systems and Soldiers producing location and system status information will add to the digital fog of war. These large data sets may require quantum computing systems for analysis and processing of this data. Additionally, advanced analytics

will improve decisionmaking, increase the autonomy of unmanned systems and operationalize the internet of things as potential key terrain within the cyber domain. Horizon technologies like these will change operations across the multi domain battlefield. Ethical problems on the employment of these technologies will challenge policy makers to further understand analytics and artificial intelligence concepts to make informed decisions. The rapid pace in which people and devices will interconnect will require an effort to automate routine processes and decisions at a greater scale. To that end it is important to understand the current state of the art in cyber warfare, its possibilities—as well as its limitations—beyond today's concepts and models.

Advanced nations' over-reliance on computer aided operational processes can open a number of opportunities for threat actors to use in future cyberattacks. One potential approach would be to maximize cyber effects in a onetime massive strike that degrades, or destroys as many networks as possible across the PMESII-PT operational variables. The potential for catastrophic damage would be high if cyber threat actors could shut down both industrial sites and utilities while at the same time attacking the ability of first responders to gain situational awareness. If such an attack were timed with a natural disaster or with supporting lethal operations like a missile launch casualties could be even higher.

Another approach would be to degrade a large organization or an entire economic sector as a show of force while retaining other information related capabilities to use in future operations. By displaying a significant level of competency a threat actor could use the threat of future attacks as a bargaining chip.

A third option could be to conduct extensive full scope information warfare operations with an emphasis on intelligence gathering, propaganda, and limited attacks against as many sectors of the target nation as possible. This along with a significant perception management campaign could influence changes in behavior without garnering an excessive military response.

The first of these attack approaches would have the effect of isolating the target as it attempts to recover and reestablish situational awareness. The second type would be retaliatory in nature as unwanted reactions from the target would lead to more attacks. The third type of attack is a long term strategy that seeks to influence the target while slowly degrading its ability to defend itself in cyberspace. This approach would mostly be a shaping operation used to prepare the information environment for future operations.

Cyber Condition in Support of Multi Domain Operations in the Decisive Action Training Environment

The Decisive Action Training Environment (DATE) includes cyber as part of the five main characteristics of Multi-Domain Operations (MDO) that are likely to impact land force operations in the future. The cross-sectional nature of cyber elements in contemporary discussions leads analysts to consider its importance across the MDO characteristics.

Cyber and computer science advances including artificial intelligence can potentially lead to adversary overmatch in particular situations. DATE Africa includes artificial intelligence as part of the information variable as an emerging technology. Considering the impact of information technology and communications

(ICT) and other physical elements of the information environment has led to an increase in the momentum of humanitarian interactions and events. Networks described in the information and infrastructure sections of the DATE provide context for these momentum shifts in time, space, and purpose. Weapons of Mass Destruction (WMD) are an integral part of the Hybrid Threat's strategic and asymmetric capabilities. The spread of WMD technology via threat group networks is another avenue in which the cyber domain potentially impacts MDO. Finally, tech reliant societies living in dense urban terrain present a greater attack surface for the defensive and offensive operations in the cyber domain. Modern conditions such as cashless transactions and the internet of things in the Amari information variable provides deeper context for dense urban terrain and other conditions of urbanization. ♦

1. George Perkovich; Ariel Levite. "[Understanding Cyber Conflict: Fourteen Analogies, Conclusions.](#)" Georgetown University Press. 16 October 2017. Pg.252.
2. Mike Milford. "Leadership Change a Reflection of Steady Progress for Army Cyber Command." [www.army.mil](#). October 19, 2016
3. Joint Electronic Library, "[Joint Publication \(JP\) 3-12, Cyberspace Operations](#)". Joint Chiefs of Staff. 8 June 2018. Pg.100
4. George Perkovich; Ariel Levite. "[Understanding Cyber Conflict: Fourteen Analogies, Conclusions.](#)" Georgetown University Press. 16 October 2017. Pg.257.
5. Nadiya Kostyuk and Yuri M. Zhukov. "[Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?](#)" *Journal of Conflict Resolution*. 2017
6. Sam Jones. "[Russia Steps Up Cyber Assault.](#)" *Financial Times*. 19 February, 2016
7. White House Office of Trade and Manufacturing Policy. "[The White House Office of Trade and Manufacturing Policy. How China's Economic Aggression Threatens The Technologies And Intellectual Property Of The United States And The World.](#)" June 2018; U.S.- China Economic and Security Review Commission. "[2015 Report to Congress of the U.S.- China Economic and Security Review Commission.](#)" U.S. Government Publishing Office. 2015. Pg.39
8. Deloitte Threat Intelligence and Analytics. "[Black-market Ecosystem Estimating the cost of 'Pwn-ership'.](#)" Deloitte Development LLC. December 2018. Pg.3
9. Curtis Franklin. "[NSA Brings Nation-State Details to DEF CON.](#)" *Dark Reading*. 10 August. 2018
10. Max Boot and Michael Doran. "[Political Warfare, Policy Innovation Memorandum no.33.](#)" Washington, DC: Council on Foreign Relations. June 2013. Pg.2
11. Peter Pomerantsev and Michael Weiss. "[The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money.](#)" The Institute of Modern Russia, 2014, Pg.29
12. Ellen Kakashima; Phillip Rucker. "[U.S. declares North Korea Carried out Massive WannaCry cyberattack.](#)" *Washington Post*. 19 December. 2018
13. James Brady. "[Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea.](#)" 19 December 2017
14. George Perkovich; Ariel Levite. "[Understanding Cyber Conflict: Fourteen Analogies, Conclusions.](#)" Georgetown University Press. 16 October 2017. Pg.259
15. George Perkovich; Ariel Levite. "[Understanding Cyber Conflict: Fourteen Analogies, Conclusions.](#)" Georgetown University Press. 16 October 2017. Pg.255
16. Office of the Director of National Intelligence. "[A Guide to Cyber Attribution.](#)" 14 September 2018
17. Mandiant. "[M-Trends 2019: FireEye Mandiant Special Report.](#)" *FireEye*. 2019
18. Ponemon Institute. "[2018 Cost of a Data Breach Study: Global Overview.](#)" IBM. 2019
19. George Perkovich; Ariel Levite. "[Understanding Cyber Conflict: Fourteen Analogies, Conclusions.](#)" Georgetown University Press. Pg.255. 2017
20. Elizabeth Clarke. "[The Underground Hacking Economy is Alive and Well.](#)" *Secureworks*. 18 November. 2013
21. Deloitte Threat Intelligence Analytics. "[Black Market Ecosystem Estimating the cost of 'Pwner-ship'.](#)" December 2018
22. Mike Snider. "[Your Data Was Probably Stolen in Cyberattack in 2018 – And You Should Care.](#)" *USA Today*. 28 December. 2018
23. Ed Targett. "[6 Months, 945 Data Breaches, 4.5 Billion Records.](#)" *Computer Business Review*. 9 October. 2018
24. Ponemon Institute. "[2018 Cost of a Data Breach Study: Global Overview.](#)" IBM. 2019
25. PR News Wire. "[The Global Military Cyber Security Market 2018-2028.](#)" 29 October. 2018
26. Michael Connell; Sarah Vogler. "[Russia's Approach to Cyber Warfare.](#)" CAN Analysis Solutions. March 2017
27. Defense Intelligence Agency. "China Military Power," Pg. 21. 2019
28. Bryan Krekei; Patton Adams and George Bakos. "[Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage.](#)" U.S.-China Economic and Security Review Commission Pg. 75-76. 2012
29. Defense Intelligence Agency. "China Military Power," p.21. 2019
30. Ian Berman. "[Nuclear Deal Fallout: The Global Threat of Iran.](#)" Statement before the House Foreign Affairs Committee Subcommittee on Terrorism, Nonproliferation, and Trade. 24 May 2017 Pg. 3
31. Florian Roth. "[APT Groups and Operations.](#)" 15 August 2018
32. Office of the United States Trade representative Executive Office of the President. "[Update Concerning China's Acts, Policies, and Practices, Related to Technology Transfer, Intellectual Property, and Innovation.](#)" U.S. Government, 20 November 2018
33. Katherine Koleski. "[The 13th Five-Year Plan.](#)" U.S.- China Economic and Security Review Commission. Staff Research Project. 14 February 2017
34. Mandiant. "[APT 1 Exposing One of China's Espionage Units. Appendix A: How Does Mandiant Distinguish Threat Groups?](#)" Pgs. 61. 18 February 2013
35. Katherine Koleski. "[The 13th Five-Year Plan.](#)" U.S.- China Economic and Security Review Commission. Staff Research Project. 14 February 2017
36. Edgar Alvarez. "[Sony Pictures Hack: The Whole Story.](#)" *Engadget*. 10 December 2014
37. Patrick Winn. "[How North Korean Hackers Became the World's Greatest Bank Robbers.](#)" PRI. 16 May 2018
38. Raju Gopalakrishnan and Manuel Mogato. "[Bangladesh Bank Official's Computer was Hacked to Carry out \\$81 Million Heist: Diplomat.](#)" Reuters. 19 May 2016
39. Dorothy Denning. "[North Korea's Growing Criminal Cyberthreat.](#)" *The Conversation*. 20 February 2018
40. Stephen Blank. "[Cyber War and Information a la Russe.](#)" Georgetown University Press. 16 October 2017. Pg. 82
41. Stephen Blank. "[Cyber War and Information a la Russe.](#)" Georgetown University Press. 16 October 2017. Pg. 83
42. National Cybersecurity and Communications Integration Center. "[Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.](#)" Department of Homeland Security. 16 April 2018
43. Dustin Volz; Timothy Gardner. "[In a First, U.S. Blames Russia for Cyber Attacks on Energy Grid.](#)" Reuters 15 March 2018
44. Timothy Lee. "[Here's how Iran Censors the Internet.](#)" *Washington Post*. 15 August 2015
45. Ian Berman. "[The Iranian Cyber Threat Revisited. Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cyber security, Infrastructure Protection, and Security Technologies.](#)" 20 March 2013. Pg.2.
46. James Andrew Lewis. "[Cyber security and Stability in the Gulf.](#)" CSIS. January 2014. And Jim Finkle. "[Cyber experts warn Iranian hackers becoming more aggressive.](#)" Reuters, 13 May 2014
47. Executive Cyber Intelligence. INSS-CSFI. April 1st. 2015.
48. James Andrew Lewis. "[Cyber security and Stability in the Gulf.](#)" CSIS. January 2014. Pg.2
49. Department of Justice. "[Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities.](#)" 24 March. 2016
50. Dina Chiacu. "[Iranian Hackers Infiltrated Computers of a Small Dam in NY.](#)" *Wall Street Journal*. 21 December 2015
51. National Cybersecurity and Communications Integration Center. "[DNS Hijacking Campaign.](#)" Department of Homeland Security. 11 January 2019
52. Andy Greenberg. "[A Mystery Agent Is Doxing Iran's Hackers and Dumping Their Code.](#)" *Wired*. 18 April 2019

The Combined Arms Battalion and Combined Arms Brigade: The New Backbone of the Chinese Army

By Bradley A. Marvel, OE&TA

For nearly all of the armies of the world wars, and throughout the Cold War, the division was the primary combined-arms organization capable of independent operations. The massive land forces of WWII were almost universally built around the division, with armies on both sides adopting surprisingly homogenous organizations: most consisted of three maneuver regiments or brigades, an artillery brigade, and support and command staff. As the “big army” culture of the Cold War wound down, however, virtually all of the world’s first-order armies have transitioned from the division to the brigade—or brigade-sized units—as their basic operational building block. The world’s military thinkers seemingly simultaneously decided that an enhanced brigade was the ideal mix of firepower, maneuver, and support, while being optimally sized for decentralized command and control and rapid strategic and tactical movement.

While the division has been resigned to a largely administrative role in the modern era, the other major echelon-of-note from the WWII/Cold War era—the battalion task force—remained largely unchanged well into the 21st century. Battalions around the world are typically “pure” in their composition—armor, mechanized infantry or light infantry—which are then combined with slices from other battalion types in order to create what the WWII-era German Heer called the *Kampfgruppe*, or what the US Army, then and now, calls task forces. This archetype, too, is beginning to change, most prominently in two of the world’s premier land forces. In what is either a remarkable coincidence or the result of a copycat effort, both the US Army and the Chinese People’s Liberation Army (PLAA) have, at practically the same time, fielded organic combined-arms battalions within their armored brigades.¹ For the PLAA, this represents just one step along a decades-long reorganization effort, breaking down their older big-army corps model into smaller, more agile, and componentized force structures.

This article provides a study of the PLAA’s new tactical-level formations: the combined arms brigade (CA-BDE), and the combined arms battalion (CAB). It provides detailed descriptions of each of the three types of CA-BDEs: light (motorized), medium (mechanized), and heavy (armored). It also describes the evolution of the PLAA from massive corps-based operations to agile brigade- and battalion-based operations, and provides examples of some of the tactics that these units may employ.

From Corps to Battalion: Tracking the PLAA from Korea to 2020

When the PLA sent its “volunteer force”—the People’s Volunteer Army, or PVA—across the Yalu River and into North Korea in October of 1950, its quarter-million soldiers were organized into six corps. This army was influenced by lessons the Chinese Communist Party (CPC) learned during Second Sino-Japanese War and the Chinese Civil Wars of the previous decade, wherein Communist Chinese forces fought a years-long series of campaigns on their own soil against enemies that were more numerous, better trained, equipped, and led. The PVA can be accurately thought of as a real-world manifestation of Mao Zedong’s “People’s War” theories: a technologically inferior force designed to defeat a more powerful enemy through a mix of political motivation, rapid close-combat maneuver, and deception.²

The PVA’s corps model was very different from the approach taken by both Western and Soviet bloc militaries of the same period. Corps commanders were given a frontage in which to conduct their operations, then given a series of objectives from the PVA’s headquarters. The PVA commander, Peng Dehuai, communicated directly with his corps commanders, forcing him to manage six subordinate units.³ Military historians and theorists may cringe at this fact—it is commonly accepted that this is far too many direct subordinate organizations for one command, a fact learned by both the PVA in Korea, and the US Army during its brief “Pentomic Division” experiment, also in the 1950s.⁴ Despite his aggressiveness and dedication, Peng’s performance during his command of the PVA was decidedly mixed, but his observations about the supply and command issues that plagued the PVA was an early driver of reform both in Korea and in the PLA.⁵

While the PVA’s echelon-above-corps structure did not work well, the corps themselves performed somewhat better.⁶ The use of such a large formation as the basic tactical echelon made sense for the PVA: they had hundreds of thousands of men, but virtually no logistical support, very little in the way of modern communication equipment, few competent staff officers, and little mechanization or armor. PVA units had to remain in close proximity to their command and to adjacent units, lest they become isolated and rendered ineffective. Corps commanders typically

positioned their individual regiments for attack or defense, and then issued an objective—usually a terrain feature—to the regimental commanders.⁷ Regimental commanders then employed an approach described by one US Marine officer as “assembly on the objective⁸”—subordinate companies or platoons simply made their way to the objective as best they could, using a combination of rapid movement, stealth, and deception to overcome enormous enemy advantages in firepower. The tactical rigidity of this approach had severe shortcomings—once a unit was committed to combat, for instance, it was virtually impossible to revise its mission—but in the tight terrain of the Korean peninsula, and against an enemy trained and equipped to fight and win a mechanized war in the Atomic Age, it was formidable, and the PVA achieved astonishing successes against UN forces through the early phases of the war.⁹

Western journalists called these tactics “Human Wave.”¹⁰ It is easy to understand where the name came from—thousands of UN soldiers experienced sudden, massive surprise assaults by seemingly endless swarms of fast-moving Chinese soldiers. The name “Human Wave,” however, belies the sophistication of PVA tactics. While the final phase of an attack did often resemble a mass assault by closely-packed groups of soldiers, Chinese units were experts at long-range movement at night, silently, through rough terrain.¹¹ A Chinese regiment moving in close-quarters at night could—and often did—move so silently as to be undetected by the front line of UN troops.¹² They closed the range with enemy units quickly, and thus appeared to come out of nowhere. The overwhelming UN advantages in armor, air, and artillery firepower were largely nullified when engaging at such close ranges. Here, the couple of hand grenades and rifle or machine gun carried by the Chinese soldier was all the firepower that was needed.

The downside to what Peng eventually called the “Short Attack” was that it nearly always resulted in significant casualties to the assaulting unit.¹³ Units that were detected at longer ranges, or who became decisively engaged in periods of daytime or good weather were regularly decimated by UN firepower, particularly air and artillery strikes. The PVA had virtually no tactical flexibility: they had no modern communications equipment, no way to sustain attacking units for long periods of time, and no NCO corps to manage independent tactical actions at lower echelons.¹⁴ Moreover, the PVA had virtually no ability to conduct a true deep attack: even if PVA units managed to assault and overwhelm a frontline enemy unit, they were unable to exploit the breach by driving deep into the enemy’s rear areas due to their poor logistical support and almost complete lack of motorization and mechanization.

Eventually, the Korean War ground to a bloody stalemate, with neither side able to achieve a decisive result with the limited resources available. General Peng grew increasingly frustrated with the PVA’s shortcomings: while they had achieved remarkable victories against very powerful opponents, their shortcomings had gradually eroded their initial advantages. As the war dragged on, UN forces inflicted massive casualties on the PVA for virtually no military or political gain. Peng viewed this as a flaw in the People’s Army theory: instead of relying solely on bravery, motivation, short-range maneuver, and deception, he wanted his forces equipped with modern weapons: anti-aircraft guns, machine guns, and tanks; he wanted his artillery able to directly support maneuver forces, and to be supplied with adequate ammunition; he wanted his soldiers supplied with food, ammunition, and medical supplies—Korean winters had been brutal on the PVA.¹⁵

Despite failing to achieve a decisive victory, General Peng returned from North Korea a national hero. He immediately sought to leverage his new political influence into a top-to-bottom reform of the PLAA based on his experiences in North Korea. He argued that China should rebuild its military using the Soviet model, mixing large numbers of infantry divisions with highly mobile armored divisions able to conduct independent operations deep behind enemy front lines. He advocated for a professionalization of the PLAA, establishment of a new rank and pay structure, and issuance of modern military uniforms. Peng was successful in virtually all of these efforts initially, and many of his reforms established the basis for what would eventually become the modern PLA.¹⁶ In the process, however, he made an enemy of Mao, who began to view his reform attempts as rightist and counterrevolutionary. Peng was nothing if not a fanatical devotee to Chinese communism, but his attempts to modernize the People’s Army proved too conventional for the CPC establishment. Peng was gradually stripped of power, forced to resign and live in obscurity, until radicals during the Cultural Revolution imprisoned and tortured him until his death.¹⁷

Following Peng’s fall from power, Mao and other CPC officials set to work undoing as many of Peng’s reforms as possible, reverting to a “rankless” force structure and relying on a mix of political indoctrination and manpower to achieve military success.¹⁸ These military transformations aligned roughly with two of the more extreme Maoist political movements of the era, the Great Leap Forward and the Cultural Revolution, which helped to underpin the PLAA’s extremist philosophical approach of the period. At the same time, the Sino-Soviet split removed most of the remaining Soviet military support to China, removing access to new Soviet equipment and training assistance.¹⁹ The result was a PLA that consisted of millions of poorly trained and equipped conscripts, led by officers who were

selected for their positions due to party influence or political loyalty rather than military competence. Though Mao died in 1976, his extremist legacy in the PLAA endured for a time, and was still dominant when China went to war against Vietnam in 1979.

As the French, Japanese, French (again), and Americans had discovered over the previous 150 years, Vietnamese fighting on their own ground are not to be trifled with. The Vietnamese People's Army (VPA) that the PLAA engaged in its 1979 border war had been hardened by nearly a half-century of continuous conflict—and victory—against some of the world's most powerful militaries. The PLAA expected to overwhelm the VPA with its vast manpower advantage, but after having advanced only a few dozen kilometers into Vietnamese territory, the Chinese offensive rapidly fell apart. Fighting largely against Vietnamese militia units, the PLAA suffered catastrophic failures in logistical support, command, and discipline. They attempted to use the same corps-based mass-assault structure that had proven effective in their previous campaigns, but with just slightly longer supply lines, and against an opponent seasoned in guerilla warfare, the PLAA's performance was disastrous.²⁰ Modernized VPA artillery outranged and outgunned PLAA artillery divisions, hundreds of Chinese tanks were lost to early anti-tank guided missiles, and vulnerable supply lines were savaged by Vietnamese guerillas. The Chinese eventually abandoned their plans to capture key cities in Vietnam, and instead, concentrated nearly their entire force on the city of Long Son. Facing a regular VPA division instead of just militia, it took over a week to subdue the city despite a massive numerical advantage. Having taken Long Son, the PLAA conducted a scorched-earth withdrawal, having achieved none of their major objectives, and having cost China a full year's worth of domestic investment and development initiatives. The complaints General Peng had made a generation before—poor logistics, poor communication, a lack of mechanization, and a lack of modern weapons systems—plagued the PLAA throughout the campaign.²¹

The Sino-Vietnamese War was a disaster for the PLA, but it was precisely the impetus the CPC needed to fully purge the ghosts of Mao from the PLA and begin to meaningfully modernize.²² The new Chinese leader, Deng Xiaoping, developed a decades-long plan for modernizing practically every aspect of the Chinese economy, society, and its military. Military reforms were enormous: PLA was to be purged of much of its Maoist tradition, then rebuilt along the lines of the Soviet model championed by General Peng.²³ Deng's plan culminated in 2010, and envisioned China having rebuilt its military into a modern, fully mechanized force, well on its way to becoming a first-order military capable of joint and expeditionary operations.²⁴

The first phase of these reforms began with the removal of Mao's political commissars from key military positions, and building PLAA operations around the division, abandoning the corps as its primary operational element for the first time in over 50 years. Adopting a philosophy of "quality over quantity," millions of conscripts were first mustered out, bloated headquarters were reduced, and enormous stockpiles of obsolete equipment were scrapped. The PLAA was reduced in size by massive cuts throughout the 1980s and 1990s; by 2005, it was roughly half the strength it had been in the 1970s. The PLAA's design of the late 80s and early 90s largely mimicked the Red Army's approach in the Soviet Union: the country was divided into military regions, each with a number of field armies, and each field army consisting of two or three divisions.²⁵

Two major world events further shaped the PLA's development during this era. First, the PLAA's response to the Tiananmen Square protests displayed enormous systematic problems within the army, ranging from simple incompetence in performing simple tasks to outright insubordination from thousands of active officers. Tiananmen drove the PLAA to re-introduce political and ideological training as a part of its military education system, and helped to emphasize the role of political officers in the PLA's system of leadership.²⁶ A few years after Tiananmen, China watched with great interest as a coalition of nations, led by the United States, massed forces in Saudi Arabia and Kuwait, and then, in short order, crushed a large and well-equipped Iraqi army as a part of Operation Desert Storm. Chinese military leaders watched with a mix of fascination and alarm as the US-led coalition meticulously built up combat power for months along the Iraqi border, then virtually annihilated what was regarded as one of the world's strongest ground forces in a matter of days. The PLAA noted two major implications from Desert Storm: first, American expeditionary forces were far more effective if allowed to build their combat power in a distant theater unmolested; second, Soviet-derived equipment from the early Cold War—which constituted nearly all of the PLAA's equipment—was woefully outclassed by the modernized equipment of American and other Western militaries.²⁷

The combination of Tiananmen and the Gulf War sparked a new round of reform efforts in the mid-1990s. The first effort significantly realigned the Chinese strategic approach to defending their territory. The People's War mandated that China could only fight a defensive war, but the Gulf War illustrated clearly that allowing a powerful enemy to mass their forces on one's doorstep was a losing proposition. People's War theory was thus modified, and an "active defense" idea was added. Now, Chinese forces would actively resist the buildup of enemy combat power throughout China's near seas and border regions, a technique that

would eventually be called “anti-access/area denial” by the Department of Defense.²⁸ Second, efforts to modernize equipment and create leaner but more powerful formations were accelerated. Enormous quantities of aging tanks and other armored vehicles were abandoned, and major investments were made to modernize virtually the entirety of the PLAA’s equipment.²⁹

As these reforms were put into place, experimented on, and revised, the “brigade-ization” of many of the world’s armies was fully underway. The combination of new doctrine, new equipment, and the need for smaller, more agile formations prompted the PLAA to develop two new formations: the combined arms brigade, and the combined arms battalion.

Into the 21st Century: the CA-BDE and CAB

The brigade-ization of the world’s armies dovetailed nicely with the PLAA’s ongoing drawdown in size and desire to upgrade the training and equipment of its forces. It is unclear if the PLAA was significantly influenced by the US Army’s own reform and modernization efforts during the early 2000s, but the solution that the Chinese arrived at for its brigade-sized formations looks remarkably similar to that which the US Army adopted at about the same time. Three different primary formation types were established: the light (motorized) CA-BDE, which consisted of truck-mobile or armored personnel carrier-mounted infantry; the medium (mechanized) CA-BDE, built around the infantry fighting vehicle (IFV) and IFV-mounted infantry; and the heavy (armored) CA-BDE, built around the main battle tank (MBT). Initially, CA-BDEs were built with “pure” battalions, meaning that the maneuver battalions of each were homogenous—only infantry, mechanized infantry, or armor. After a period of experimentation and revision, the traditional homogenous battalion was replaced with the combined arms battalion—the CAB.

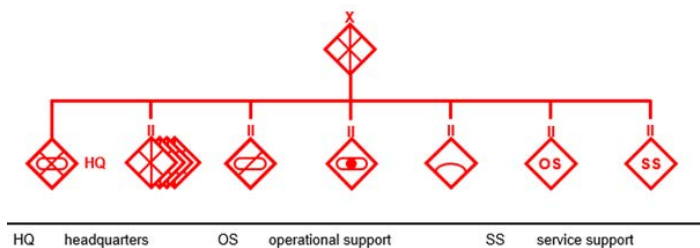
Major changes occurred at echelons above the CA-BDE as well. First, the corps as it had existed throughout the history of the PLAA was done away with, replaced by a new formation called the group army. The group army was not a field army in the traditional sense, but rather, was a corps-sized formation that mixed six CA-BDEs with six supporting brigades: artillery, air defense, aviation, SOF, engineer and chemical defense, and service support.³⁰ The group army was built specifically to support the new PLA concept of system warfare: elements of the group army are used to build the various combat groups that comprise an operational system—the task-organized unit that conducts operations.³¹ The division echelon was virtually done away with: only a handful of division structures remain extant, and it is unclear how these legacy organizations integrate within the group army/CA-BDE structure.

The operational system is the complete set of capabilities assembled to conduct a particular mission. At the group army level, an operational system can be thought of as similar to western joint task forces (JTFs).³² On a smaller scale, operational systems are assembled to conduct specific tactical missions such as an assault, defense of a key position, or wide-area security. Combat groups are sub-units of the operational system, and are built to perform specified tasks in support of the operational system’s mission. Combat groups are typically named for their task: command group, assault group, firepower group, and so on; these names do not yet appear to be standardized, and different variations appear throughout different PLAA publications. While the CA-BDE can be thought of as the tactical-level force provider for the various combat groups, the CAB is likely meant to be employed either in its organic form, or augmented by attached capabilities. The PLAA describes the CAB as the lowest echelon capable of independent operations, and for many tactical-level combat groups, a CAB serves as the group’s manpower backbone and bulk of its combat power.³³

The PLAA describes the differences between motorized and mechanized infantry in how supporting vehicles are employed: motorized units are only transported by their assigned vehicles, while mechanized forces employ their vehicles as combat platforms that support the infantry.³⁴ The PLAA employs a variety of APCs and IFVs that feature a broad range of firepower and protection; some are tracked, some are wheeled, and there is considerable overlap. As such, one must look at how the unit intends to fight, rather than its composition and equipment, when assessing a unit as motorized versus mechanized. Airborne, mountain, and amphibious CA-BDEs are described as light.

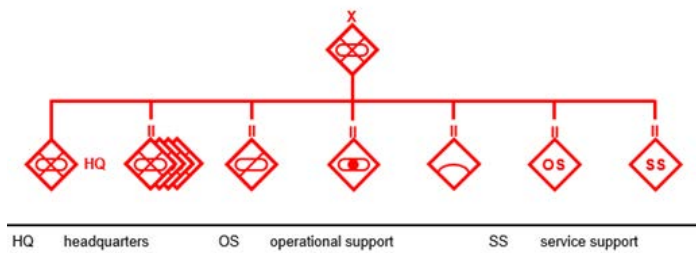
The three basic types of CA-BDE are designed as follows:

Light combined arms brigade



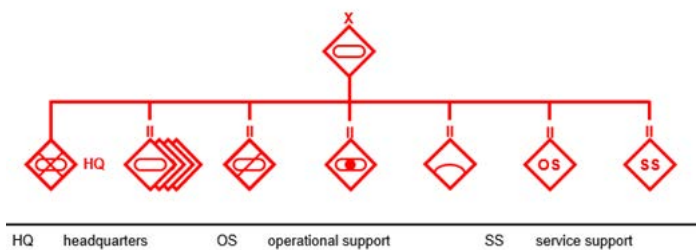
- 4 motorized combined arms battalions
- 1 reconnaissance battalion
- 1 artillery battalion
- 1 air defense battalion
- 1 headquarters unit
- 1 operational support battalion
- 1 service support battalion

Medium combined arms brigade



- 4 mechanized combined arms battalions
- 1 reconnaissance battalion
- 1 artillery battalion
- 1 air defense battalion
- 1 headquarters unit
- 1 operational support battalion
- 1 service support battalion

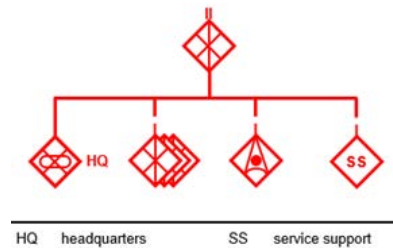
Heavy combined arms brigade (CAB)



- 4 armored combined arms battalions
- 1 reconnaissance battalion
- 1 artillery battalion
- 1 air defense battalion
- 1 headquarters unit
- 1 operational support battalion
- 1 service support battalion

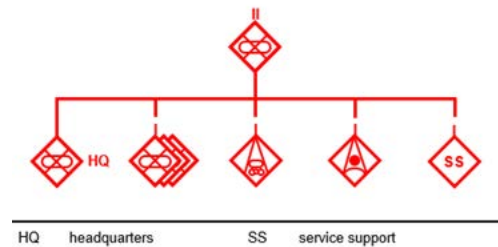
The CAB takes the basic combined arms approach used to build the CAB and applies it to the battalion echelon. CABs appear to only combine different maneuver elements along with organic short-range fires elements (assault guns and mortars), with the provision that other headquarters can attach elements from other brigade organizations as required. The CAB is very similar to the US battalion task force concept employed by mechanized and armored units since the WWII era, mixing company-level infantry and armor units to create a single combined arms command. Each CAB also houses an organic short-range air defense capability in the form of man-portable air defense systems (MANPADS). Of note, the CAB appears to have only limited staff, which may affect its ability to function as the PLAA intends—as an independent unit.³⁵ CAB structures are as follows:

Light combined arms battalion



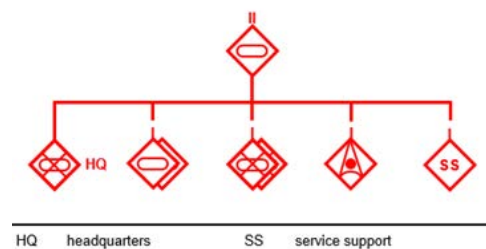
- 3 motorized infantry companies (10 light wheeled vehicles or APCs per company)
- 1 firepower company (6–9 rapid-fire 81-mm mortars, MANPADS, crew-served weapons)
- 1 headquarters unit
- 1 service support company

Medium combined arms battalion



- 3 mechanized infantry companies (10 wheeled or tracked infantry fighting vehicles per company)
- 1 assault gun company (14 wheeled 105-mm assault guns)
- 1 firepower company (6–9 rapid-fire 120-mm self-propelled mortars, MANPADS, crew-served weapons)
- 1 headquarters unit
- 1 service support company

Heavy combined arms battalion

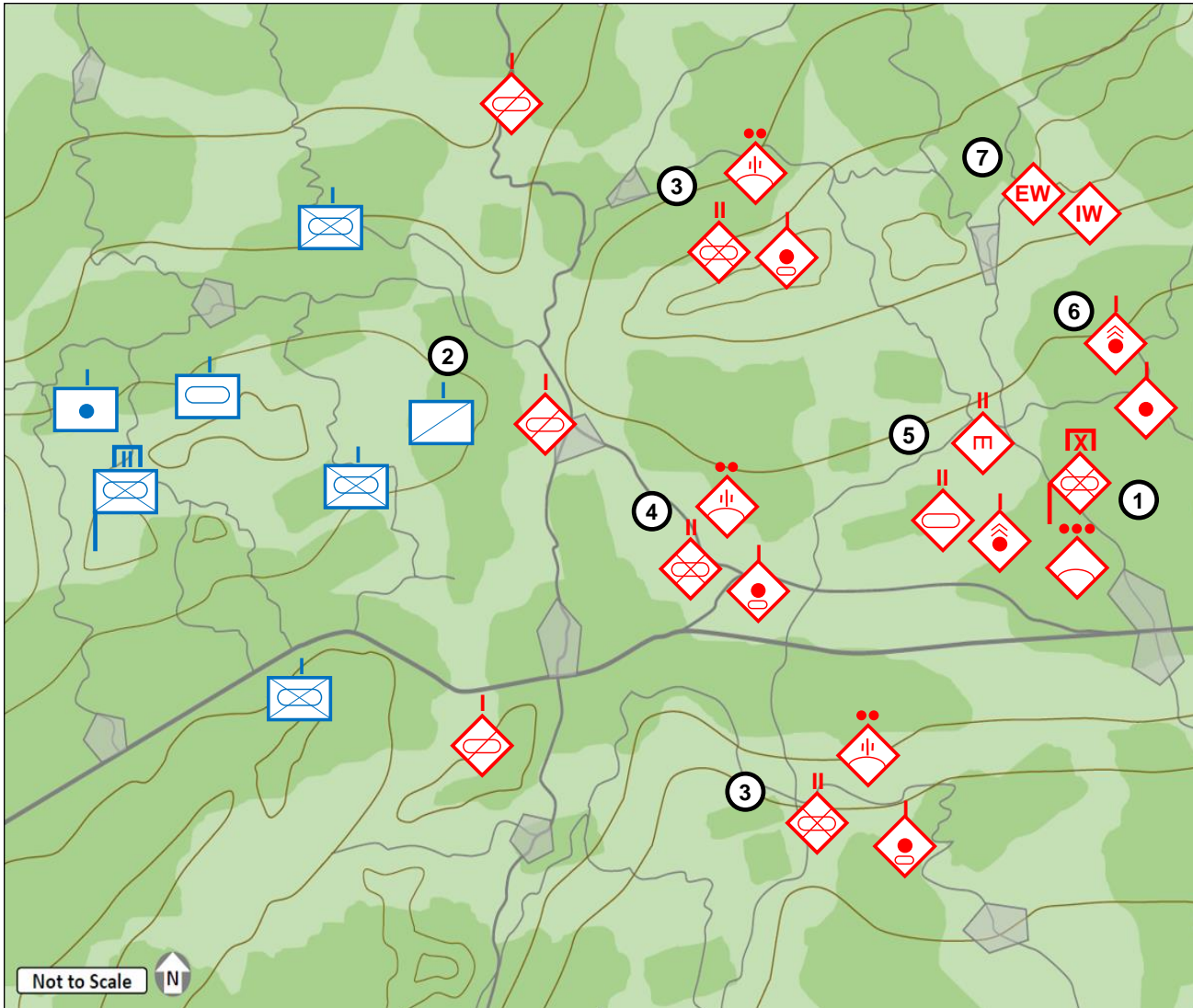


- 2 tank companies (10–14 tanks per company)
- 2 mechanized infantry company (10 infantry fighting vehicles per company)
- 1 firepower company (6–9 rapid-fire 120-mm self-propelled mortars, MANPADS, crew-served weapons)
- 1 headquarters unit
- 1 service support company

CA-BDE and CAB operations in Practice

This section provides two vignettes describing the CA-BDE and CAB operations in action.ⁱ

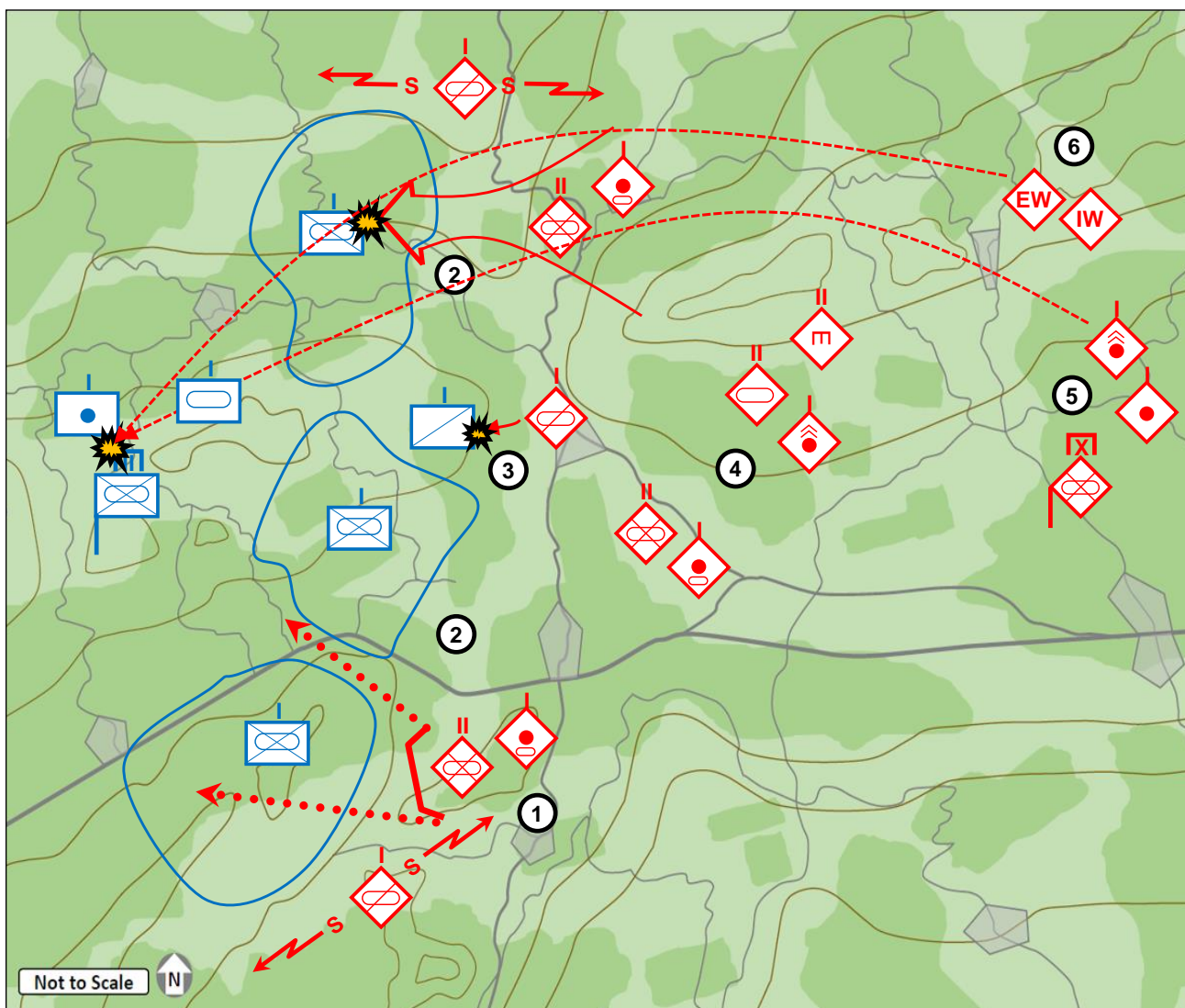
7-1. Advance



(1) An offensive group advances in preparation for an assault against an enemy mechanized task force that has taken up a defensive position. The offensive group is to annihilate the enemy task force in order to weaken the enemy's overall defensive strength and provide an approach route for follow-on forces. (2) The reconnaissance group deploys in an advance guard position, with order to reconnoiter enemy defensive positions and identify potential weak points and strong points. (3) Two frontline attack groups comprise the bulk of the main assault. They will fix the enemy and enable actions by the depth attack and thrust maneuver groups. (4) The depth attack group is positioned to exploit any weaknesses in the enemy defenses. This group attempts to conceal its axis of advance in order to surprise the enemy. (5) The thrust maneuver group, consisting of an armor battalion, a mechanized engineer battalion, and a rocket battery, waits in the rear area to exploit the successful attack of the depth attack group. (6) The firepower group, consisting of a heavy howitzer battery and a heavy rocket battery, wait to deliver decisive indirect fire anywhere on the battlefield. (7) IW and EW groups stand by to conduct EW and deception operations, aimed primarily at fooling enemy sensors, deceiving the enemy commander, and suppressing enemy communications.

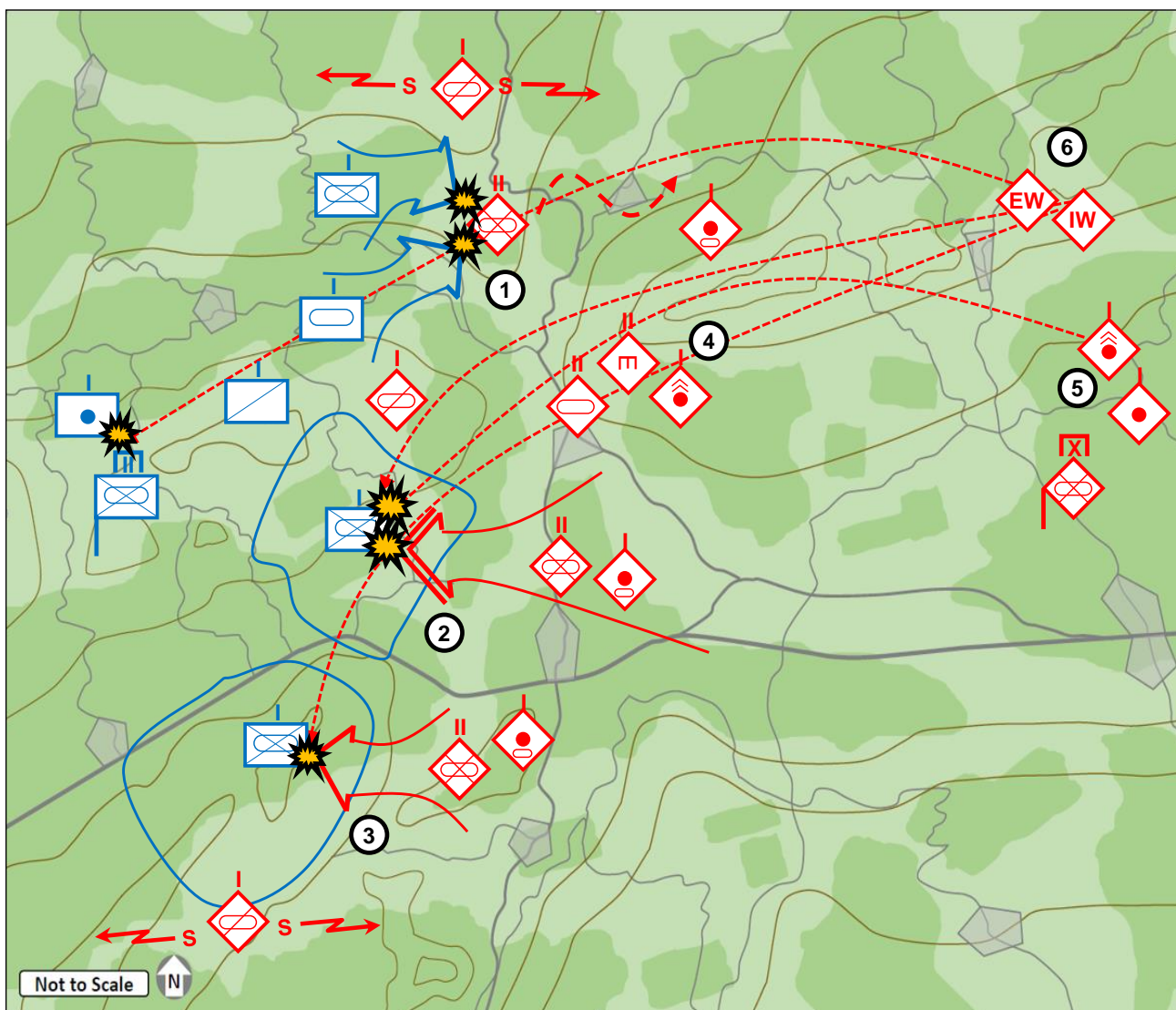
i. Note: these vignettes are excerpts from the upcoming publication ATP 7-100.3, Chinese Tactics

7-2. Unfold



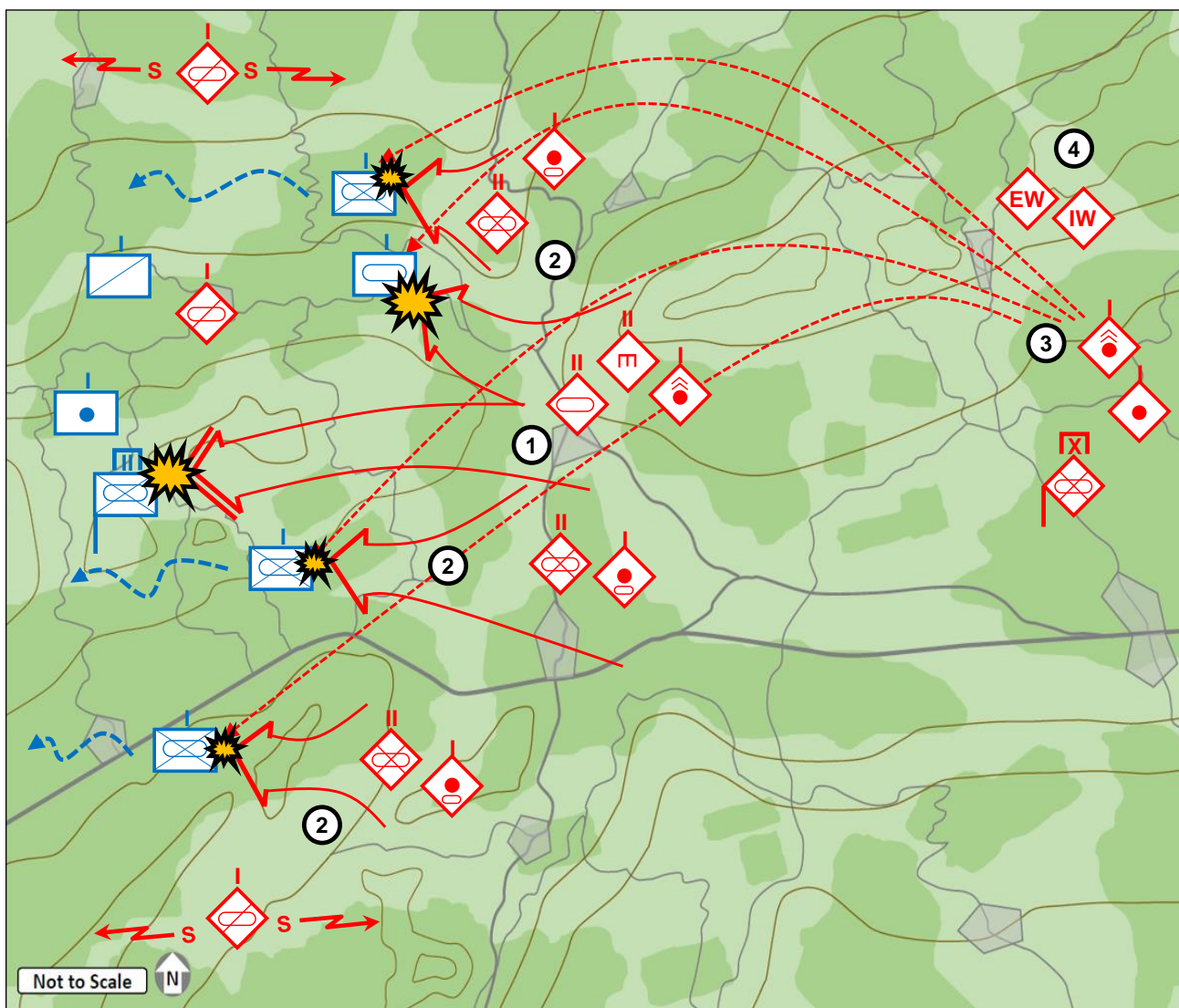
(1) One of the frontline attack groups positions itself in a support-by-fire position, engaging an enemy unit and fixing them in position. (2) At the same time, the other frontline attack group conducts a limited attack against the enemy's left flank, testing the strength of the enemy defenses. These two actions, conducted in concert with one another, are intended to confuse the enemy commander about the location and axis of the main assault, forcing him to commit reserves early. (3) Reconnaissance units engage enemy scouts, preventing them from effectively reconnoitering friendly units and ensuring the enemy commander remains ignorant about the location and direction of the main assault. (4) The depth and thrust groups move under concealment to their initial attack positions. As the frontline attack groups conduct their attacks, the offensive group commander develops his understanding of the situation, and finalizes the axis of the main assault. Combat power is concentrated along this axis. (5) The firepower group conducts a fire assault against the enemy's rear area, disrupting enemy command and communications and causing casualties. (6) EW and IW direct conduct electronic warfare and information warfare against the enemy command, with their main effort focused on deceiving the enemy about the location and axis of the main assault.

7-3. Initiate



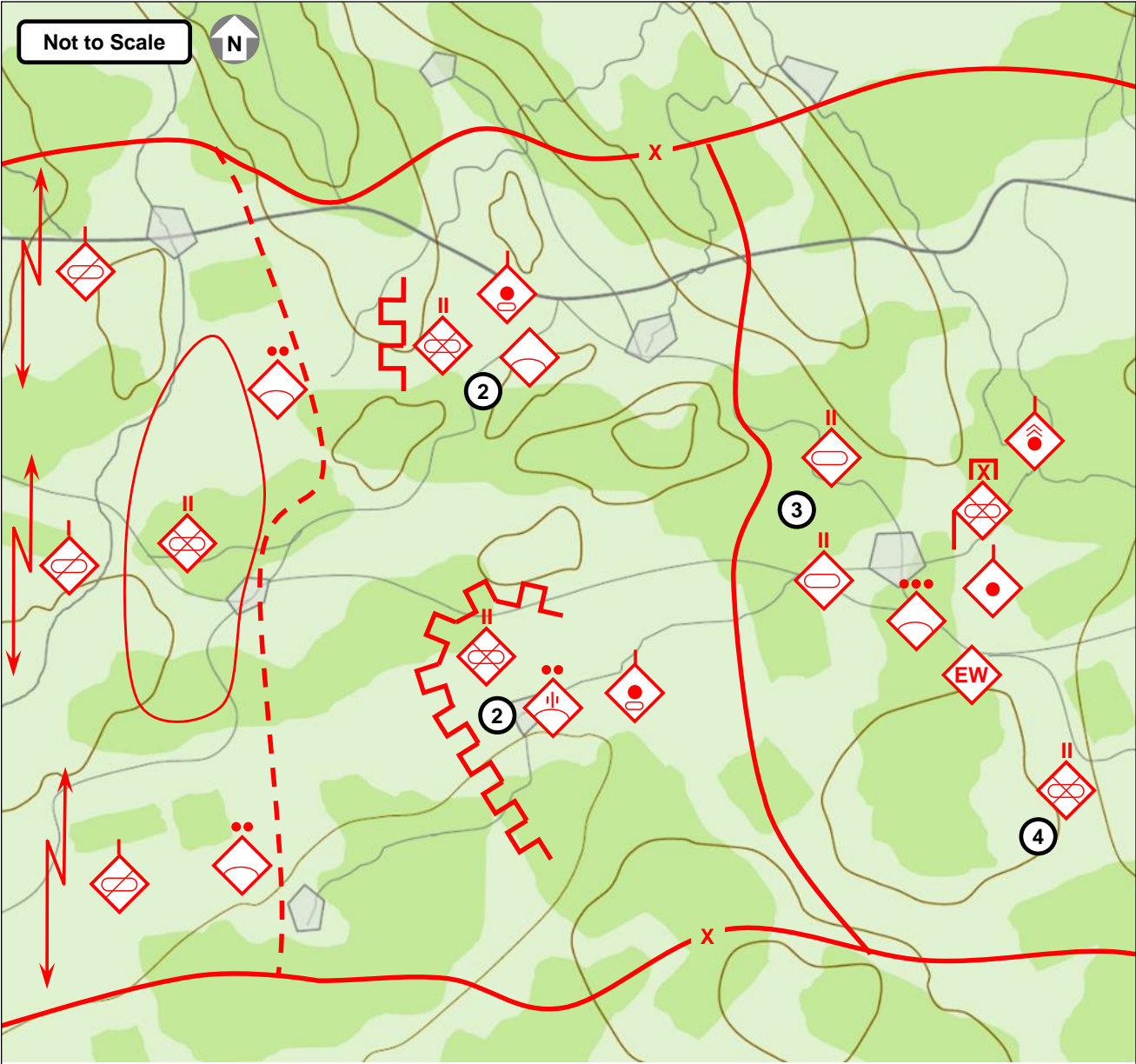
(1) The enemy commander, deceived into thinking that the main effort is targeting his left flank, commits his reserve in a counterattack against the northern frontline attack group. This group rapidly transitions to a defensive posture and begins a deliberate retrograde operation, intended to overextend the enemy's counterattack force and eventually isolate them from their command. (2) The commander, having identified the enemy's center as vulnerable, commits the depth attack group in a decisive assault. Their objective is to breach the enemy's main defensive line and isolate the two enemy flanks. (3) The other frontline attack group conducts an assault against the enemy's right flank, fixing the enemy unit and preventing them from reinforcing the group under assault in the center. (4) The thrust group positions itself to exploit the breach created by the depth attack group. (5) The firepower group conducts a fire assault against the enemy center in support of the depth group's assault. (6) The EW group commences its decisive effort, suppressing enemy communications in order to electronically isolate enemy units and confuse response to the main assault. The IW group transitions to information attack operations, attempting to increase enemy units' perception of isolation.

7-4. Annihilate



(1) The thrust maneuver group conducts the decisive deep assault into the enemy's rear area, targeting command posts, supply areas, artillery units, and potential escape routes. This completes the isolation of enemy units and compromises the enemy's overall defensive position. The thrust maneuver group also conducts a hasty attack against the exposed flank of the enemy's counterattack force, ensuring they cannot be redeployed and maintaining their isolation. (2) The frontline attack and depth groups conduct storming attacks against the isolated and depleted enemy units. Local fire support is integrated with maneuver to either destroy or force the withdrawal of enemy units. Assaults are coordinated as much as possible to ensure the enemy cannot reinforce units under attack. (3) Firepower assaults target retreating enemy units, disrupting their movement and ensuring that retrograde actions cannot be mounted. (4) EW and IW groups shift their focus to disrupting adjacent enemy units from reinforcing the now-defeated enemy unit, and on preventing the enemy's higher echelon from communicating with the defeated unit.

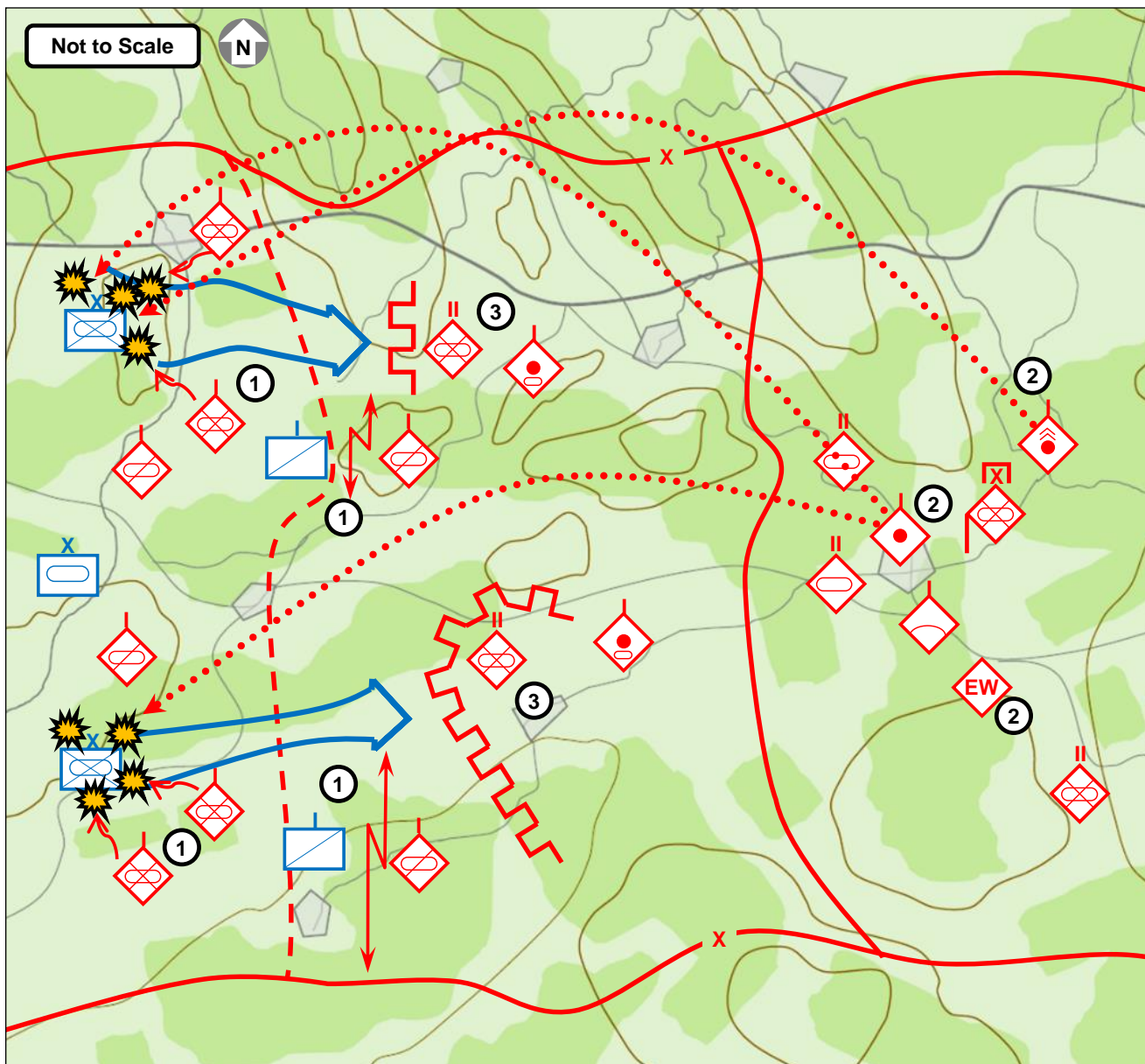
8-2. Reconnaissance and Deployment (conceptual)



(1) The cover group deploys a mix of reconnaissance and light infantry units into the frontal blocking zone. These units conduct reconnaissance and counter-reconnaissance missions while screening the main body. MANPADS sections establish ambush zones along potential aerial avenues of approach. (2) The frontier defense zone is occupied by the frontier defense group. The main line of defense consists of two key defense points each defended by a mechanized CAb. SPG batteries provide and SPAAG sections are in direct support. (3) The depth defense group consists of two armored CAb supported by a heavy towed battery, a rocket battery, and a SHORAD platoon. This group is charged with conducting the decisive counterattack against the enemy’s main effort. (4) The reserve group consists of a mechanized CAb. They await orders to block enemy advances or to support the depth group’s counterattack.

CAb	combined arms battalion	MANPADS	man-portable air defense system
S	screen	SAM	surface-to-air missile
SPG	self-propelled gun	SPAAG	self-propelled anti-aircraft gun

8-3. Spoil (conceptual)

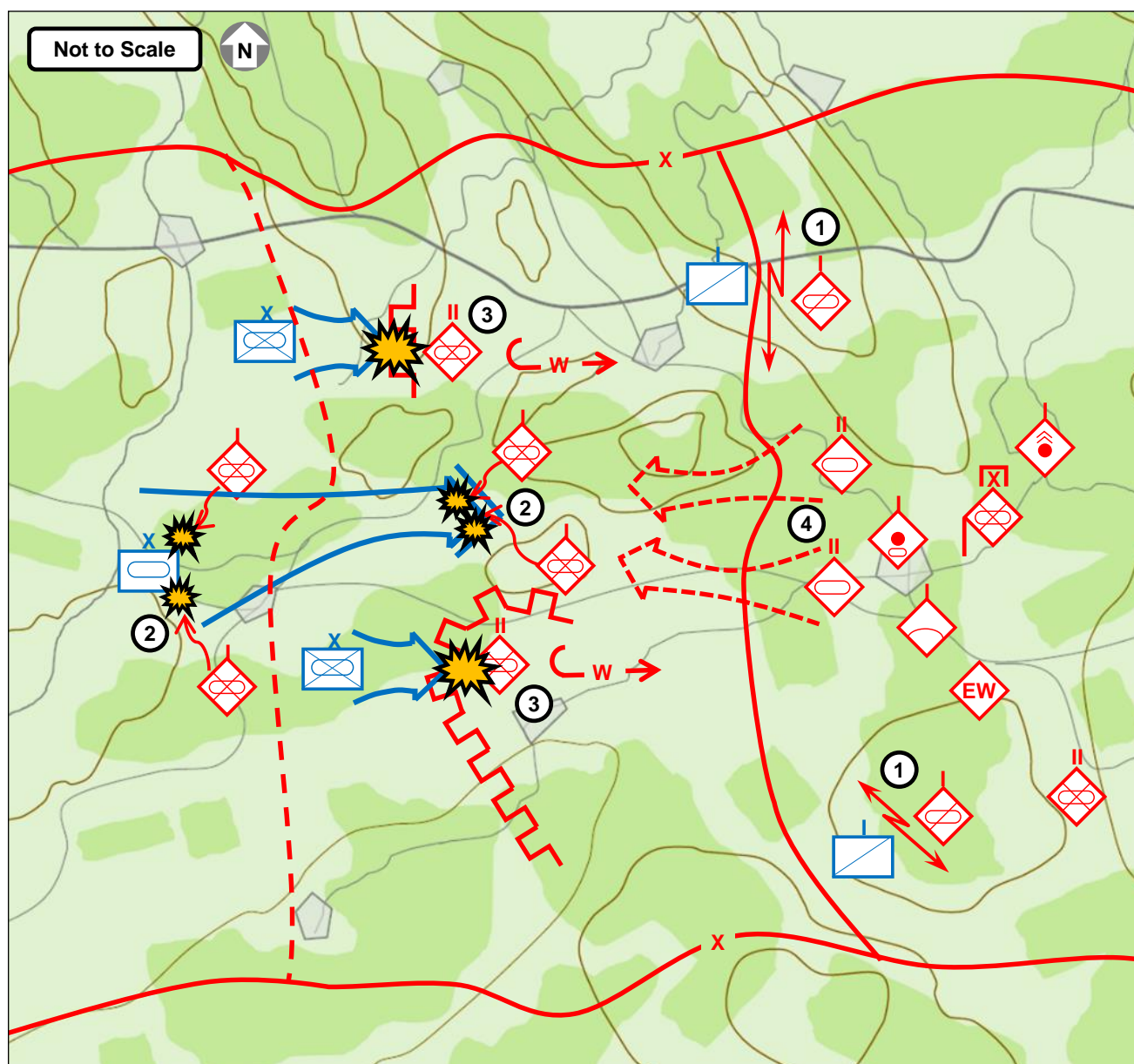


(1) Two enemy mechanized brigades begin an attack on the defensive group's position. Reconnaissance units conduct counter-reconnaissance operations against enemy scouts. Mechanized CAb units in the cover group conduct spoiling hit-and run attacks against the enemy, forcing them to deploy early and slowing their progress through the frontal blocking zone. (2) The firepower group delivers firepower assaults against high-value enemy units, and the EW group simultaneously attempts to suppress enemy communications and deceive enemy collection systems. (3) The frontier defense group entrenches around the key defensive points and prepares to conduct a blocking action.

CAb combined arms battalion

EW electronic warfare

8-4. Resist (conceptual)

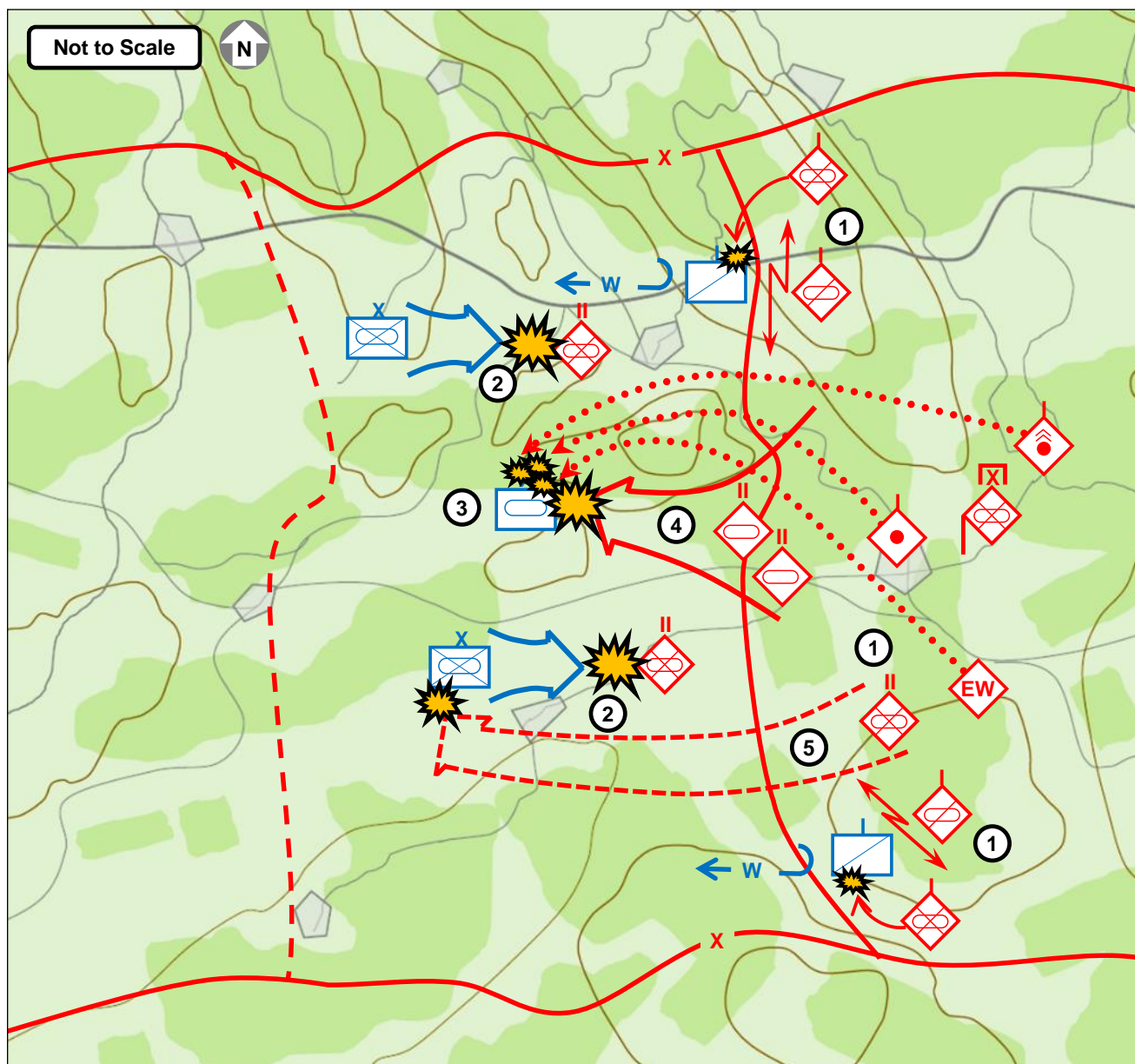


(1) Reconnaissance units continues to conduct counter-reconnaissance operations against advancing enemy scouts to prevent detection of the disposition and axis of the main counterattack. (2) The cover group commences spoiling attacks and raids against the enemy's main effort, causing disruption and forcing early deployment. These attacks are continuous and intended to canalize the enemy's main effort, directing it to the point in the frontier defensive zone where the main counterattack is planned. (3) The frontier defense group conducts strong resistance against enemy attacks on key defensive positions. The enemy attempts to fix the two CABs and destroy them in detail; entrenchments and firepower blunt the attack. The CABs conduct a retrograde action, falling back slowly and blocking enemy penetrations into rear areas. (4) The depth group begins to move toward the counterattack position. By this time, the enemy's position and axis of advance are well known, and the commander carefully chooses the time and place for the counterattack.

CAB combined arms battalion

EW electronic warfare

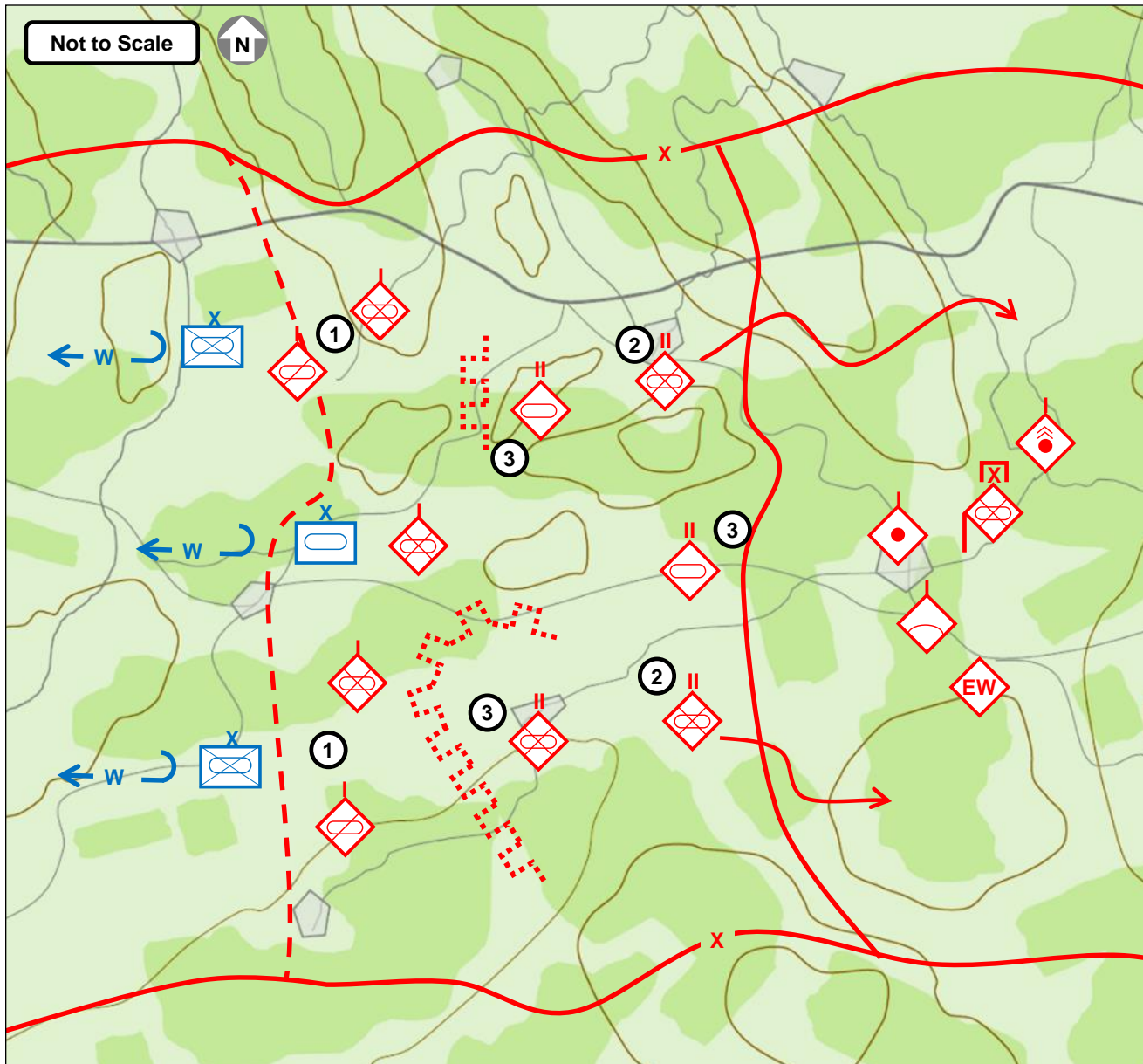
8-5. Counterattack (conceptual)



(1) The cover group continues to conduct counter-reconnaissance operations against enemy scouts. Mechanized infantry elements of the cover group conduct attacks against enemy scouts, forcing their withdrawal and exposing the flanks of the enemy assault group. (2) The frontier defense group continues to conduct blocking actions against the enemy's supporting attacks, preventing penetrations and slowing the enemy's advance. (3) Firepower is concentrated on the enemy's main effort. Tube and rocket artillery plus electronic attack are massed on the target in order to disrupt movement, reduce cohesion, and cause casualties. (4) The depth group conducts its counterattack assault. Despite being outnumbered, the depth group achieves local superiority through mobility, deception, and the effective use of firepower. The depth group assaults the enemy's main body head on, attempting to destroy the enemy's momentum and cohesion. (5) The combat reserve group is deployed in an attack on the enemy's exposed flank in an attempt to isolate the enemy's main body and force the enemy's withdrawal.

EW electronic warfare

8-6. Consolidate (conceptual)



(1) The cover group maintains contact with the retreating enemy, employing firepower to keep enemy forces off balance and ensure they cannot quickly reconsolidate. (2) Having suffered heavy casualties during its blocking actions against superior forces, the frontier defense group moves to rear areas for consolidation and refit, becoming the new reserve group. (3) The original depth and reserve groups occupy the key defensive positions and begin entrenching, preparing for the next enemy assault and providing a strong position from which to begin offensive operations in the sector.

EW electronic warfare

The Post-Reformation PLAA: Training Implications

For US Army training audiences, the first step to understanding the PLAA in the 21st century is to immediately throw out the stereotypes of a poorly-trained and ill-equipped conscript army attempting to overwhelm their opponents with sheer weight of manpower. The modern PLAA is a mostly modernized and largely mechanized force, with advanced EW capabilities, and several weapons systems that are competitive with their Western counterparts. While their reforms are not yet complete—and numerous capabilities and conventions are not yet mature—the contemporary PLAA should be viewed as a modern,

mechanized force, largely comparable to other first-order armies around the world.

Key PLAA capabilities that should be carefully replicated are their skill and tenacity in combat reconnaissance; the integration of reconnaissance, maneuver, and firepower; the density of anti-tank and anti-air weapons of all types; and the toughness, enthusiasm, and dedication of the Chinese soldier. Limitations that should be replicated are immature staff procedures and structure, relatively weak logistical and sustainment support, the presence of large numbers of legacy systems—particularly tanks and artillery—and limited joint integration. ♦

1. Blasko, D. J. (2019). PLA Weaknesses and Xi's Concerns about PLA Capabilities". *Panel on "Backlash from Abroad: The Limits of Beijing's Power to Shape its External Environment"*.
2. Zhang, S. G. (1995). *Mao's Military Romanticism: China and the Korean War, 1950–1953*. Lawrence, KS: University Press of Kansas.
3. George, A. L. (1967). *The Chinese Communist Army in Action: the Korean War and its Aftermath*. New York: Oxford University Press.
4. Sepp, K. I. (2001). *The Pentomic Puzzle: The Influence of Personality and Nuclear Weapons on U.S. Army Organization 1952–1958*. Washington DC: U.S. Army Center of Military History.
5. Ho, A. K.-I. (2004). *China's Reforms and Reformers*. Westport: Praeger.
6. George, A. L. (1967). *The Chinese Communist Army in Action: the Korean War and its Aftermath*. New York: Oxford University Press.
7. Zhang, S. G. (2003). *Command, Control, and the PLA's Offensive Campaigns in Korea, 1950–1951*. New York City: Routledge Taylor & Francis Group.
8. Lynn Montross, N. A. (1957). *U.S. Marine Operations In Korea 1950-1953: Volume III - The Chosin Reservoir Campaign*. Historical Branch, G-3. Headquarters U.S. Marine Corps.
9. George, A. L. (1967). *The Chinese Communist Army in Action: the Korean War and its Aftermath*. New York: Oxford University Press.
10. Salmon, A. (2010, January 10). *Massive Attack in 1951: Human Wave Rolls South*. Retrieved from The Korea Times: http://www.koreatimes.co.kr/www/news/nation/2010/01/120_58792.html
11. George, A. L. (1967). *The Chinese Communist Army in Action: the Korean War and its Aftermath*. New York: Oxford University Press.
12. Lynn Montross, N. A. (1957). *U.S. Marine Operations In Korea 1950-1953: Volume III - The Chosin Reservoir Campaign*. Historical Branch, G-3. Headquarters U.S. Marine Corps.
13. Zhang, S. G. (2003). *Command, Control, and the PLA's Offensive Campaigns in Korea, 1950–1951*. New York City: Routledge Taylor & Francis Group.
14. Ibid
15. Ho, A. K.-I. (2004). *China's Reforms and Reformers*. Westport: Praeger.
16. Ibid
17. Teiwes, F. C. (1986). Reviewed Works: *Memoirs of a Chinese Marshal—The Autobiographical Notes of Peng Dehuai (1898-1974)*. by Zheng Longpu; Peng Te-huai: The Man and the Image. by Jurgen Domes. *The Australian Journal of Chinese Affairs*.
18. Ho, A. K.-I. (2004). *China's Reforms and Reformers*. Westport: Praeger.
19. Westad, O. A. (1998). *Brothers in Arms: The Rise and Fall of the Sino-Soviet Alliance, 1945-1963*. Washington DC: Woodrow Wilson Center Press.
20. Jencks, H. W. (1979). China's "Punitive" War on Vietnam: A Military Assessment. *Asian Survey*.
21. Ibid
22. Maclaren, J. (2019, May 24). *The Diplomat*. Retrieved from The Sino-Vietnam War and China's Long Route to Winning: <https://thediplomat.com/2019/05/the-sino-vietnam-war-and-chinas-long-route-to-winning/>
23. Ho, A. K.-I. (2004). *China's Reforms and Reformers*. Westport: Praeger.
24. Garnaut, R. (2018). China's 40 Years of Reform and Development: 1978–2018. *China Update Series*.
25. Li, X. (2007). *A History of the Modern Chinese Army*. University Press of Kentucky.
26. Blasko, D. J. (2012). *The Chinese Army Today: Tradition and Transformation for the 21st Century*. Routledge.
27. Phillip C. Saunders, A. S. (2019). *Chairman Xi Remakes the PLA*. Washington DC: National Defense University Press.
28. The Diplomat. (2012, May 25). *An Anti-Access History Lesson*. Retrieved from The Diplomat: <https://thediplomat.com/2012/05/an-anti-access-history-lesson/>
29. Blasko, D. J. (2012). *The Chinese Army Today: Tradition and Transformation for the 21st Century*. Routledge.
30. Ibid
31. People's Liberation Army. (2010). *Services and Arms Application in Joint Operations*. Shenyang: Baishan Press.
32. Ibid
33. Ibid
34. People's Liberation Army. (2009). *Army Combined Tactics under the Condition of Informationization*. Beijing: Shijiazhuang Army Command Academy Press.
35. Blasko, D. J. (2019). PLA Weaknesses and Xi's Concerns about PLA Capabilities". *Panel on "Backlash from Abroad: The Limits of Beijing's Power to Shape its External Environment"*.

INTERVIEW

Dennis J. Blasko, LTC, USA (Ret)

By Bradley A. Marvel, OE&TA

A seemingly endless number of writers, analysts, and officials endlessly discuss the political goals and strategies of China. The amount of noise makes it very difficult to tell truth from fiction from hyperbole from propaganda. Can you give us your take on the modern Chinese political objectives, and the strategies they intend to use in order to get there?

First and foremost, China and the CPC (Communist Party of China) are looking to become what they call a “Great Power,” as they were centuries ago. We can trace much of this back to 1979, when Deng Xiaoping implemented a massive reform effort in the wake of Mao’s death a few years earlier. He set the goal to become a “moderately developed” country by the mid-21st century, which is usually interpreted as the centennial anniversary of the PRC, or 2049. When this goal was first established, China was very literally dirt-poor by global standards. They had to make major changes to their economy and society at large in order to build the foundation for achieving what they now call the “China Dream.”

Officially, they do not use language that suggests they’re looking to supplant any existing world power; they don’t discuss spreading the communist political ideology; they don’t discuss having the most powerful military, or the most political influence, or the greatest scientific or industrial base. Instead, they talk about being a leader in each of these areas—one of many leaders. That being said, they still face significant challenges in achieving their goals.

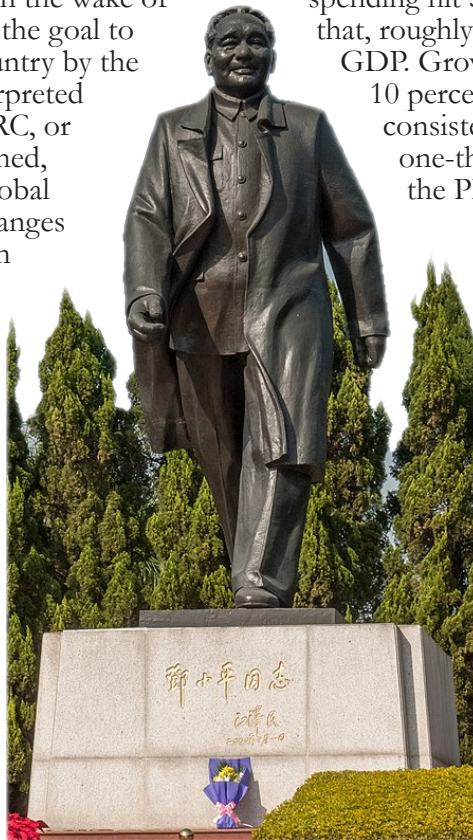
In my opinion, the most important aspect of this from the military’s perspective is understanding the path that China adopted following Deng Xiaoping’s ascent. In the early 1980s, Deng stated that he did not think a large-scale war was likely. At the time, this meant that China could essentially postpone building a strong military, and instead, focus China’s limited resources on building their economy, their science and technology base, and a variety of other social, non-military issues. This was a significant contrast compared to the massive investments in the military one saw in other one-party states, such as the Soviet Union or North Korea. The military’s development essentially was subordinated to national economic development, and for much

of the first 20 years after Mao’s death, the military was relegated to a background role from a budgetary perspective. Their defense spending in this era was in the single-digit billions, for a force numbering between 3 and 4 million soldiers. Compare this to American spending of around \$400 billion for a force roughly half that size.

In the mid to late 1990s, with the economy growing at a rapid rate, they started spending more money directly on the military. In the mid 1990s, Chinese defense spending hit \$10 billion, and grew consistently after that, roughly in step with the growth of the Chinese GDP. Growth varied year to year, averaging over 10 percent annually, but the upward trend was consistent. Today, their spending is around one-third of the United States. This has given the PLA far more resources to throw at new equipment and training. However, it should be noted that the growth of the military budget remains subordinate to, but coordinated with, national economic development and the communist party controls the allocation of resources.

Chinese military development goals were first quietly announced in the late 1990s, then announced more publicly in 2006. They described a three-step development process for military modernization: placing benchmarks at 2010, 2020 and mid-century, meaning 2049, indicating a very long-term outlook for military modernization. Specific objectives have been adjusted slightly over the years and Xi Jinping recently added a new milestone in 2035, acknowledging that the 2010 date had passed. By 2020, they expect that their current set of reforms to be complete, and

will have achieved mechanization of the PLA (People’s Liberation Army). By the time of Xi’s new benchmark, they seek to have fully modernized equipment, training, personnel structure, and doctrine. By 2049, they look to be a “world-class military.” Officially, they consistently use the wording **A** world class military, not **THE** world class military. But, they don’t define what a world-class military is, a lesson learned from previous rounds of reform, where certain goals were set out, and then adjusted.



A famed statue of Deng Xiaoping, the architect of many Chinese reform efforts following the Mao era.

Source: Ermell [CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>)], https://commons.wikimedia.org/wiki/File:Statue_of_Deng_Xiaoping_in_Lianhuashan_Park_Shenzen_China_1310759.jpg

One important thing about these development objectives is that while some western analysts and governments suggest that the Chinese are attempting to achieve hegemony in the Indo-Pacific region in the near term—and global hegemony in the long term—the Chinese do not use the term hegemony to describe their own objectives. In fact, they use the term “hegemony” to describe other powers—currently, like the US, and historically, like the USSR—in a pejorative sense. They also do not use the term Indo-Pacific as we understand it—their focus is on Chinese-claimed territories and the near seas.

As for more specific Chinese objectives, I see securing Chinese borders and territory, deterring attacks on the mainland, peaceful reunification of Taiwan, and maintaining Chinese claims in the near seas as their primary political objectives. Most other international objectives focus more on economic and commercial development, such as the Belt-Road Initiative. While these efforts are widely publicized, they likely are not as well-planned and organized as we’re led to think they are. They may, however, eventually necessitate a greater Chinese military presence overseas that likely will require an improved naval and expeditionary capability. We’re seeing this effort drive the expansion of the Chinese navy and marine corps -- the marine corps, for example, has more than tripled its size over the last few years, increasing from two marine brigades of 5,000 to 6,000 personnel each, to six brigades, plus new SOF and aviation units.

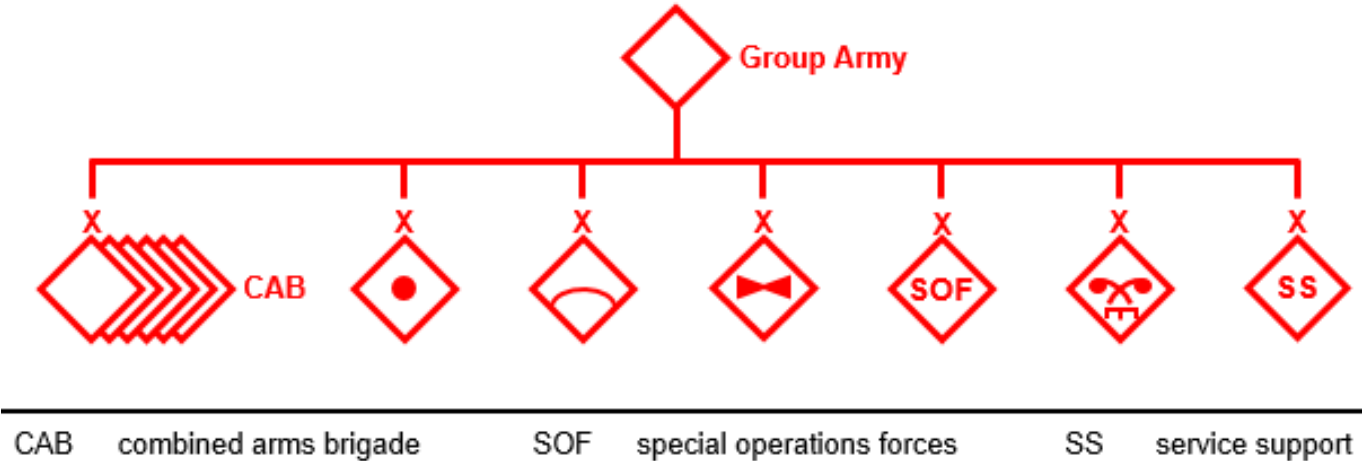
In short, the PLA’s primary focus will remain maintaining its deterrence and defensive posture in Chinese territory and in the near seas, while gradually expanding its expeditionary capability, all done in concert with national economic development.

You mentioned military reforms numerous times - do you think that the Chinese will achieve these goals that they’ve set out for themselves, or might it end up being too much, too soon?

Reforms are always a learning process. The PLA is certainly moving in the direction it wants to go, but the more they try to implement some of these initiatives, the more they discover that these things are harder to do in real-life than it is to write about them in books. In fact, the army in particular has already begun to reform some of their reforms. One good example is standardizing the structure of the group army, their corps-level organization. Two years ago, group armies were standardized with six combined arms brigades and six supporting brigades, one each artillery, air defense, SOF, army aviation (helicopter), engineer and chemical defense, and service support brigade. A recent change they’ve made has been to break up the engineer and chemical defense brigade into two separate brigades: an engineer brigade and a chemical defense brigade. This change isn’t universal yet,—at least one group army has retained the old structure. This series of rapid changes illustrates that they will decide on something, experiment and train with it, and discover what does and does not work. They then must go back and revise based on the lessons learned. Many of these new adjustments are not announced officially and we have to catch glimpses of them in Chinese media reports, making open source analysis ever more difficult.

I’ve said for some time that when the 2020 “deadline” rolls around that the PLA will announce successful completion of reforms, but experimentation and modification will continue. Every time a Chinese unit goes on a field exercise, new equipment, unit structure, tactics, and doctrine are tested. The results of these tests get sent up the chain of command, and then drives change throughout the organization. Running up to the 2035 “deadline”, I anticipate many more significant changes in the PLA, but fewer public announcements.

Regarding that 2035 date, I think it is very likely that the complete overhaul of the PLA’s equipment—begun under Deng Xiaoping back in the early 1980s—will finally be complete. All of the early Cold-War Soviet derived material will finally be gone, replaced by mostly



The group army as it is currently configured. PLAA experimentation on the structure of organizations like this is constant and ongoing.

Chinese-designed equipment dating from the 1990s or 2000s. You can track this replacement in a publication like *The Military Balance*. For example, about two years ago more than half of the Chinese tank force was composed of Type 59 tanks, a Soviet-derived design dating from the 1950s. Today, newer Type 96 and Type 98/99 tanks, designed in the 1990s, slightly outnumber Type 59s. It took some 20 years to move to a majority modern tank types, so it is reasonable to think that it may take another decade at least to finally purge all of the legacy tanks from the inventory. Ironically enough, by that time, some of the early Type 96 and 98 tanks may themselves be obsolete and ready for replacement. The same process is underway for every category of equipment—modernized APCs, IFVs, artillery, helicopters, and so on—with many of the same challenges and similar timelines.

One of the huge upgrades we've seen to PLAA (People's Liberation Army Army) capability in this time period is a series of new systems significantly increasing the range at which ground commanders can strike. Ancient 152mm artillery pieces are being replaced by modernized, longer-range 155mm systems, older multiple rocket launchers are being augmented by highly capable 300-mm multiple launch rocket systems, and attack helicopters and UAVs (Unmanned Aerial Vehicles) have significantly increased their operating radii. While longer range is a valuable, it has several second- and third- order effects that must be considered. Intelligence and targeting must now extend to the maximum range of their capabilities to support the new systems; coordination and communications with other units and with the joint force are now necessary to deconflict airspace, and so on. All of these supporting efforts are ongoing, but it all results in increasingly complex operations that the PLA will have learn on the training field.

One of the things you've written about extensively is the professionalization of the PLAA's NCO (noncommissioned officer) corps. The career NCO is one of the most important components of most western militaries, but the PLAA had virtually no NCO corps to speak of 20 years ago. Could you describe how the PLAA has gone about building a professional NCO corps from scratch, and how that process may look going forward?

Prior to 1998, squad leaders were simply 3rd or 4th year conscripts; NCO leaders weren't a part of the PLAA's personnel system. That year, however, they established their first cohort of professional NCOs, along with the educational and training support necessary to develop them into military leaders and technicians. The first cohort was chosen from the conscript pool and given additional training. Some jobs that previously were assigned to officers were handed off to NCOs, including many billets that we traditionally associate with NCOs, such as supply sergeants. Professional NCOs became squad leaders.

Developing an NCO corps was a huge effort, requiring a number of major reforms and significant resources. The relationship between officers and NCOs had to be established; the duties and responsibilities of NCOs had to be built from scratch; the ranks of NCOs had to be filled by competent soldiers. One of the most significant changes undertaken was the training and education of NCOs. Today, several stand-alone NCO schools exist in which NCO cadets may attend two- or three-year degree programs. Many PLA officer academies have subordinate NCO departments, where NCOs receive both academic instruction and military leadership training. Some NCO positions require significant functional, job-focused technical training as well, which may be done formally or at the NCO's unit.

Figuring out the relationship between NCOs and officers has been a challenge. Higher level NCO leadership positions, such as company first sergeants or sergeants major, have been established only in the last few years. Many of the leadership duties that we typically associate with senior NCOs, such as supervising soldier welfare, morale, and discipline, were traditionally handled by the unit's political officer. The PLA recently added a 7th NCO rank in order to allow more senior NCOs to finish their careers and retire from the military. Last year, the first cohort of PLAA NCOs hit the 20-year mark, which means we are only now seeing the first NCOs who have gone through the new system from the beginning to the end of their careers.

One of the major benefits from the development of the NCO corps is that NCOs now can work in staff positions at battalion and higher level headquarters. The newer PLAA unit structures and approach to operations and planning requires far more staff than previously—a battalion staff used to consist only of a commander, political officer, and deputy commander, for example, which was sufficient when all they had to do was pass higher echelon orders down to their company commanders. Now combined arms battalion are tasked to conduct independent operations, requiring a full range of staff work at that level. The PLAA discovered that staff NCOs can both provide assistance to officers and fill key staff roles. A significant amount of PLAA experimentation over the last few years focused on how the future battalion staff should be structured—getting the right mix of officers, NCOs, and trained specialists, in the right jobs, with the right relationships. At this time, it appears they've landed on a formal structure employing a chief of staff, a unit "master sergeant," and four principal staff officers or NCOs. Of note, while this staff is now probably capable of fighting independently for short periods of time, it does not look to be large enough to be capable of conducting both current operations and planning on a 24-hour, high intensity cycle over an extended period of time.

As I said above, the PLAA is just now seeing its first batch of NCOs go through the new system from beginning to end. It will take time for them to get it right, much as it did for us. The role of the NCO in the US Army has been codified in its modern form for over a century.

One of the elements of the Chinese security apparatus that is most confusing to westerners is the People's Armed Police (PAP).. It doesn't have an equivalent in the US government or in most western nations, but it is a very large and important part of the Chinese system. Could you give a description of the PAP, and how you think it will evolve over the same period of time as the PLA as discussed above?

First, it is important to understand that there really is not an American equivalent organization to the PAP. They are not a military reserve, nor are they a form of National Guard or militia, and they are not “military police” as we know them. The PAP is one of the three elements of the Chinese Armed Forces, along with the PLA and Militia. The PLA is what we think of as a traditional military, focused on external threats, and the Militia, with some exceptions, is an enormous, low-readiness paramilitary organization with limited military capabilities, serving mainly as a source of manpower. The PAP's primary mission is to work with civilian police forces during law enforcement and stability operations internal to China. The PAP also has a secondary mission to support PLA operations, which mostly takes the form of light infantry and security operations. Domestic security missions include crowd control, riot control, and counter-terrorism operations. China sees the division between internal security/law enforcement and external security in much the same way America does, and this is outlined in their national defense law.

We don't have a good estimate of how large the PAP is, but we do know that there are PAP units spread throughout every province in China. During a round of reforms last year, the PAP lost several hundred thousand personnel—mostly border security and security for key natural resources—that were handed off to local civilian governments. At the same time, the PAP assumed control of the Chinese Coast Guard, along with its assortment of maritime missions. My best guess is that the PAP today has around a half million personnel.

The modern PAP era began after their very poor performance during the Tiananmen Square demonstrations in 1989. In the following decades they were reorganized at least twice and re-equipped mainly as a truck-mobile organization reinforced with some armored vehicles, helicopters, and highly-trained special operations units. In addition to the provincial units, a number of well-trained and equipped “mobile units” were established as a mobile reserve, ready to travel and deploy as needed to support provincial units in domestic stability operations.

The big problem that we're having today in understanding the PAP is deconflicting their role in anti-terrorism operations from their role in domestic security and stability. The Chinese aren't helping this confusion with their own procedures—they often train on situations where a peaceful protest devolves into a violent riot overlaid with terrorism or separatist events. These situations require wildly varied sets of capabilities: crowd control is a very different mission from assaulting small groups of armed terrorists. The first requires large numbers of paramilitary personnel, armored and shielded, employing mostly nonlethal weapons to control the behavior of a mostly unarmed crowd, with the objective of ending the protest or demonstration with as few casualties on both sides as possible. Direct action antiterrorism missions, on the other hand, require small units utilizing extremely precise and rapid application of lethal force at an exact time and place. One of the major confusing factors is that both of these unit types are in the same organization, which makes their employment potentially very problematic.

An important aspect of the latest reform was spreading out “mobile units” to the entirety of the country rather than concentrating them in certain areas. This capable reserve force at the provincial level, which American audiences might understand as a Quick or Rapid Reaction Force.

Is it accurate to say that there are three tiers of capability level within the PAP? Elite antiterrorism units, the mobile/mechanized units, and then the local, provincial units?

It is accurate to describe them as having three tiers, but it is important to remember that PAP units receive training in their specific areas of responsibility—this isn't a poorly trained militia. It is tricky to say that one unit type is better trained than another, as their mission sets vary significantly. Under the new organization, provincial PAP units control multiple local internal security units usually based in large cities, plus one or more mobile units capable of moving throughout their area of operations and small SOF units for antiterrorism tasks. Two new large mobile units have been formed, one located in northern China and one in the south; each commands multiple internal security forces that may deploy wherever needed, supported by larger specialized anti-terrorist units (the Snow Leopards and Falcons) and helicopters. Specialized PAP units, such as engineers, have an important role in responding to emergencies like natural disasters. In certain circumstances, the PLA may be called upon to support the PAP, such as responding to a chemical or biological incident or providing transportation.

Is there anything else in particular you'd like to emphasize for the American military training audience?

I'd like to reinforce how many differences there are between the Chinese armed forces and the US military. It is clear that the PLA has studied the US military carefully and has adopted some of our best practices in their own reform efforts, but they are not attempting to become "just like us" because of China's social, political, economic, and geographic circumstances.

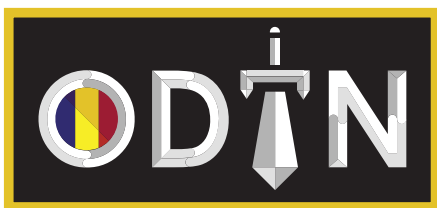
They've also studied Russia and European militaries; how they've performed both in hot wars and peacekeeping operations. They've tried to learn from each country they study and have come up with a

uniquely Chinese solution. There are many reasons for this—China's size, geographic position and terrain diversity—and their political system—are all important factors in their strategy and policy choices. So, though they may mirror what other countries do in some ways, there are a number of important differences in their approach to foreign and military policy.

In the end, the point I often try to leave people with is that the PLA is not the Russian military; they are not the North Koreans; nor are they European or American. They are something completely different, and they will come up with ways of doing things that are very different from what we may expect. ♦

Dennis J. Blasko, Lieutenant Colonel, US Army (Retired), served 23 years as a Military Intelligence Officer and Foreign Area Officer specializing in China.

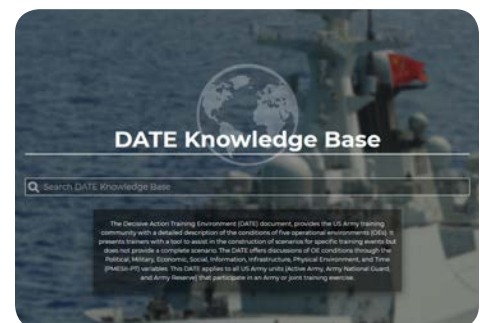
Mr. Blasko was an army attaché in Beijing from 1992-1995 and in Hong Kong from 1995-1996. He also served in infantry units in Germany, Italy, and Korea and in Washington at the Defense Intelligence Agency, Headquarters Department of the Army (Office of Special Operations), and the National Defense University War Gaming and Simulation Center. Mr. Blasko is a graduate of the United States Military Academy and the Naval Postgraduate School. He has written numerous articles and chapters on the Chinese military and defense industries and is the author of the book, *The Chinese Army Today: Tradition and Transformation for the 21st Century*, second edition (Routledge, 2012).

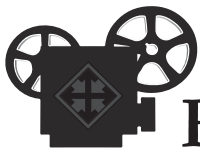


Operational Environment Data Integration Network

ODIN is the authoritative source for DATEs, their accompanying Threat Force Structures, the Worldwide Equipment Guide (WEG), and other threat doctrine publications such as the TC 7-100 series.

<https://odin.tradoc.army.mil/>





FILM REVIEW

Operation Red Sea (2018)

By Kevin M. Freese, OE&TA



Operation Red Sea is a 2018 action film written by Zhuzhu Chen, J. Feng, and Eric Lin. Six production companies were involved, including the PLA Navy Government TV Art. Most of the filming took place in Morocco.¹ The film's director, Dante Lam, is also known for other major Chinese box office successes in Hong Kong as well as mainland China, including the highly successful 2016 action film *Operation Mekong*.²

The movie begins in the Red Sea, where a PLA Navy surface action group with an embarked tier one *Jiaolong* team is conducting counter-piracy operations. The first action (which is

almost non-stop for the majority of the nearly 2.5-hour long film) shows the team dramatically disrupt a pirate attack on a container ship. Soon after, the group is ordered to conduct a noncombatant evacuation operation of Chinese citizens from the fictitious Middle Eastern country Yewaire (a thinly disguised Yemen), which is embroiled in a chaotic civil war. Meanwhile, a Chinese journalist stumbles upon information that the local terrorist group "Zaka" has acquired "yellow cake" and intends to make a radiologic "dirty" bomb.

As the *Jiaolong* team rescues the Chinese embassy staff and Chinese civilians under heavy fire and car bomb attacks, the journalist alerts the team of the dirty bomb plot. However, the team is given a follow-on mission to escort Yewaire civilians to an evacuation point, and the journalist tags along by slipping in among the locals. Zaka ambushes the convoy, killing the local government escorts, all of the civilians except the journalist, and several of the *Jiaolong* team. As a result of the ambush, the surviving team members learn that the terrorists have hostages at a nearby compound, including one Chinese citizen. Despite being severely outnumbered, they infiltrate the compound and successfully rescue the hostages. Although they lose team members in the process, they also gain additional information about the dirty bomb plot. After reinforcements arrive and the hostages are safe, the surviving team members set out on their own and without permission to disrupt the transfer of dirty bomb material. In the end, they succeed, and the fallen members are honored as national heroes. The film jumps forward in time a few months, and then ends as the PLA Navy intercepts an American Navy group that is entering Chinese-claimed waters.

Operation Red Sea is very loosely based on real events. During a period of increased violence in Yemen in March-April, 2015,



the governments of Pakistan, Ethiopia, Singapore, Italy, Germany, Poland, Ireland, Britain, Canada, and Yemen requested Chinese Navy support evacuating their citizens. A Chinese frigate assisted in the rescue of 225 non-Chinese citizens to Djibouti, having previously evacuated 571 Chinese citizens and 8 non-citizen employees of Chinese companies.³

Operation Red Sea is intense, non-stop action from beginning to end. What little character development occurs is formulaic if not clichéd, because that isn't what the film is about – it's about the fight scenes. The film combines realistic fighting with over-the-top stunts that avoid any sense of campiness through persistent, exaggerated, and graphic violence and gore. It does not pull any punches depicting the chaos and confusion of combat.

Operation Red Sea is not really meant to be entertaining; entertainment is the means. The objective is to showcase PLA military capabilities, and the film has it all. There are running gun battles in the street, car bombs, visit, board, search, and seizure operations, close-in ship weapons, mortar attacks, surface-to-air missiles, close air support, explosive drones, naval gunfire, combatives, a sniper duel, and a tank battle. The PLA Navy is shown excelling at all of this.

Operation Red Sea portrays cutting edge military equipment. The *Jiaolong* team uses diverse small arms, including FN Minimi machine guns, Remington 870 compact shotguns, Blaser R93 rifles, Norinco QBU, and FN SCAR-L CQC rifles, CZ 805 G1 grenade launchers, Norinco QSZ-92 pistols, and Glock 9mm variants with silencers.⁴ Navy assets exhibited include the Chinese type 054A Jiangkai II frigate and the type 071 amphibious transport dock.⁵ The *Liaoning* (*Kuznetsov*

class) carrier even makes a cameo, deploying Shenyang J-15 Flying Sharks.⁶

Operation Red Sea is one of a few recent films including *Sky Hunter* (2017), *Wolf Warrior* (2015), and *Wolf Warrior II* (2017) that represent a major paradigm shift in Chinese cinema. Mainland and Hong Kong cinema may be replete with contemporaneous action movies, but modern-day military films are actually anomalous. Traditionally, Chinese war films are period pieces set during WWII at the latest, and are used as a mechanism to promote traditional values.⁷

Perhaps more important than being emblematic of a change in Chinese cinema is simply the fact that the movie was a success. It grossed \$579 million in China, making it the second most financially successful Chinese movie of all time.⁸ This reviewer watched the film on Netflix, which is providing new life to it through streaming audiences.

Operation Red Sea is propaganda. However, it is kind of good propaganda that is worth seeing for those who like extremely violent movies. It is also worth seeing for the Army, as it provides insight into how China – both the government and the people – see their place on the global stage. *Operation Red Sea* depicts China as a country capable of projecting power to remote locations, successfully, with altruism and moral authority. Chinese military personnel appear professional, dedicated, capable, and disciplined, but also with enough independence to do the right thing in the absence of orders. Chinese weapons and tactics are depicted as modern and effective as any used by Chinese competitors such as the US. This is the face of the PLA Navy that China wants to present to the world, and the box office numbers show that the Chinese people ate it up. ♦

1. IMDb, *Operation Red Sea* (2018), https://www.imdb.com/title/tt6878882/?ref_=ttfc_fc_ti.

2. Patrick Frater, "Why Dante Lam's 'Rescue' May Be a Lifeline for the Chinese Movie Industry (EXCLUSIVE)," *Variety*, February 8, 2019, <https://variety.com/2019/film/asia/dante-lam-ed-die-peng-rescue-lifeline-chinese-movie-industry-1203132374/>.

3. Megha Rajagopalan and Ben Blanchard, "China Evacuates Foreign Nationals from Yemen in Unprecedented Move," *Reuters*, April 3, 2015, <https://www.reuters.com/article/us-yemen-security-china/china-evacuates-foreign-nationals-from-yemen-in-unprecedented-move-idUSKB-NOMU09M20150403>.

4. IMDb, *Operation Red Sea*, August 12, 2019, http://www.imdb.com/wiki/Operation_Red_Sea.

5. Charles Clover and Sherry Fei Ju, "New Crop of Chinese War Movies Focuses on Present-Day Geopolitics," *Financial Times*, May 19, 2018, <https://www.ft.com/content/4aaf5fe4-59ba-11e8-bdb7-46677d2e1ce8>.

6. Robert Farley, "Operation Red Sea: The Chinese Public's Introduction to Beijing's New Navy," *Diplomat*, November 28, 2018, <https://thediplomat.com/2018/11/operation-red-sea-the-chinese-publics-introduction-to-beijings-new-navy/>.

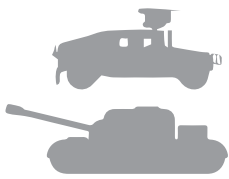
7. Li Yang, "Why 'Operation Red Sea' Isn't Like Other Chinese War Movies," *Sixth Tone*, March 11, 2018, <https://www.sixthtone.com/news/1001880/why-operation-red-sea-isnt-like-other-chinese-war-movies>.

8. Robert Farley, "Operation Red Sea: The Chinese Public's Introduction to Beijing's New Navy," *Diplomat*, November 28, 2018, <https://thediplomat.com/2018/11/operation-red-sea-the-chinese-publics-introduction-to-beijings-new-navy/>.



Chinese aircraft carrier the *Liaoning*.

Source: Baycrest [CC BY-SA 2.5 (<https://creativecommons.org/licenses/by-sa/2.5/>)]; https://commons.wikimedia.org/wiki/File:Aircraft_Carrier_Liaoning_CV-16.jpg



WORLDWIDE EQUIPMENT GUIDE (WEG) SHOWCASE



ZLT-05 (Type 05) Chinese Amphibious Light Battle Tank (LBT)

Tanks and AT Vehicles > Tanks > Amphibious Tank > ZLT-05 (Type 05) Chinese Amphibious Light Battle Tank (LBT)

Tiers:



Notes

The ZLT-05 was publicly revealed in 2006. At that time it was already in service with the PLA Marine Corps. Type ZLT-05 is very similar to the US Expeditionary Fighting Vehicle in concept, though it has heavier armor protection. Additionally, the ZLT-05 has a large welded hull, specially designed for high-speed swimming. The Vehicle is armed with a fully-stabilized 105-mm rifled gun, which is the same gun, found of the Type 63A. With an effective range of over 2,000 meters against armored targets, the ZLT-05 HEAT round can penetrate between 460-500mm of steel. Also, the ZLT-05's main gun can fire APFSDS, HE rounds, and a gun-launched anti-tank guided missiles. Originally developed for the Russian 9M117 Bastion, these laser guided missiles have a maximum range of 5 kilometers and a 90% hit probability against static targets. Secondary armament consists of coaxial 7.62-mm machine gun and another 12.7-mm MG, mounted on top of the roof. The ZLT-05 has a crew of four and can accommodate a additional four troops. The vehicle has a maximum amphibious speed on water of around 45 km/h. Vehicle can travel 10 km or more at sea, however it may not reach the swimming performance of the US EFV. Development and expansion of this new high-speed amphibious vehicle family shows the high level of resources China is devoting towards the amphibious assault capabilities. This vehicle is being proposed for export customers. Its export designation is VN16. This amphibious light tank has been exported to Venezuela

System

Alternative Designation: ZTD-05, ZBD 2000, ZLT-05, VN16
Date of Introduction: 2006
Estimated out of Service Date: 2056
Manufacturer: Norinco
Proliferation: China: over 50, Venezuela: INA
Type: Amphibious Light Battle Tank (LBT)
Family: Type 05
Crew: 4 ea
Maximum Effective Range (Land): 500 km
Maximum Effective Range (Sea): 90 km

Dimensions

Length: 9.5 m
Width: 3.36 m
Height: 3.04 m
Weight, Combat: 28.5 tons
Ground Pressure: INA kg/m

Automotive

Engine Name: INA
Engine Type: Four-stroke turbocharged water-cooled diesel
Engine Power (Land): 500 hp
Engine Power (Sea): 1,577 hp
Transmission: Mechanical
Cruising Range (Land): 500 km
Cruising Range (Sea): INA, estimates have it going as far as 2/3 of it's land range. km
Speed, Maximum Road: 65 km/h
Speed, Average Cross: 40
Speed, Maximum Swim: 25 (Wow that is fast for a IFV) km/h
Maximum Distance at Sea: 90 km
Tracks: Tracks are supported by two return rollers located between the first and last pairs of road wheels.
Suspension: Hydropneumatic
Wheels: 6, unevenly-spaced road wheels per side
Gradient: 60 %
Side Slope: 30 %
Vertical Obstacle: 0.6 m
Trench: 2.9 m
Fording Depth: Amphibious m
Sea State Capable: Sea State 4
Buoyancy Reserve: Yes

Communications

Blue Force Tracker: Yes

TBR-121

VHF Transceiver: Yes
VHF Range: 1 to 50 km
Proliferated: Widely
Digital Data: Yes, Full
Control: Self-Adaptive Control (Including Automatic Antenna Tuner)
Frequency Agile: Yes
Wireless Network Capabilities: Yes
Note: Very similar in capabilities to the US SINCGARS ASIP

Main Gun

System

Name: ZTS63A, or Type 83
Type: 105 mm
Caliber: 44
Rate of Fire: 6-8 rds/min
Bore evacuator: Yes
Maximum Firing Range: 17.2-22 km
Traverse Range: 360 deg
Traverse Left: 180 deg
Traverse Right: 180 deg
Maximum Elevation: +18 deg
Minimum Elevation: -5 deg
Muzzle Brake: Yes
Bore Evacuator: Yes
Loading Type: Manual with a hydraulic ram assistance

Ammunition (Option 1)

Name: BTA2 105mm Projectile
Type: APFSDS
Basic Load: 30 total rounds of 105mm Projectiles rds
Warhead Type: INA
Maximum Effective Range: 2,800 m
Penetration: 220mm of RHA set at 66.4 deg from 2,000 meters

Main Gun (continued)

Ammunition (Option 2)

Name: DTP1A, 105mm Projectile
Type: HEAT
Basic Load: 30 total rounds of 105mm Projectiles ea
Warhead Type: HEAT warhead
Maximum Effective Range: 3,000 m
Penetration: 80mm of RHA set at 60 deg and protected by ERA

Anti-Tank Guided Missile (ATGM)

ATGM Type: HJ-73 Red Arrow Anti-Tank Missile System

HJ-73 Red Arrow ATGM (Option 1)

Name: Red Arrow 73B
Type: Anti-Tank Missile System
Muzzle Velocity: 120 m/s
Maximum Range: 2,800 m
Warhead Type: Tandem-HEAT
Hit Probability: 90 %
Penetration Probability: 80 %
Penetration: 200 mm of RHA set at 68° and protected by ERA

HJ-73 Red Arrow ATGM (Option 2)

Name: Red Arrow 73D
Type: Anti-Tank Missile System
Muzzle Velocity: 130 m/s
Maximum Range: 2,800 m
Warhead Type: Tandem-Heat
Hit Probability: 90 %
Penetration Probability: 80 %
Penetration: 280 mm of RHA set at 68° and protected by ERA

HJ-73 Red Arrow ATGM (Option 3)

Name: Red Arrow 73E
Type: Anti-Tank Missile System
Muzzle Velocity: 135 m/s
Maximum Range: 3,000 m
Warhead Type: Tandem-HEAT
Hit Probability: 90 %
Penetration Probability: 80 %
Penetration: 300 mm of RHA set at 68° and protected by ERA

HJ-73 Red Arrow ATGM (Option 4)

Name: Red Arrow 73F
Type: Anti-Tank Missile System (Bunker Buster)
Muzzle Velocity: 130 m/s
Maximum Range: 2,800 m
Warhead Type: Fuel Air Explosive Warhead
Hit Probability: 90 %
Penetration Probability: 80 %
Penetration: 300 mm of RHA set at 68° and protected by ERA

Coaxial Weapon System

System

Name: Type 80 Chinese Heavy Machine Gun
Manufacturer: Norinco
Type: 7.62mm Heavy Machine Gun
Length, Total: 1,192 mm
Length, Barrel: 658 mm
Diameter: INA
Action: Gas Operated
Rate of Fire: 700-800 rds/min
Feed System: Belts in 100/200/250 round boxes
Sights: Open sights. Optical/Night vision scope can be outfitted.

Ammunition

Type: 7.62×54mmR
Caliber: 7.62x54 mm
Muzzle Velocity: 840 m/s
Basic Load: Belts in 100/200/250 round boxes
Max Range: 100-1,500 m
Min Range: 100 m
Armor Penetration: INA

Commander's Weapon System

System

Name: QJZ-89 or Type 89
Type: 12.7mm Heavy Machine Gun
Manufacturer: NORINCO
Length, Total: 2,119 mm
Length, Barrel: 1,003 mm
Weight (Gun Only): 17.5 kg
Weight, (Tripod Only): 8.5 kg
Max Rate of Fire: 600 rds/min
Sustain Rate of Fire: 400-600 rds/min
Action: Gas/Recoil
Feed System: Belt
Sights: Iron/Optical

Ammunition

Type: Rifle
Caliber: 12.7 mm
Cartridge: 12.7x108 mm
Basic Load: 1,200 ea
Max Effective Range: 1,600 m

Fire Control

Name: BMS System
Computerized FCS: Yes
Thermal Vehicle Commander: Yes
Thermal Gunner: Yes
Main Gun Stabilization: Yes
3D Map of the OE: Yes, Standard
Satellite Navigation System: BeiDou Satellite
Battle Management System: Yes
Navigation System: BeiDou satellite navigation system

Protection

Hull Armor Type: Hull is of aluminium base armor protected by composite appliqué armor.
Hull Armor: 30 mm
Sides and Rear Armor: 14.5 mm
Turret Armor: INA
Applique Armor: Yes
Explosive Reactive Armor: INA
Active Protection System: Yes
Mine Clearing: INA
Self-Entrenching Blade: INA
NBC Protection: Yes
Smoke Equipment: Yes, 8 Total, 4 on each side 76mm
Bow Blade: Yes
Belly Plate: Yes
Self-Sealing Fuel Tank: Yes, capable of stopping a 25 mm APFSDS round at 2,000 m.
Automatic Fire Suppression Device: Yes

Variants

PLZ-07B: The PLZ-07B is an SPH designed for the Chinese Marine Corps. It is based on the Type 05 hull and uses the weapon system from the PLZ-07, which is based on a different hull. The vehicle is designed to have the same mobility and protection as the ZBD-05, however, it is equipped with a large-calibre howitzer and attendant FCS so that it can provide organic indirect fire support for ZBD-05 formations.

Type 001: The Type 001 is an APC based on the Type 05 hull. It is believed that the Type 001 is more likely to be found in service with the amphibious elements of the PLA rather than the Marine Corps, as it has been shown on exercises with the 74th Army Group. It is designed to perform as an APC and is capable of carrying a section of equipped infantry into combat alongside other Type 005 variants.

Worldwide Equipment Guide (WEG)

Equipment Added/Updated Tracker

4th Quarter FY19

Number	Equipment Name	Country	Added	Updated
1	ZTZ-96A Chinese Main Battle Tank (MBT)	China	✓	
2	ZTL-11 Chinese Infantry Fighting Vehicle (IFV)	China	✓	
3	ZTZ-99A Chinese Main Battle Tank (MBT)	China	✓	
4	Z-9 Harbin (WZ-9) Gun Ship Chinese Medium Multi-Role	China		✓
5	Z-19 Chinese Attack Helicopter	China	✓	
6	Z-10 Chinese Attack Helicopter	China		✓
7	YW534 Type 89 Chinese Armored personnel Carrier (APC)	China	✓	
8	YW31H Type 85 Chinese Armored Personnel Carrier (APC)	China		✓
9	Yitian TY90 Chinese Short-Range Air-Defense (SHORAD)	China	✓	
10	PLL-01 Chinese 155mm Towed Artillery	China	✓	
11	AH-4 Chinese 155mm Towed Lightweight Gun / Howitzer	China	✓	
12	PHL-03 Chinese Multiple Rocket Launcher	China	✓	
13	ASN-209 Chinese MAME Unmanned Aerial Vehicle	China	✓	
14	CSK-141 Chinese 4x4 Tactical Vehicle	China	✓	
15	FB-6A Chinese Mobile Short Range Air Defense System	China	✓	
16	FN-6 Chinese Man Portable Air Defense System (MANPADS)	China	✓	
17	WZ551 Chinese 6x6 Wheeled Armored Personnel Carrier (APC)	China	✓	
18	WZ 523 Type 05P Chinese 6x6 Wheeled Armor Personnel Carrier (APC)	China	✓	
19	WS-3 Chinese 400mm Guided Multiple Launcher Rocket System	China	✓	
20	Wing Loong I Chinese Medium-Altitude Long Endurance (MALE) Unmanned Aerial Vehicle (UAV)	China	✓	
21	Wing Loong II Chinese Medium-Altitude Long Endurance (MALE) Unmanned Aerial Vehicle (UAV)	China	✓	
22	Wing Loong ID Chinese Medium-Altitude Long Endurance (MALE) Unmanned Aerial Vehicle (UAV)	China		✓
23	Dongfeng Warrior EQ2101 Chinese 6x6 Truck	China	✓	
24	VT5 Type 15 Chinese Light Tank	China	✓	
25	VT4 (MBT3000) Chinese Main Battle Tank	China	✓	
26	VP10 Chinese 8x8 Armored Personnel Carrier (APC)	China	✓	
27	CS/VP3 Chinese Mine-Resistant Ambush Protected (MRAP)	China	✓	
28	VN17 Chinese tracked Infantry Fighting Vehicle (IFV)	China	✓	
29	VN11 Chinese Infantry Fighting Vehicle (IFV)	China	✓	
30	ZBD-03 (WZ506) Chinese Airborne Infantry Fighting Vehicle (IFV)	China	✓	
31	VN3 Chinese Reconnaissance Vehicle	China	✓	
32	VN1 (ZBL09) Chinese 8x8 Armor Personnel Carrier (APC)	China	✓	
33	VN18 (ZBD-05) Type 05 Chinese Amphibious Infantry Fighting Vehicle (AIFV)	China	✓	
34	Type 90 Chinese Towed Air Defense Gun	China	✓	✓
35	T-55AMV Russian Main Battle Tank (MBT)	China	✓	✓
36	Type 83 Chinese 152mm Self-Propelled Howitzer	China	✓	✓
37	Type 59D Chinese Main Battle Tank (MBT)	China	✓	✓
38	Type 59G Chinese Main Battle Tank (MBT)	China	✓	
39	Tiger 2065 Armored Personnel Carrier (APC)	China	✓	
40	SR5 Chinese Guided Multiple Launch Rocket System (GMLRS)	China	✓	
41	SH3 Chinese 122mm Self Propelled Howitzer (SPH)	China	✓	
42	SH2 Chinese 122mm Self Propelled Howitzer (SPH)	China	✓	
43	SH1 Chinese 155mm Self Propelled Howitzer (SPH)	China	✓	
44	HJ-73 (Red Arrow-73) Chinese Man Portable Anti-Tank Guided Missile (ATGM) System	China	✓	
45	HJ-10 Red Arrow 10 Chinese Anti-Tank Guided Missile (ATGM)	China	✓	
46	HJ-9 Red Arrow 9 Chinese Anti-Tank Guided Missile (ATGM)	China	✓	✓
47	PLZ-07 (Type 07) Chinese 122mm Self Propelled Artillery	China	✓	
48	PLZ-05 (Type 05) Chinese 155mm Self-Propelled Howitzer	China	✓	

Continued on next page...

Worldwide Equipment Guide (WEG)

Equipment Added/Updated Tracker (continued)

4th Quarter FY19

Number	Equipment Name	Country	Added	Updated
49	PLZ-45 (Type 88) Chinese 155mm Self-Propelled Howitzer (SPH)	China	✓	
50	PLL-09 Chinese 122mm Self-Propelled Howitzer (SPH)	China	✓	
51	PLL-05 (Type 05) Chinese 120mm Self-Propelled Mortar Howitzer (SPMH)	China	✓	
52	GCZ-110 Chinese Engineer Vehicle	China	✓	
53	GSL-130 Chinese Mine Clearing Vehicle	China	✓	
54	MBT-2000 (Type 90-11) Chinese Main Battle Tank (MBT)	China		✓
55	Al-Khalid Chinese/Pakistan Main Battle Tank (MBT)	China		✓
56	HQ-9 Chinese Long Range, Ground Based Mobile Air and Missile System	China	✓	
57	T-72 Russian Main Battle Tank (MBT)	Russia		✓
58	Type 63A (ZTS63A) Chinese Amphibious Light Tank	China		✓
59	Chonma-ho (Pegasus) North Korean Main Battle Tank (MBT)	North Korea		✓
60	T-90 Russian Main Battle Tank (MBT)	China		✓
61	T-90K Russian Main Battle Tank (MBT)	Russia	✓	
62	T-80B Russian Main Battle Tank (MBT)	Russia		✓
63	T-80U Russian Main Battle Tank (MBT)	Russia		✓
64	T-80BK Russian Main Battle Tank (MBT)	Russia	✓	
65	T-80UK Russian Main Battle Tank (MBT)	Russia	✓	
66	T-80UD Russian Main Battle Tank (MBT)	Russia	✓	
67	T-90A Russian Main Battle Tank (MBT)	Russia		✓
68	Challenger 2 (FV4034) British Main Battle Tank (MBT)	Great Britain		
69	ZTZ-96A Chinese Main Battle Tank (MBT)	China		
70	T-64B Russian Main Battle Tank (MBT)	Russia		
71	T-64BK Russian Main Battle Tank (MBT)	Russia	✓	
72	T-64BV Russian Main Battle Tank (MBT)	Russia	✓	
73	T-64 BM Bulat Ukrainian Main Battle Tank (MBT)	Ukraine	✓	
74	T-64U Ukrainian Main Battle Tank (MBT)	Ukraine	✓	
75	T-64BV Model 2017 Ukrainian Main Battle Tank (MBT)	Ukraine	✓	
76	Leopard 2 German Main Battle Tank (MBT)	Germany		✓
77	Leopard 2A4 German Main Battle Tank (MBT)	Germany	✓	
78	Pz 87 (Panzer 87) Switzerland Main Battle Tank (MBT)	Switzerland	✓	
79	Pz 87WE (Panzer 87 Werterhaltung) Switzerland Main Battle Tank (MBT)	Switzerland	✓	
80	Type 96 (ZTZ96) Chinese Main Battle Tank (MBT)	China		✓
81	Type 96A (ZTZ-96Gai) Chinese Main Battle Tank (MBT)	China	✓	
82	Type 96B (ZTZ96B) Chinese Main Battle Tank (MBT)	China	✓	
83	T-55AMV Russian Main Battle Tank (MBT)	Russia		✓
84	Chieftain MK 5 British Main Battle Tank (MBT)	Great Britain		✓
85	2S1 (Gvozdika) Russian Self-Propelled Howitzer (SPH)	Russia		✓
86	2S3 Akatsiya (M1973) Russian 152mm Self-Propelled Howitzer (SPH)	Russia		✓
87	2S3M1 Russian 152mm Self-Propelled Howitzer (SPH)	Russia		✓
88	2S19 Msta Russian Self-Propelled Howitzer (SPH)	Russia		✓
89	2S19M1 (Msta-SM1) Russian Self-Propelled Howitzer (SPH)	Russia		✓
90	2S19M2 (Msta-SM2) Russian Self-Propelled Howitzer (SPH)	Russia	✓	
91	QN-506 Chinese Fire Support Vehicle (FSV)	China	✓	
92	YW-531 (Type 63) Chinese Armored Personnel Carrier (APC)	China		✓
93	2S35 Koalitsiya-SV Russian Self Propelled Howitzer (SPH)	Russia		✓
94	2S35-1 Koalitsiya-SV-KSh Russian Self Propelled Howitzer (SPH)	Russia	✓	
95	2S23 Nona-SVK Russian 120mm Self-Propelled Mortar System (SPMS)	Russia		✓
96	2S5 Giatsint-S Chinese 152mm Self-Propelled Howitzer (SPH)	China		✓

Continued on next page...

Worldwide Equipment Guide (WEG)

Equipment Added/Updated Tracker (continued)

4th Quarter FY19

Number	Equipment Name	Country	Added	Updated
97	2S9-1 Russian 120mm Self-Propelled Mortar (SPM)	Russia		✓
98	2S9 NONA Russian 120mm Self-Propelled Mortar (SPM)	Russia		✓
99	BMD-1 Russian Airborne Amphibious Infantry Fighting Vehicle (IFV)	Russia	✓	
100	BMD-1K Russian Airborne Amphibious Infantry Fighting Vehicle (IFV)	Russia	✓	
101	BMD-1P Russian Airborne Amphibious Infantry Fighting Vehicle (IFV)	Russia	✓	
102	2S9-1M Russian 120mm Self-Propelled Mortar (SPM)	Russia	✓	
103	SH1 Chinese 155mm Self Propelled Howitzer (SPH)	China		✓
104	SH2 Chinese 122mm Self Propelled Howitzer (SPH)	China		✓
105	SH3 Chinese 122mm Self Propelled Howitzer (SPH)	China		✓
106	Type 83 Chinese 152mm Self-Propelled Howitzer	China		✓
107	G6 Rhino South African 155mm Self-Propelled Howitzer (SPH)	South Africa		✓
108	GCT (AUF1) French 155mm Self-Propelled Gun (SPG)	France		✓
109	GCT (AUF1-TA) French 155mm Self-Propelled Gun (SPG)	France	✓	
110	Caesar French 155mm Self-Propelled Howitzer (SPH)	France		✓
111	M-1978 Koksan North Korea 170mm Self-Propelled Gun (SPG)	North Korea		✓
112	M-1989 Koksan North Korea 170mm Self-Propelled Gun (SPG)	North Korea		✓
113	ZBL-09 (Type 09) Chinese 8x8 Armor Personnel Carrier (APC)	China		✓
114	ZTL-11 Chinese Infantry Fighting Vehicle (IFV)	China		✓
115	ZZH-09 (Type 09) Chinese 8x8 Armor Personnel Carrier (APC)	China	✓	
116	ZBD-04 (Type 4) Chinese Infantry Fighting Vehicle (IFV)	China		✓
117	ZBD-04A (Type 4) Chinese Infantry Fighting Vehicle (IFV)	China		✓
118	VN17 Chinese tracked Infantry Fighting Vehicle (IFV)	China		✓
119	ZBD-05 (Type 05) Chinese Infantry Fighting Vehicle (IFV)	China		✓
120	ZSL-92 (WZ551) Chinese 6x6 Wheeled Armored Personnel Carrier (APC)	China		✓
121	ZBD-03 (WZ506) Chinese Airborne Infantry Fighting Vehicle (IFV)	China		✓
123	ZTL-11 Chinese Infantry Fighting Vehicle (IFV)	China		✓
124	Dongfeng EQ2101 Chinese 6x6 Tactical Vehicle	China		✓
125	V-150 American Light Armored Vehicle (LAV)	America		✓
126	AMX-10P French Infantry Fighting Vehicle (IFV)	France		✓
127	MILAN 1 French Anti-Tank Guided Missile (ATGM)	France	✓	
128	MILAN 2 French Anti-Tank Guided Missile (ATGM)	France	✓	
129	MILAN 3 French Anti-Tank Guided Missile (ATGM)	France	✓	
130	MILAN 2T French Anti-Tank Guided Missile (ATGM)	France	✓	
131	MILAN ER French Anti-Tank Guided Missile (ATGM)	France	✓	
132	AMX-10P Marines French Infantry Fighting Vehicle (IFV)	France	✓	
133	AMX-10 PAC 90 French Infantry Fighting Vehicle (IFV)	France	✓	
134	FN MAG French 7.62mm General Purpose Machine Gun	France	✓	
135	AMX-10RC Renove French Armored Reconnaissance Vehicle (ARV)	France	✓	
136	AMX-10RC French Armored Reconnaissance Vehicle (ARV)	France		✓
137	AMX-10P French Infantry Fighting Vehicle (IFV)	France	✓	
138	Marder 1A3 German Infantry Fighting Vehicle (IFV)	Germany		✓
139	Rheinmetall MG 3 German General Purpose Machine Gun	Germany	✓	
140	Marder 1A5 German German Infantry Fighting Vehicle (IFV)	Germany	✓	
141	BMD-3 Russian Airborne Amphibious Infantry Fighting Vehicle (IFV)	Russia		✓
142	9M113 Konkurs Russian Anti-Tank Guided Missile (ATGM)	Russia		✓
143	RPK-74 (AK-47) Russian Assault Rifle	Russia	✓	
144	AGS-17 Russian Automatic Grenade Launcher	Russia		
145	PKT Russian 7.62mm Machine Gun	Russia		✓