Adapting and overcoming is a hallmark of Marines. The emergence of strategic competitors in China and Russia coincides with an evolving character of warfare driven by social, informational, and technological changes that require us to adapt our thinking to match the evolving circumstances of the current era. As the Marine Corps pursues Force Design, we need to leverage wargames, analyses, experiments, and exercises, to examine and refine how we apply our most valued and time-tested warfighting theories and concepts to meet the challenges of 21st-century competition and warfare. The words of our 29th CMC, Gen Al Gray, say it best: “Like war itself, our approach to warfighting must evolve. If we cease to refine, expand, and improve our profession, we risk becoming outdated, stagnant, and defeated.” This article provides a way of thinking about one of our most important and enduring warfighting concepts—combined arms—as it should be applied in today’s environment to create dilemmas for our competitors and enemies.

The Changing Character of Combined Arms

MCDP 1, Warfighting, states, “Combined arms is the full integration of arms in such a way that to counteract one, the enemy must become more vulnerable to another. We pose the enemy not just with a problem, but with a dilemma—a no-win situation.” These words from Warfighting capture why we conduct combined arms, and they remain as applicable today as in any previous century. In short, we follow the doctrine of combined arms to maximize combat power through the use of all available resources to best advantage. Through combined-arms tactics, we integrate fires, maneuver, and information by using complementary forces to put a competitor or enemy in a no-win situation.

Current events show us that the character of combined arms is changing in three primary ways. First, continuing advancements in information and related technologies, particularly in the areas of cyberspace, space, and influence technologies like social media, provide a widening array of capabilities that can be combined to generate advantages. Integrating these information capabilities with maneuver and lethal fires to present a dilemma at the right time and place is key to 21st-century combined arms. To illustrate the expanding use of technology, consider the near-realtime view of the unfolding conflict in Ukraine that we have all witnessed through various media. The widespread use of social media to livestream battles was unfathomable 20 or 30 years ago, but today demonstrates the power of using information as a means of exploiting tactical events to mobilize public opinion and galvanize will on a national or global scale.

Second, the delivery of combined arms has changed a great deal due to the mature precision-strike regime (MPSR). Integrating this level of precision into combined arms is changing how competitors and enemies approach warfighting. The proliferation of the MPSR places a premium on winning the all-domain reconnaissance and counter-reconnaissance fight. The actor who wins this fight can apply combined arms, with the loser suffering the consequences. Furthermore, the actor who best exploits the massive amounts of data generated by the widespread proliferation of sensors gains a tremendous advantage in the reconnaissance and counter-reconnaissance fight. The side which can make sense of the data faster than the other will find and engage targets faster than the other. In this way, the reconnaissance and counter-reconnaissance fight, and therefore combined arms in the 21st century, presents a “big data” exploitation challenge.

The third change we are witnessing is the use of combined arms across the competition continuum. Understanding this change requires adopting an expanded concept of combined arms that makes it as applicable below the violence threshold as it is above. We see examples of this at work in places where
our competitors create dilemmas against their neighbors who are allied with the United States, and where the competitor seeks objectives without triggering a military response from the targeted nation, or the United States. For example, the People’s Republic of China (PRC) is employing fishing boats and the coast guard to “seize” territory in disputed nearby seas while the People’s Liberation Army Navy provides overwatch. The scheme presents a dilemma: choose to attack the encroaching fishing boats and risk war, or do not interfere and allow the PRC to establish positions that advance its claims and objectives.

**Toward a Refined Model of Combined Arms**

If our frame for understanding 20th-century combined arms involved combining supporting arms, organic fires, and maneuver, then our frame for 21st-century combined arms should involve combining supporting arms, organic fires, maneuver, and information. Information is added as a component of 21st-century combined arms because it underpins many of the changes underway in broader society, the global security environment, and in the Marine Corps. The digital transformation of our networked society and Marine Corps is characterized by hyper-connectivity, mass data storage and computational power, and the fusion and correlation of data to drive outcomes. These information-based changes introduce vulnerabilities and opportunities that were not possible in previous decades. In response to this new reality, the Marine Corps established the information warfighting function to formalize an approach to leveraging the power of information in campaigning, operations, and combined arms.

The specific purpose of the information warfighting function derives from our maneuver warfare theory and practice of combined arms as a key means of gaining advantage. MCDP 8, Information, states “the purpose of the information warfighting function is to create and exploit information advantages as a means of achieving our objectives as effectively as possible.” Information, like all other warfighting functions, can be thought of as an activity that Marines perform to generate advantages and effects—no different than when Marines generate advantages and effects through fires and maneuver. Information activities encompass the four functions of information: generation, preservation, denial, and projection. All Marine Corps units can create and exploit information advantages by generating, preserving, denying, and projecting information more effectively than a competitor or enemy. Through combined arms, Marines integrate the functions of information, and associated capabilities, with fires and maneuver to create no-win situations for our competitors and enemies. To illustrate the discussion, Figure 1 provides a model of 21st-century combined arms.

A key feature of Figure 1 is the concept of information fires and information maneuver. Within combined arms, we can think about and apply information as a form of fires and as a form of maneuver. An example of information fires is conducting a cyberspace or electromagnetic attack to deceive the enemy or destroy the enemy’s critical systems. An example of information maneuver is altering, suppressing, or manipulating electronic, digital, or physical signatures to deceive the enemy, reveal or conceal a capability or movement, or to slow the enemy’s decision making. There are many examples of information fires and information maneuver. Table 1 provides a non-exhaustive list of examples for Marines to consider in planning. It is up to the creativity of Marines to combine all available capabilities and lethal and non-lethal actions to create 21st-century combined-arms dilemmas.

Implementing a refined model of combined arms requires the Marine Corps to continue learning through wargames, analyses, experiments, and exercises. The DOD, Joint Force, other Services, and the interagency are all developing new technologies, capabilities, and formations dedicated to long-range precision fires and a wide variety of information capabilities that fall into a range of categories (e.g., space, cyberspace, influence). What is eluding

---

**Figure 1. Moving from 20th-century to 21st-century combined arms.** (Figure provided by authors.)

**Table 1. Examples of Information Fires and Information Maneuver.** (Table provided by authors.)
all parties, however, is a focus toward developing a coherent concept of combined arms, applicable across the competition continuum, which seamlessly fuses fires, maneuver, and information for maximum advantage and effect (i.e., to create dilemmas below or above the threshold of armed conflict).

A dedicated wargaming and experimentation effort must be pursued to develop a mature understanding of how this 21st-century model works. To focus our learning, the Marine Corps should wargame and experiment with this concept to inform all types of MAGTF missions, including missions envisioned for Stand-in Forces (SIF).

21st-Century Combined Arms and the MEU

The MEU is well trained and equipped to perform 21st-century combined arms. To illustrate how the MEU can perform 21st-century combined arms, consider a hypothetical MEU mission to strike and eliminate a high-value individual (HVI) (e.g., key leader, technical expert, financier) within a violent extremist organization (VEO). In this scenario, the MEU creates a combined arms dilemma by using one capability to deny the HVI use of a critical asset, another to track the HVI, and yet another to strike and eliminate the HVI when the individual attempts to access, use, or repair the asset. This technique of “herding” individuals to a specific location to address a problem exposes them to physical harm.

In this example, the MEU—working under the authority of the combatant commander, and in concert with applicable intelligence agencies and the Department of State—is assigned the mission to disrupt a VEO’s online media operations. The VEO’s core leadership group is located in a relatively small and geographically isolated area within the MEU’s reach. However, its media operations, to include its propaganda and recruitment efforts, are highly sophisticated and effective at projecting an outsized image through a global online presence. This presence has proved effective at increasing the group’s support, funding, and influence, and thus represents a growing threat.

For this mission, the MEU receives intelligence on the physical locations of the VEO’s media production studio, primary server, and backup server. These three assets are located in two separate buildings approximately three miles apart. At the designated time, the MEU’s cyber planner coordinated with USCYBERCOM, through the geographic combatant commander, to initiate the pre-planned denial of service attack (a form of information fires) against the VEO’s servers. At the same time, the MEU’s psychological operations detachment delivers tailored messages via cell phone (a form of information maneuver) to the VEO’s chief of media operations (the HVI). These carefully crafted, pre-approved messages are consistent with the HVI’s language, culture, and current events in the local area. This makes the HVI unsuspecting when notified of the malfunctioning servers.

As the cyber-attack and deceptive messaging occur, MEU reconnaissance teams occupy positions to observe and report on all relevant activity at the two locations. A cascade of rapidly unfolding events is triggered when the HVI arrives at the primary site to investigate the server issue. These events begin with the reconnaissance report notifying the MEU commander of the HVI’s arrival. The commander’s decision to strike unleashes two orbiting F-35’s waiting to deliver ordinance on both locations. The no-win situation created by this scenario is either accepting disrupted media operations or attempting to repair and suffer physical harm and destruction. The strike results in eliminating the HVI, several support personnel, and destroys the buildings housing the studio and both servers.

21st-Century Combined Arms in SIF Sea Denial Operations

SIF deter our adversaries by establishing forces that persist forward alongside allies and partners within a contested area. These forces provide the fleet, joint force, interagency, and allies and partners more options for countering an adversary’s strategy. When directed, SIF perform sea denial operations to support fleet maneuver and operations. SIF support sea denial through the application of both organic sensors and weapons and integration with naval and joint sensors and weapons. Achieving this requires SIF that are capable of conducting combined arms in all warfighting domains and the electromagnetic spectrum.

To illustrate how SIF can combine fires, maneuver, and information to create dilemmas in sea denial operations, we use another hypothetical scenario where conflict erupts between the United States and a competitor turned enemy. The dilemma created in this scenario is the enemy’s inability to counter a friendly force electromagnetic attack, which renders the enemy more vulnerable to precision strike.

In this scenario, a Marine Littoral Regiment (MLR) maritime fires element occupies key maritime terrain sufficient for conducting long-range precision fires in the vicinity of a critical chokepoint. While maneuvering to the objective (key maritime terrain) the fires element relies on combined arms to occupy the position undetected, and then again when conducting fires against the enemy.

Moving undetected is a result of winning the counter-reconnaissance fight. Prior to conflict, the SIF succeeded in uncovering and mapping out the enemy’s collection methods, capabilities, and techniques in the area of and surrounding the key maritime terrain. Knowing how the fires element would be collected upon, the plan to maneuver is supported by tactical deception, astute timing to exploit known gaps in the enemy’s collection windows, offensive cyber operations (OCO), and physical attacks to divert the enemy’s attention away from the unit’s maneuver to the objective.

In this example, the MLR has in place the plans to use OCO, which includes pre-approved authorities and permissions. The fires element coordinates with the MLR headquarters’ cyberspace operations cell (a component of regimental fires and effects), to ensure that the timing of the OCO mission supports their movement. The OCO mission specifically targets the one remaining signals intelligence as-
set the enemy had been collecting in the vicinity of the objective. The cyber planner at the MLR headquarters facilitates the OCO mission through pre-coordinated joint fires channels and through the combatant commander.

In occupying the firing position and in conducting the firing mission, the maritime fires element uses passive and active signature management techniques (which are a form of information maneuver) to suppress and manipulate their physical and electromagnetic signatures. Passive measures include the use of communications discipline, concealment, and camouflage. Active measures include the use of decoys to deceive enemy collection.

At the precise time, the firing unit executes long-range precision fires in combination with joint forces. The timing is critical to mass several different munitions from air, surface, and land-based systems against the enemy surface target. This joint combined-arms operation includes airborne electromagnetic attack from close-in unmanned aerial systems and from manned stand-off jamming aircraft to reduce the enemy’s defenses against the MLR’s strike. The inability of the enemy ship to counter joint force electromagnetic attacks reduces the ship’s defenses and makes the ship vulnerable to precision strike.

Upon completion of the fire mission, the MLR unit immediately displaces from its position using combined arms to support movement to a pre-designated hide position. Movement is facilitated by a pre-approved concept of operations that includes the use of joint electromagnetic protection and attack capabilities designed to screen the MLR’s movement against known collection threats. In this scenario, the MLR unit coordinates with the MLR headquarters’ electromagnetic spectrum operations cell to synchronize the timing of the joint screening action with diversionary attacks to cover the MLR’s movement from the firing position to the hide position.

**Combined Arms and Reconnaissance and Counter-reconnaissance**

An operating environment characterized by the proliferating MPSR places a premium on gaining and maintaining contact with potential adversaries. The actor who sees first can orient first, decide first, and attack effectively first, gaining a tremendous advantage. This idea is a core principle in the SIF’s theory of success, and it establishes reconnaissance and counter-reconnaissance as a SIF enduring function that enables combined arms.

SIF provide the Joint Force with access to the host nation and perform all domain reconnaissance on every point of the competition continuum. These mutually supporting essential tasks help the fleet and joint partners establish target custody and develop an understanding of a potential adversary’s activities and capabilities. This allows the Joint Force to identify and counter a potential adversary below the violence threshold, and if armed conflict does begin, allows the joint force to take the initiative and attack first. SIF conduct counter-reconnaissance to uncover potential adversary collection methods and capabilities. This is done to deny the potential adversary’s ability to understand and locate SIF, thereby creating an operational problem for the competitor or enemy.

The reconnaissance and counter-reconnaissance fight is characterized primarily as a contest between two opposing systems each trying to observe and know what the other is doing while preventing the other side from doing the same. This means the reconnaissance and counter-reconnaissance fight is effectively a battle for information and actionable intelligence. The crux of SIF maritime reconnaissance is to help the fleet locate the potential adversary or the enemy sufficiently to deliver effective firepower. The key to maritime reconnaissance is fusing all domain collection capabilities into a coherent real-time intelligence picture. This requires developing and executing an intelligence collection plan that employs a wide variety of collection capabilities, to include open-source intelligence, publicly available information, and ally and partner capabilities, to gain and maintain target custody and complete kill webs. All domain reconnaissance also requires fusing the MLR’s organic human intelligence and signals intelligence from ground locations with combatant commander and national level collection capabilities employed via the space and cyberspace domains.

A requirement of any actor employing the MPSR is to conceal the capabilities of sensors and the exact methods of employing their kill webs. In support of counter-reconnaissance operations, SIF find opponent sensors and understand enemy kill webs oriented on the fleet. History provides many examples of using creative and deceptive tactics to cause the adversary to reveal sensors and expose capabilities. For example, during the Cuban Missile Crisis, the United States combined the use of a specialized transmitter from a Navy destroyer with the release of radar reflecting balloons from a Navy submarine to stimulate Cuban air defense radars. The mission successfully caused Cuba to employ their radar and subsequently revealed previously unknown characteristics and capabilities of the system to U.S. intelligence.

Using similar creative tactics, SIF, working in concert with the Joint Force and allies and partners must devise ways of causing potential adversaries/enemies to reveal their methods and capabilities of collection. This begins with leveraging a persistent presence of SIF in ally and partner nations, which over time allows for the observation of patterns of life and patterns of collection used by a potential adversary and around the host nation. Upon establishing a baseline understanding, SIF resolve gaps in understanding by stimulating the rival’s sensors, causing them to reveal capabilities or collection techniques.

Actions may involve deliberately using SIF formations to conduct regular predictable movements and activities over an extended period of time to condition the potential adversary’s expectations of friendly force patterns. This can include using exercises to integrate and coordinate with host nation forces, U.S. Coast Guard vessels, inter-agency organizations, or the MEU. To stimulate the potential adversary, SIF may conduct unexpected movements, or unexpected engagements with local
leaders, with the intent of observing changes in the opponent’s collection activities and posture.

Counter-reconnaissance also involves activities by SIF to prevent the potential adversary or enemy from locating the fleet. If SIF are engaged in armed conflict, any maneuver of combined arms may be used to deny, defeat, or destroy the enemy’s collection capabilities. This may include combining physical attack and maneuver with OCO or electromagnetic spectrum operations to engage and destroy critical enemy command and control nodes within their MPSR. The seeds of successful SIF counter-reconnaissance operations during armed conflict are sown well before conflict erupts. The proliferation of the MPSR means our competitors have developed robust, multi-layered, and redundant intelligence, surveillance, and reconnaissance networks to enable precision strike. SIF forces must be present and tasked to penetrate the potential adversary’s MPSR and hold any segment of the kill web at risk, to include communications links, nodes, and weapons systems.

21st-Century Combined Arms in Competition Below Armed Conflict

The widespread improvement of intelligence, surveillance, reconnaissance, and targeting capabilities by peer competitors is a fundamental characteristic of the MPSR. Rivals use the MPSR as a hedge against long-held U.S. power projection advantages. This provides potential adversaries cover to pursue coercive strategies against neighboring countries who are often allies or partners of the United States. There is no clearer example of this than the PRC’s efforts to work under the protection of their MPSR to undermine U.S. strategy and change the balance of power in East Asia. Aside from the PRC, the United States is also challenged by other strategic competitors such as Russia, Iran, and VEOs—all of whom seek to present dilemmas that challenge the United States by using the MPSR as cover for coercive activities.

The MAGTF is by design an effective counter to competitors endeavoring to undermine U.S. objectives using the MPSR as cover. This is especially true when MAGTFs coordinate their actions with a host nation, other MAGTFs, joint forces, and interagency partners like the Department of State and the Coast Guard. To illustrate, we introduce another hypothetical scenario where a MEUcoordinates action with the Amphibious Ready Group (ARG), host nation, combatant commander, Department of State, and the Coast Guard to stymy a potential adversary’s illegal territorial claims over a key international trade route.

This potential adversary has been conducting a small boat harassment campaign targeting international cargo vessels transiting a narrow but heavily trafficked shipping lane. In this scenario, the potential adversary uses the cover of their MPSR to employ a network of fast small boats to conduct high-speed approaches and near misses to harass transiting vessels. The objective of the harassment campaign is to slow the movement of these vessels and disrupt trade. The specific dilemma is: engage the small boats and risk escalation or suffer the economic consequences of trade and supply chain disruptions. While this campaign results in international criticism, the lack of an effective response signifies an inability to oppose the potential adversary’s long-term pursuit of a territorial fait accompli.

In response to this dilemma, the MEU is tasked for a period of 30 days to disrupt the small boat harassment campaign, without triggering armed conflict, to facilitate the free flow of trade through international waters. The goal of the MEU-led mission is to create a dilemma for the potential adversary, such that the more they pursue harassment, the more harmful it becomes to achieving their territorial ambitions. The mission involves the MEU planning and coordinating the effort to find, fix, track, interdict, disrupt, and then expose (through various media) the harassing swarms of small boats.

To accomplish this, the ARG vessels with embarked MEU, the Coast Guard cutter, and two host-nation coast guard vessels position themselves in the straits to demonstrate resolve through physical presence. The Coast Guard vessels patrol in international waters nearest the potential threat. ARG vessels patrol in international waters between the Coast Guard vessels and commercial ships transiting the straits. This highly visible presence coincides with a significantly ramped-up strategic messaging campaign that involves regular joint statements and press briefings held by senior U.S. and host nation government leaders. The messaging campaign highlights the strengthening ties between the U.S. and the host nation to ensure freedom of navigation in international waters.

For 30 days the MEU S-2 fuses intelligence from ARG sensors, Coast Guard sensors, theater and national assets, and organic MEU aviation assets to maintain maritime domain awareness in the contested zone. Integrating these assets provides a multi-layered network of sensors that gives indications and warnings of small boat swarm formation on the
near shores of the potential adversary. Early warning is key to tracking and interdicting the swarm. Upon finding, fixing, and tracking the swarm, the interdiction begins with the host nation coast guard and Coast Guard vessels moving to intercept the swarm formation before they can approach a commercial ship. As the coast guard vessels approach the swarm, a MEU UAS is piloted to fly over the small boat swarm. The UAS is equipped with video recording equipment and a radio frequency jamming payload.

Using a pre-approved concept of operations with authorities and permissions from the combatant commander, the UAS is used to record the swarm and jam its radio communications. Jamming disrupts the ability of the swarm commander to direct and coordinate action. The simultaneous arrival of host nation and Coast Guard vessels causes the harassing swarm to lose cohesion and abandon its mission. This interdiction concludes with the MEU releasing video footage of the harassing swarm, along with a combined public statement from the MEU, ARG, Coast Guard, and host nation coast guard commanders. This public statement is followed up and reinforced by additional public statements and press briefings by U.S. and host nation senior leaders.

To communicate additional resolve, the Coast Guard interdiction, disruption, and exposure operation is conducted against the backdrop of a MEU combined-arms demonstration exercise with the host nation. Images and videos from both the interdiction mission and the combined-arms demonstration are used to illustrate resolve in a multimedia campaign.

Conclusion

To compete and fight effectively in the 21st century, the Marine Corps must adapt to the evolving security environment by applying a modern approach to 21st-century combined arms. The combined arms approach is how the Marine Corps executes maneuver warfare. Rapid, flexible, and opportunistic maneuver can only be accomplished by a combined arms force and through a diversity of means that maximizes combat power, flexibility, and responsiveness. The Marine Corps’ success in the 20th century was characterized by mastery of combined arms. However, in today’s ever-changing environment, there exist many more capabilities that must be combined. This includes a wide range of new information capabilities that we employ in all the domains of warfighting.

Current events show us that the character of combined arms changes as precision strike networks proliferate in a hyper-connected world. The MPSR provides U.S. competitors the cover they need to apply coercive strategies below the threshold of armed conflict. By deterring escalation, the MPSR helps competitors achieve their objectives incrementally, with the goal of imposing their will on targeted neighbors without triggering a response from the victim nation or the United States. Additionally, the MPSR makes it feasible to quickly find and strike targets across large swaths of geographic space. This requires gathering and exploiting huge quantities of data to achieve and maintain target quality tracks. Fusion and correlation of data through massed storage and computation establish decision speed, focus, and scale as key characteristics of 21st-century combined arms. Succeeding in data fusion and exploitation means the winning side will experience the faster decision speeds needed to focus a widening array of available capabilities that can be combined to generate advantages at scale over an opponent.

This challenge sits at the core of winning in all domains. Both our SIF and traditional MAGTFs must be manned, trained, and equipped to win this fight, across all points of the competition continuum. Creating combined-arms dilemmas, and then exploiting success to achieve decision in battle, is the foundation of maneuver warfare. In the 21st century, we must move toward a refined combined-arms model to ensure we do not become stagnant in our thinking and tactics. We must recognize that information, as a warfighting function, is a pillar of combined arms. We must employ every ounce of creativity and tactical acumen to combine every capability in new ways, to generate advantages and fulfill our role as the Nation’s expeditionary force-in-readiness in the 21st century.

Notes

3. Ibid.
4. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Ibid.