Red Diamond
Threats Newsletter

TRADOC G-2 Operational Environment Enterprise
Analysis & Control Element Threats Integration

Fort Leavenworth, KS **Volume 8, Issue 10** **October 2017**

INSIDE THIS ISSUE

North Korean UAVs 3
Snow Dome Pt 3 7
Area Defense..... 14
Loitering Munitions 29
ACE-TI POCs..... 32

OEE *Red Diamond* published by TRADOC G-2 OEE ACE Threats Integration

For e-subscription, contact:
Nicole Bier (DAC),
Intel OPS Coordinator,
G-2 ACE-TI

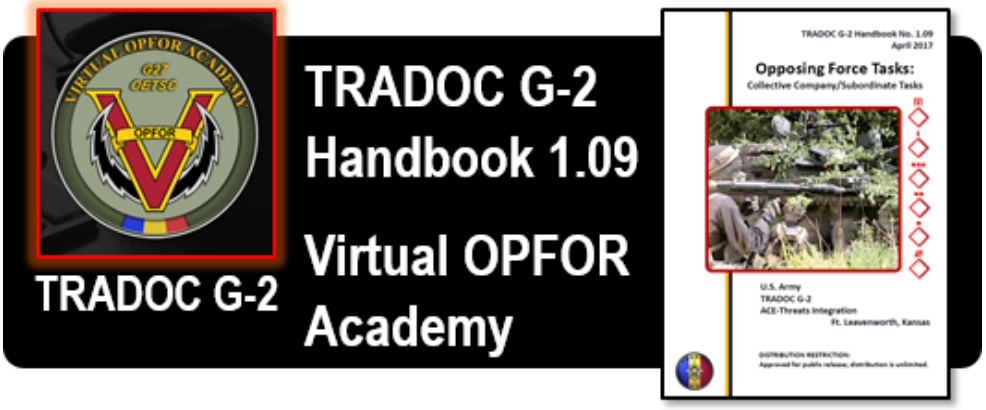
Topic inquiries:
Jon H. Moilanen (DAC),
G-2 ACE-TI
or
Angela Williams (DAC),
Deputy Director, G-2 ACE-TI

Copy Editor:
Laura Deatrick (CGI CTR),
G-2 ACE-TI

TRADOC G-2 VIRTUAL OPFOR ACADEMY

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration (DAC)

A key opposing force (OPFOR) resource for US Army training readiness is the TRADOC G-2 Virtual OPFOR Academy (VOA) on the TRADOC G-27 Training Support Center website. Among the many training, professional education, and leader development resources related to an OPFOR found in the VOA, a recently added training aid is TRADOC G-2 Handbook 1.09, Opposing Force Tasks: Collective Company and Subordinate Tasks. This handbook contains 17 revised OPFOR tactical tasks and drills as posted in the US Army Combined Arms Training Strategies (CATS). These tasks are formatted in the "Objective T" format as task, conditions, standards, and performance measures for effective training readiness. Additional OPFOR tasks will be revised in the future.



For access to OPFOR tasks and drills in the TRADOC G-2 Virtual OPFOR Academy, go to https://tbr.army.mil/index.html. You can also access the VOA on milSuite with common access card entry at https://www.milsuite.mil/book/groups/voa.

RED DIAMOND TOPICS OF INTEREST

by TRADOC G-2 ACE Threats Integration

This issue of *Red Diamond* opens with an article on North Korean unmanned aerial vehicles (UAVs). It is estimated that the country has no more than 1,000 UAVs in its inventory. The North Koreans primarily test and modify imported UAVs, but it is likely that they are starting to develop their own. This article reviews platforms that are commonly found in the country's inventory.

The next article is part three of a series on the Russian Snow Dome. It discusses the Russian approach to strategic-, operational-, and tactical-level anti-access/ area denial: the ways and means available to Russian commanders to deny their opponents the ability to mass combat power prior to an engagement. It discusses how Russian commanders at the theater, operational command, and brigade levels integrate capabilities to create a kind of "exclusion zone" designed to attrite, disrupt, or deter enemy actions within their area of operations.

Area defense is a threat tactic to deny key areas or access to key terrain by an enemy. Threat actions focus on attacking key components of the enemy's combat system at selected times and locations that cause the most effective disruption, defeat, and destruction of an enemy. Area defense is designed to achieve a successful outcome by forcing an enemy's offensive operations to culminate before he can achieve his objectives, or by denying an enemy his objectives while preserving friendly forces' combat power. The third article explains the tactical concept of area defense and provides a vignette illustrating its use by an opposing force brigade tactical group.

Loitering munitions, also known as suicide drones or "kamikaze" drones, are a capability typically representative of more advanced regular threat actors. They have a dual-use capability that combines tactical surveillance with the destructive effects of a guided missile. The fielding of these systems is expected to steadily increase as miniaturization of precision-guided munitions and micro platforms continue to improve. The final article reviews Iranian development and proliferation of such weapons and their associated technology.

UNMANNED AERIAL VEHICLE ASSESSMENT:

NORTH KOREA

by Nicole Bier (DAC) and Patrick Madden (BMA CTR), TRADOC G-2 ACE Threats Integration

This is the first in a series of country unmanned aerial vehicle (UAV) assessments based exclusively on open-source information. This first article provides an overview of North Korea's broad UAV capabilities. The next article in this series will cover Iranian UAVs.

It is estimated that North Korea (NK) has 1,000 or fewer total UAVs in its inventory.[1] The North Koreans primarily test and modify imported UAVs, but it is likely that they are starting to develop their own. NK has portable UAV launcher capabilities comparable to the Soviet/Russian Zil-130 cargo trucks (Figure 1). Due to the North Korean's mountainous terrain, their UAV inventory includes a significant number of runway independent UAVs that can be catapult or rocket launched from the ground or from a vehicle-mounted rail. The potential for NK to modify various types and classes of UAVs into intelligence, surveillance, and reconnaissance (ISR) or one-way strike assets exists. Expect NK to use low-altitude and short- to medium-range-capable UAVs for ISR and basic target acquisition (TA) operations, as well as possible attack missions in a mass kamikaze-style formation using light weapons or biological and chemical agents.[2] North Korean UAVs can carry munitions, but specific types of munitions are unknown. Some North Korean UAVs flying into South Korea are a spotted light-blue/dark-blue pattern with a dark nose for camouflage purposes.

Figure 1. Soviet/Russian Zil-130 truck with UAV launch capability (left) and assessed North Korean one-way strike UAVs, similar to an MQM-107D, on Zil-130 truck chassis (right)

A review of open-source reports indicates that the North Koreans use various types and classes of UAVs, but it is assessed that they regularly train with and operate the MQM-107D, ASN-104, Pchela-1T (Shmel-1), and Sky-09P (there are at least nine Sky-09 variants). Their UAV inventory also includes the DR-3, Durumi, and Panghyon I/II—all with similar capabilities—and emerging reports suggest the Durumi is a multi-role UAV (e.g., ISR and TA). The North Koreans are developing the Banghyun-5 UAV, which is designed to carry radiological material for use as a dirty bomb.[3] They also tested high explosives on the US-made MQM-107D, a variant now out of production in the US; this aircraft and other variant(s) manufactured under different names by multiple manufacturing companies are used for training in the US.[4] The MQM-107D was originally exported to Syria or Egypt, then resold to NK.[5] North Korea may also be manufacturing or replicating a Sky-09 variant and reverse engineering other platforms.[6] Micro-sized unmanned aircraft with limited endurance, such as the Phantom series, are not addressed due to insufficient open-source reports indicating NK's use of these across the demilitarized zone. General information about North Korean UAVs is shown in Table 1.

Operational Echelon	Imports	Modifications/ Variants	Mission	Launch and Recovery
Strategic (Theater)	MQM-107D (US-made, proliferated throughout the Middle East)	Multiple modifications/ variants	Strike and TA	Rocket-assisted take off (RATO) and parachute recovery
Operational (Corps)	ASN-104 (Chinese)	Multiple modifications/ variants	ISR and TA	RATO and skid belly recovery
Tactical (Division and below)	ASN-104 (Chinese) Pchela-1T (Russian) Sky-09P (Chinese)	Multiple modifications/ variants for the all three	ISR and TA	RATO/catapult launch and skid belly/parachute recovery

Table 1. Example of North Korean UAVs[7]

Figure 2. US MQM-107E during a US exercise in the early 2000s

UAV	Maximum Gross Take-Off Weight (lbs)	Maximum Speed (miles/hr)	Endurance (min)	Maximum Altitude (ft)	Launch and Recovery
MQM-107D/E	1,460	631	138	40,000	RATO/vehicle mounted and parachute recoverable

Table 2. US MQM-107D/E parametric data

Figure 3. Chinese ASN-104 UAV; the wing and vertical stabilizer have 201 markings, but aircraft characteristics cross-referenced with open-source databases confirm this is an ASN-104

UAV	Maximum Gross Take-Off Weight (lbs)	Maximum/ Cruise Speed (miles/hr)	Endurance (min)	Maximum Range (miles)	Maximum Altitude (ft)	Launch and Recovery
ASN-104	309	127/93	120	62	10,500	RATO (assessed to be vehicle launch capable) and skid belly/parachute recoverable

Table 3. Chinese ASN-104 parametric data

Figure 4. Russian Pchela-1T/Shmel-1 UAV

UAV	Maximum Gross Take-Off Weight (lbs)	Maximum Speed (miles/hr)	Endurance (min)	Maximum Range (miles)	Maximum Altitude (ft)	Launch and Recovery
Pchela-1T/ Shmel-1	304	112	120	37	8,200	RATO (vehicle mounted) and parachute recoverable

Table 4. Russian Pchela-1T/Shmel-1 parametric data

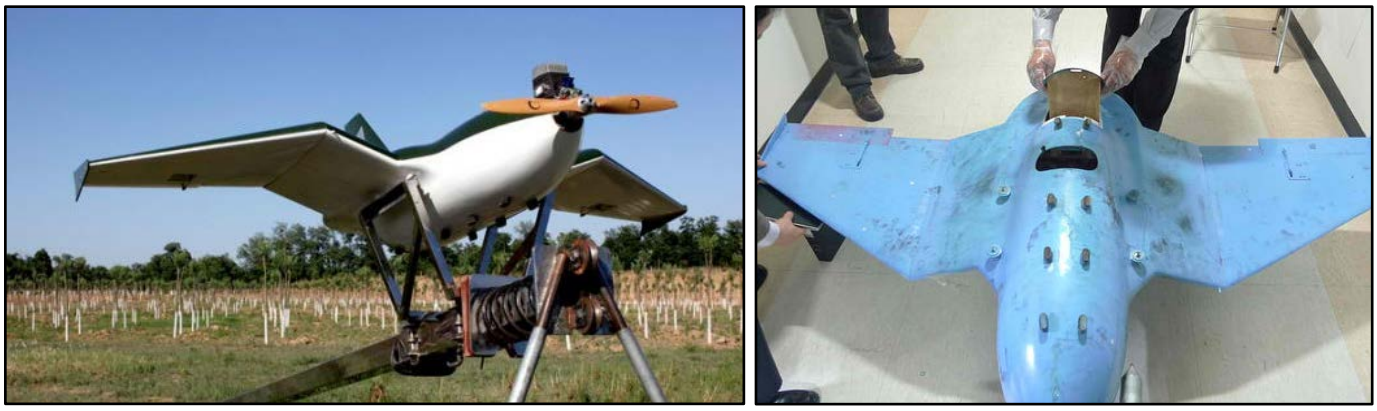


Figure 5. Chinese Sky-09P UAV (left) and Underside of a Chinese Sky-09P UAV found in South Korea (right)

UAV	Maximum Gross Take-Off Weight (lbs)	Cruise Speed (miles/hr)	Endurance (min)	Maximum Range (miles)	Maximum Altitude (ft)	Launch and Recovery
Sky-09P	26.5	62 Wind resistance speed=24	180	19	13,120	Catapult and parachute recoverable

Table 5. Chinese Sky-09P parametric data

Parametric data provided in Tables 2–5 portray current information from reputable commercial open-source databases and will be included in the next update of the Worldwide Equipment Guide (WEG). Due to the evolving nature of unmanned aircraft, capabilities change and new variants are produced. Additionally, the WEG introduces UAV parametric information according to the International Systems of Units, whereas this article provides UAV parametric information according to the US measurement system for convenience.

Notes

[1] David Choi. "North Korea Reportedly has a Fleet of 1,000 Drones it can use for Chemical Attacks." Business Insider. 30 March 2017; Ju-min Park. "South Korea Finds Apparent North Korean Drone near Border." Reuters. 9 June 2017; Joseph S. Bermudez Jr. "North Korea Drones On." 38 North. 1 July 2014; Sputnik. "Inside North Korea's Secret UAV program." Defence Talk. 19 January 2016.

[2] Ryan Pickrell. "South Fears North Korean Drones could unleash Terror from the Sky." The Daily Caller. 29 March 2017.

[3] Ryan Pickrell. "South Fears North Korean Drones could unleash Terror from the Sky." The Daily Caller. 29 March 2017; Kyle Mizokami. "Experts: North Korea May be developing a Dirty Bomb Drone." Popular Mechanics. 28 December 2016.

[4] Brian Whitaker, Project Director, Air Defense Artillery Targets PEOSTRI, PM ITTS, Targets Management Office. Email correspondence with Nicole Bier. 11 October 2017; Association of Unmanned Vehicle Systems International (AUVSI): All Things Unmanned. "AUVSI." 2017. (Account required)

[5] Sputnik. "Inside North Korea's Secret UAV program." Defence Talk. 19 January 2016; Joseph S. Bermudez Jr. "North Korea Drones On." 38 North. 1 July 2014; Robert Johnson. "REPORT: North Korea is rebuilding these US Drones and Strapping them with High Explosives." Business Insider. 7 February 2012.

[6] Sputnik. "Inside North Korea's Secret UAV program." Defence Talk. 19 January 2016; Joseph S. Bermudez Jr. "North Korea Drones On." 38 North. 1 July 2014; Jeffrey Lin and P.W. Singer. "North Korea's New Drones are Chinese (which opens a New Mystery)." Popular Science. 24 April 2014.

[7] Data sources: Association of Unmanned Vehicle Systems International (AUVSI): All Things Unmanned. "AUVSI." 2017. (Account required); Shephard (Media) Plus. "Datasets: Unmanned Systems." 2017. (Account required)

The Snow Dome, Part 3
Integrated Anti-Access/ Area Denial

by Brad Marvel, TRADOC G-2 ACE Threats Integration (CGI Federal CTR)

Through the summer and fall of 1990, the world watched as the United States and its allies massed nearly a million combat troops on the southern border of Iraq. This force buildup was meticulous, time consuming, and resource heavy: it included several heavy armor/mechanized divisions, fixed- and rotary-wing attack aviation, and heavy air defense systems. All the while, Iraqi forces sat just across the border, constructing entrenchments and fortifications, watching and waiting for the inevitable attack. When it finally came, all of their preparations were utterly inadequate: their command structure and most important theater-level assets were devastated by an air campaign, leaving their ground forces adrift and leaderless. After only three days of fighting, the Iraqi army—thought to be one of the most capable in the world—had surrendered.[1]

Figure 1. F-15E Strike Eagles during Operation Desert Shield; over 2,200 coalition aircraft were deployed as a part of the operation

The Desert Storm campaign as a whole is an excellent historical example of applying the principle of force concentration. Coalition forces were almost completely unmolested in their buildup, allowing coalition commanders to precisely position their forces to achieve overmatch at the time and place of their choosing. The Iraqi army surrendered the initiative to the coalition and, as a result, was completely unable to effectively defend against the combined arms assault. Desert Storm showed the world that America and its allies, when given the time to carefully assemble combat power, were virtually unbeatable, even when deployed across huge distances. Almost immediately, military thinkers in America's peer and near-peer competitors took in the hard lessons learned by the Iraqi army and developed a new set of strategies. Instead of focusing on resisting coalition ground forces at the tactical level, they instead looked much broader, focusing on disrupting or preventing the buildup of forces in the first place.[2] The Department of Defense responded by naming (and then quickly unnaming) these strategies "anti-access/area denial," or A2AD.[3]

The general concept of A2AD is nothing new. Historical examples are numerous: The Sixth Coalition attempted to impede Napoleon from concentrating all of his forces in defense of France; Imperial and then Nazi Germany attempted to interdict troop buildups across the Atlantic with U-boats and maritime attack aircraft; Soviet strategy versus NATO relied heavily on interdicting troop movements across the Atlantic.[4] These strategies were very limited, however, by the range and combat power of the weapon systems available at the time. This changed dramatically at the end of the 20th century and at the beginning of the 21st, as two key technological developments proliferated almost simultaneously: network warfare and precision long-range munitions. These systems enabled a nation pursuing an A2AD strategy to project power effectively across hundreds of miles without the need for manned aircraft, ground forces, or a naval presence. Almost overnight, A2AD went from being simply a good idea to being a viable strategy and a serious threat.

Most A2AD literature today focuses on the strategic level of war and on the Pacific Area of Responsibility (AOR).[5] As such, A2AD has been broadly categorized as a strategic problem that requires strategic solutions. Only recently has the idea of tactical- and operational-level A2AD emerged as a significant issue, and even then the problem is still not well-framed.

Figure 2. Chinese ballistic missiles are highly effective anti-access weapon systems

This article discusses the Russian approach to strategic-, operational-, and tactical-level A2AD: the ways and means available to Russian commanders to deny their opponents the ability to mass combat power prior to an engagement. It discusses how Russian commanders at the theater, operational command, and brigade levels integrate capabilities to create a kind of "exclusion zone" designed to attrite, disrupt, or deter enemy actions within their area of operations (AO).

This three-dimensional exclusion zone is described as a "Snow Dome," evoking an image of a trinket encased in a watertight plastic half-sphere. This comparison is useful, but also somewhat misleading: the Russian Snow Dome is really a series of mutually supporting capabilities that create defense in depth from a combined arms effect. It is perhaps more accurate to picture a series of interlocked capabilities radiating outward from a critical asset, rather than a single impenetrable layer.

Why the Snow Dome?

The Russian concept for area denial can be traced to summer 1941, in the early days of Operation Barbarossa. A poorly trained, poorly equipped, and poorly led Red Army faced a combined arms onslaught from what was, at that time, the world's premier land force—the Wehrmacht. The German blitz of the Soviet Union combined rapid maneuver, air power, and artillery so effectively that the Red Army was virtually unable to effectively resist. Through a combination of willpower, sacrifice, and military brilliance, the Soviet Union gradually reversed German gains and eventually pushed them all the way back to Berlin. The lessons learned from this—history's largest and most destructive conflict—colored Soviet and Russian military thinking all the way to the present day.

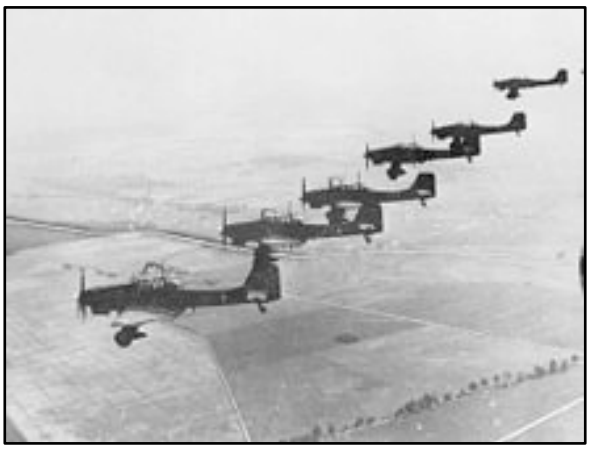


Figure 3. The Ju-87 Stuka is often used as a symbol of WWII-era blitzkrieg tactics; lessons learned defeating the Wehrmacht continue to color Russian military thinking to this day

The Soviet commanders who faced—and learned from—the decisive effects of massed artillery and air power throughout the early days of Barbarossa placed a huge emphasis on three key areas:

1) **Achieving local air superiority.** The Second World War in general showed the world what air power could accomplish. Soviet commanders recognized that effective maneuver warfare virtually required air superiority over the critical parts of the battlefield. Having lived through the brutal effectiveness of the Blitzkrieg air attack, Soviet commanders devoted enormous resources to winning control of the air over key battles. This fear of air power never left the Soviet/Russian psyche, which helps to explain why Soviet/Russian forces invested so heavily in air defense capabilities throughout the Cold War and into the 21st century.[6]

2) **Winning the artillery battle.** As outlined in part 2 of this series, Russian and Soviet commanders traditionally relied very heavily on artillery. Barbarossa was no different in this regard, except that Red Army artillery was initially badly outmatched by the Wehrmacht. Enormous emphasis was placed on rebuilding the Red Army's artillery capability, with good effect: By 1944, the Red Army featured the largest and most effective artillery corps on the planet. With this superiority in firepower, Soviet commanders were reliably able to neutralize or destroy enemy artillery via counterfire, then create windows of opportunity for maneuver forces to exploit.[7]

3) **Integrating fires and maneuver across the battlefield.** "Deep Battle" evolved as the primary Soviet operational concept during WWII; it endured through the entirety of the Cold War and beyond. Deep Battle required precise coordination between fires (both air and artillery) and a variety of maneuver elements in order to mass fires on critical targets at the right time. This process of coordination was greatly refined by the Red Army at the end of WWII, then moved right along into Red Army Cold War doctrine.[8]

The Snow Dome concept can be thought of as a development of Deep Battle with one major difference: it is defensive in nature. Russian military thinking today is dominated by the need for security within the Russian sphere of influence. Russia's military has only a limited expeditionary capability; as such, Russian strategists view any possible confrontation with a peer opponent as a fundamentally defensive exercise.[9] Russia also views its military as a powerful deterrent and source of diplomatic leverage: Potential opponents are made to believe that their cost of action will be too high relative to the possible gains, and thus potential offensive actions are discouraged before they begin.

The Snow Dome was, in large part, developed to support this two-part vision of security and deterrence. Russia saw the devastating effect of US/NATO combined arms operations in the Gulf War and responded by building a force specifically to counter US/NATO strengths. Instead of attempting to match the US/NATO capability-for-capability, Russia instead sought out more asymmetric solutions, which manifested in both tactical and strategic A2AD. The Snow Dome is one of these solutions.

Describing the Snow Dome

The basic description of the Snow Dome is a set of mutually supporting capabilities that create a combined arms effect intended to deter enemy attack or inhibit the free accrual of enemy combat power. Capabilities that contribute to the Snow Dome include, but are not limited to:

- Medium- and long-range air defense systems;
- Mobile short-range air defense (SHORAD) systems;
- Man-portable air defense (MANPADS) systems;
- Manned and unmanned aircraft;
- Tube and rocket artillery;
- Direct fire/maneuver systems;
- Ballistic and cruise missiles; and
- Information warfare (INFOWAR), with particular emphasis on cyber and electronic warfare.

Figure 4. The SS-26 is a short-/medium-range ballistic and cruise missile system; the ballistic missile can perform dramatic terminal phase maneuvers, intended to defeat anti-ballistic missile interceptors

Each one of these capabilities reinforces or supports others, mitigating weaknesses or gaps through all domains. Air defenses create localized air superiority from the ground, dissuading or neutralizing air and missile attacks on Russian forces. Artillery stands off enemy artillery and maneuver forces, defending fragile and highly visible air defense assets from enemy suppression efforts. Maneuver forces defend air defense and artillery forces from ground attack. Ballistic and cruise missiles attack the highest-value targets at extended ranges on land and at sea. Electronic warfare protects key systems such as radars and communications from electronic attack, while simultaneously disrupting enemy electronic emitters. Other INFOWAR elements reinforce the psychological deterrent effect of all forces and seek to disrupt enemy systems with cyber and information attack. The result is a three-dimensional geographic area wherein there are no significant weaknesses for an enemy to exploit. The objective of the Snow Dome is not to completely prevent enemy attack. Rather, it is to make attack so costly that a deterrent effect is achieved or, if deterrence fails, to attrite and suppress the enemy so effectively that he is unable to close with and destroy Russian ground forces in close combat.

The Snow Dome by Echelon

Brigade Tactical Group (BTG)

At the BTG, the primary missions for Snow Dome participants are to disrupt the buildup of enemy combat power at the brigade level, to attrite enemy forces as they maneuver, and to deny the use of key terrain—particularly valuable airspace—to enemy commanders. Key contributors at this echelon include:

- MANPADS: SA-24/25;
- SHORAD systems: SA-13, SA-19;
- Tube and rocket artillery: 2S19 self-propelled gun (SPGs), BM-21/27 multiple rocket launchers (MRLs);

- Direct fire/maneuver systems; and
- Electronic warfare (EW).[10]

The BTG's Snow Dome extends across its AO. The BTG commander relies on MANPADS and SHORAD to deter or defeat low-altitude fixed- and rotary-wing air attack; perhaps more importantly, these systems must defeat enemy surveillance from small unmanned aircraft. Artillery systems' primary roles in this scenario are counterfire and fire support: Counterfire falls largely to rocket systems, while fire support falls to tube systems. Maneuver forces defend both air defense and artillery systems from ground attack, while electronic warfare enables Russian electronic emitters while disrupting enemy systems. The primary intent of the Snow Dome at this echelon is to disrupt enemy forces' lower echelons (battalion and below) as they attempt to close with and destroy the BTG.

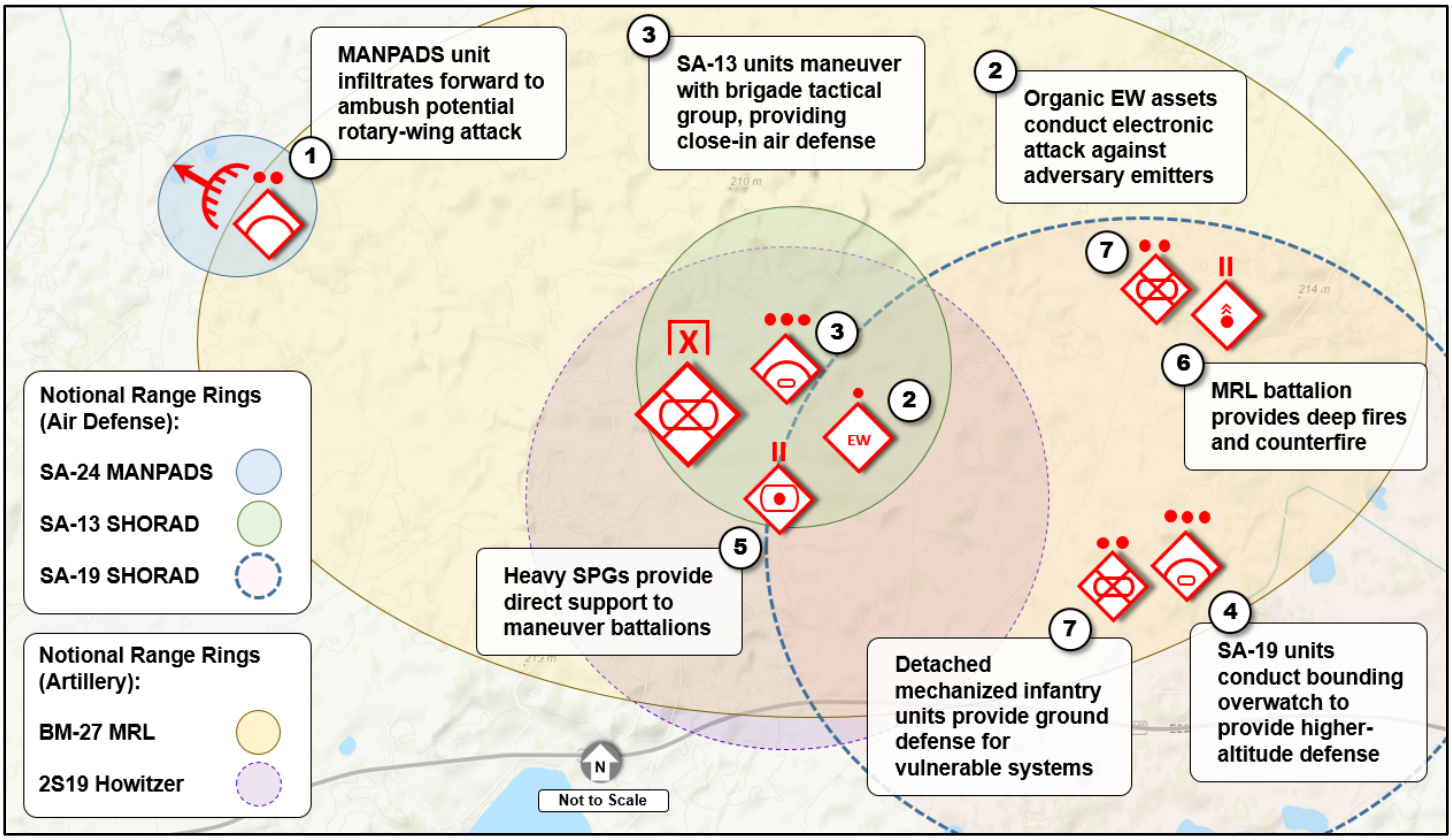


Figure 5. The Snow Dome at the BTG echelon; note how each weapon system fills a specific role while simultaneously offsetting a weakness or vulnerability of another system

Operational Command

At the operational command (the first echelon above brigade),[11] weapons systems that comprise the Snow Dome are larger, more expensive, less common, and more lethal. Their primary roles are to support subordinate units (BTGs) as required and fill in spaces between BTGs. Key contributors at this echelon include:

- SHORAD systems: SA-19/22;
- Medium-range air defense systems: SA-11/17;
- Tube and rocket artillery: 2A65 towed howitzers, BM-30 MRL;
- Direct fire/maneuver systems; and
- INFOWAR: EW and cyber warfare.

Air defense systems are a blend of short- and medium-range missile systems. Artillery is rocket-heavy to support the reinforcing fires mission, the counterfire mission, and the long-range precision strike mission. At this echelon, offensive systems target enemy deep critical operational-level assets such as headquarters, assembly areas, and supply areas. This echelon introduces a cyber warfare and other INFOWAR elements that operate within the operational command AO,

including a more robust EW capability. The primary intent of the Snow Dome at this echelon is to impede brigade-sized elements from effectively concentrating combat power and from conducting resupply/reorganization, while simultaneously providing reinforcing fires to subordinate BTGs.

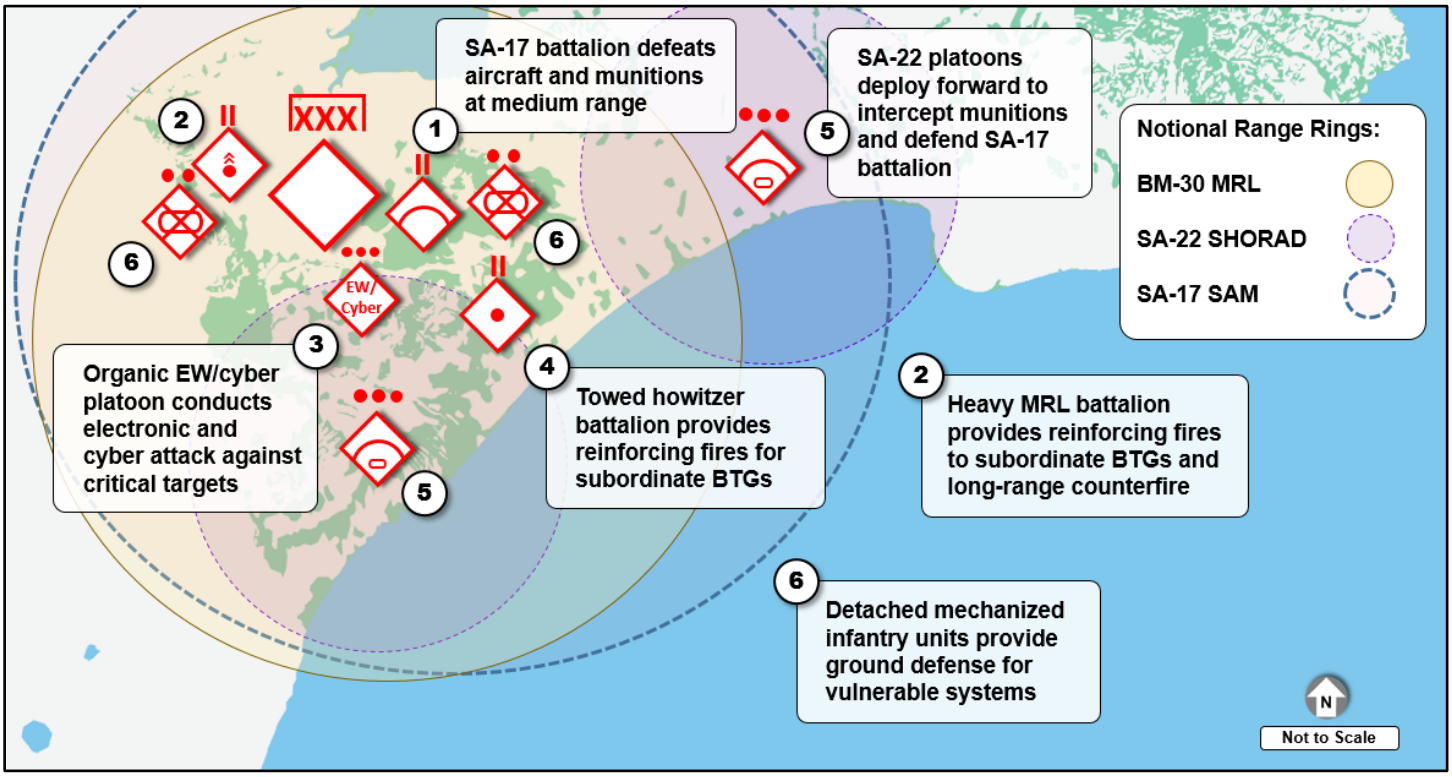


Figure 6. The Snow Dome at the operational command echelon; this Snow Dome covers a much wider geographic area than do the BTGs, restricting or deterring enemy operations over the entirety of the operational command's AO

Theater/Military District

At the theater level, the Snow Dome extends to encompass large parts of a given AOR. Weapon systems are large, expensive, and vulnerable, but have the range and lethality to significantly affect entire campaigns. Key contributors at this echelon include:

- SHORAD system: SA-22;
- Medium-range air defense system: SA-17;
- Long-range air defense systems: SA-20/21;
- Rocket artillery: BM-30;
- Short-range ballistic missile (SRBM) and land attack cruise missile: SS-26;
- Anti-ship cruise missile (ASCM): Kh-35;
- Direct fire/maneuver systems; and
- INFOWAR: EW and cyber warfare.[12]

Air defense systems are a mix of medium- and long-range systems: medium-range systems overlap/protect long-range systems from low-altitude air threats and munitions, while long-range systems inhibit and threaten hostile aircraft hundreds of miles away. Long-range surface-to-surface shooters, including both rockets and ballistic missiles, stand off enemy fires systems and threaten high-value targets across the theater. Cyber and other INFOWAR elements are larger and more capable, ready to conduct either targeted or mass operations anywhere in the theater. This echelon's primary goal is to impede enemy access to the entire theater and to restrict its freedom of maneuver long before the enemy can organize and close with tactical forces. Theater-level targets include air and seaports, major assembly areas, high-level headquarters, regional networks and communications, high-performance aircraft, and surface ships, both embarked and in port.

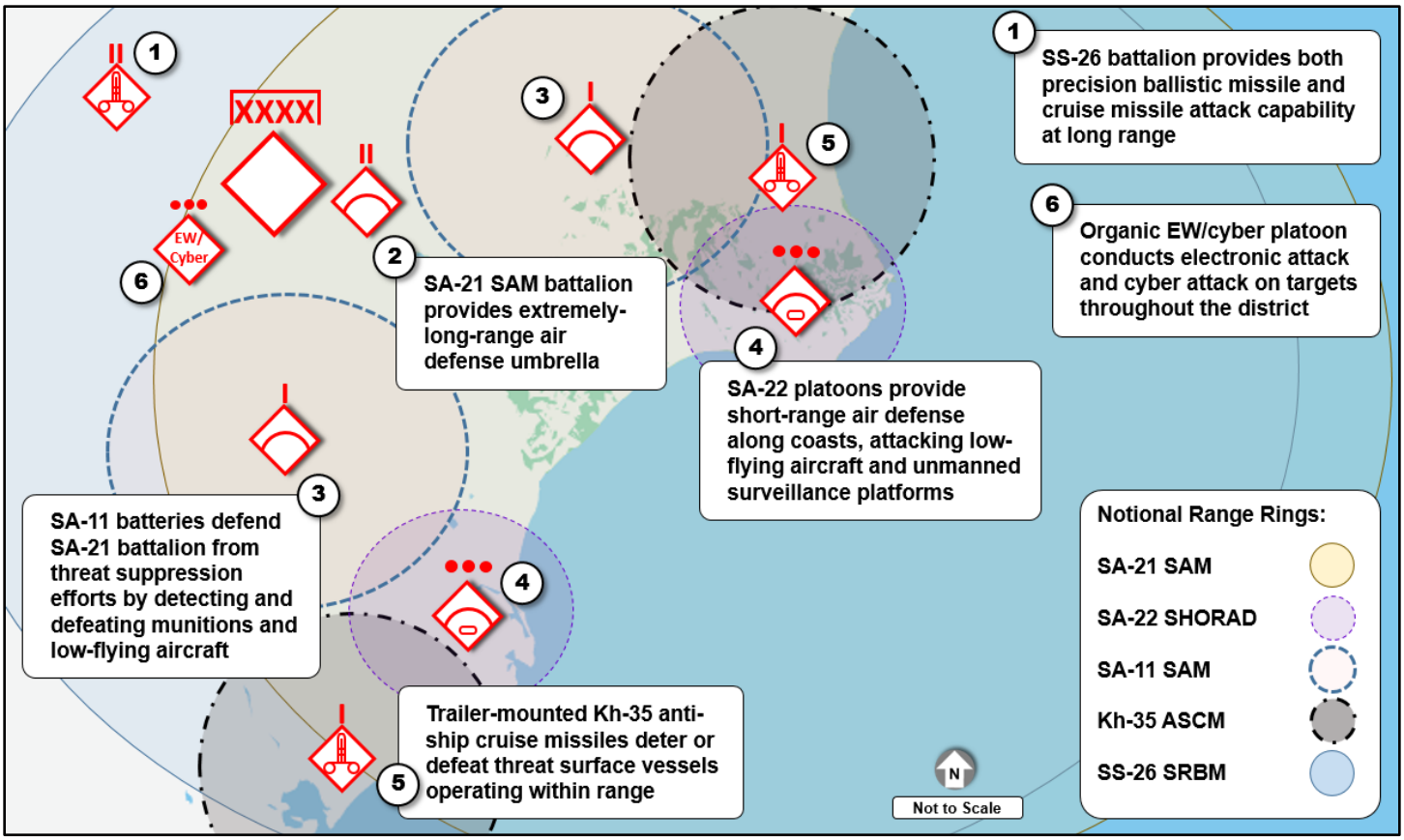


Figure 7. The Snow Dome at the theater level covers a geographic area hundreds of miles across; it consists of expensive, rare, and highly lethal weapons systems able to influence operations across an entire theater; the basic concept, however, remains the same: each component system offsets vulnerabilities of other systems

Training Implications

Creating a Snow Dome proxy in any training environment is a challenge. Several key capabilities, including MANPADS, SHORAD systems, heavy rocket artillery, and ballistic missiles, are either absent completely from US inventories or are available only in very limited quantities. Several competencies key to creating the Snow Dome have likewise atrophied in US formations: rapid, deep targeting, land-based anti-ship fires, and active/passive low-altitude air defense are some examples. Nonetheless, emulating the Snow Dome supports creation of an accurate and challenging opposing force (OPFOR). OPFOR commanders must know capabilities and limitations for all available systems and must understand how these systems can be employed using a combined arms, defense-in-depth methodology. Likewise, US and friendly forces must train in environments where friendly air and firepower superiority do not always exist: a significant change in perspective for most American commanders.

Conclusion

Though the Snow Dome is a relatively new term, the basic idea—combined arms and defense-in-depth—is as old as warfare itself. The challenges the Snow Dome presents to US forces are significant. It will impede freedom of movement throughout an operation, even at long range, and it will attrite friendly forces in a way not seen in decades. Without true joint combined arms operations, breaking down the Snow Dome will likely be impossible. This reality requires US forces to recognize their shortcomings in firepower, then to conceive creative and possibly asymmetric methods to defeat powerful threat A2AD capabilities.

Notes

[1] James Holmes. "U.S. Confronts an Anti-Access World." The Diplomat. 9 March 2012.
[2] James Holmes. "U.S. Confronts an Anti-Access World." The Diplomat. 9 March 2012.
[3] Christopher Cavas. "CNO Bans A2AD as Jargon." Defense News. 3 October 2016.

[4] John Kuehn. "The Reasons for the Success of the Sixth Coalition Against Napoleon in 1813." US Army Command and General Staff College. 6 June 1997; Daniel Goure. "Lessons From History For Countering Anti Access Area Denial Challenges." The Lexington Institute. 10 January 2012.

[5] Charles Koch Institute. "What is A2/AD and Why Does It Matter to the United States?" 21 September 2016.

[6] Alexander Korolkov. "100 years of Russian air defense: the principal milestones of the centenary." Russia Beyond. 9 March 2015

[7] Hans-Georg Richert. "Tactics and Fire Control of Russian Artillery During 1941, 1942, and 1944 and Their Development in Recent Times." All World Wars. 1952.

[8] Lester Grau. Soviet Artillery Planning in the Tactical Defense. Soviet Army Studies Office. 1990.

[9] Nikolas Gvosdev. "Just How Dangerous Is Russia's Military?" National Interest. 15 July 2015.

[10] Descriptions of all of these weapons systems can be found in previous articles in this series: Russian Tactical Air Defense Systems and Techniques (Red Diamond, June 2017), and Russian Artillery Tactics and Systems (Red Diamond, August 2017).

[11] At present, brigade/regiment-size units report directly to the operational command, the equivalent to the NATO corps. In essence, Russian Ground Forces did away with the division echelon. However, reports are emerging that this structure is problematic, and the division may reappear in the near future.

[12] Upgraded variants of the SS-26 employ both the normal ballistic missile and a long-range land-attack cruise missile (R-500/SSC-8).

———————

by Jon H. Moilanen, TRADOC G-2 ACE Threats Integration (DAC)

Area defense is a threat tactic to deny key areas or access to key terrain by an enemy. Threat actions focus on attacking key components of the enemy's combat system at selected times and locations that cause the most effective disruption, defeat, and destruction of an enemy. Area defense is designed to achieve a successful outcome by forcing an enemy's offensive operations to culminate before he can achieve his objectives, or by denying an enemy his objectives while preserving friendly forces' combat power. An area defense can also be employed when a threat is tactically overmatched in an operational environment. It is typically one aspect of a higher headquarters' mission and supports conditions for a higher headquarters to achieve mission success through tactical, operational, and strategic operations.

Ground and aerial maneuver and support forces occupy designated locations to defend in a coordinated *defensive array.* This type of array is the grouping of battle positions that subordinate commanders have orders to defend. The brigade tactical group (BTG) can plan and direct successive defensive positions at extended intervals between arrays, or concentrate defensive positions within an array. Control measures focus on a central consideration of integrated kill zones, obstacles, and simple or complex battle positions. Other control measures can include objectives, attack zones, counterattack zones, boundaries, phase lines, battle line, and support line in order to orient fires, maneuver, and support to BTG command and control.

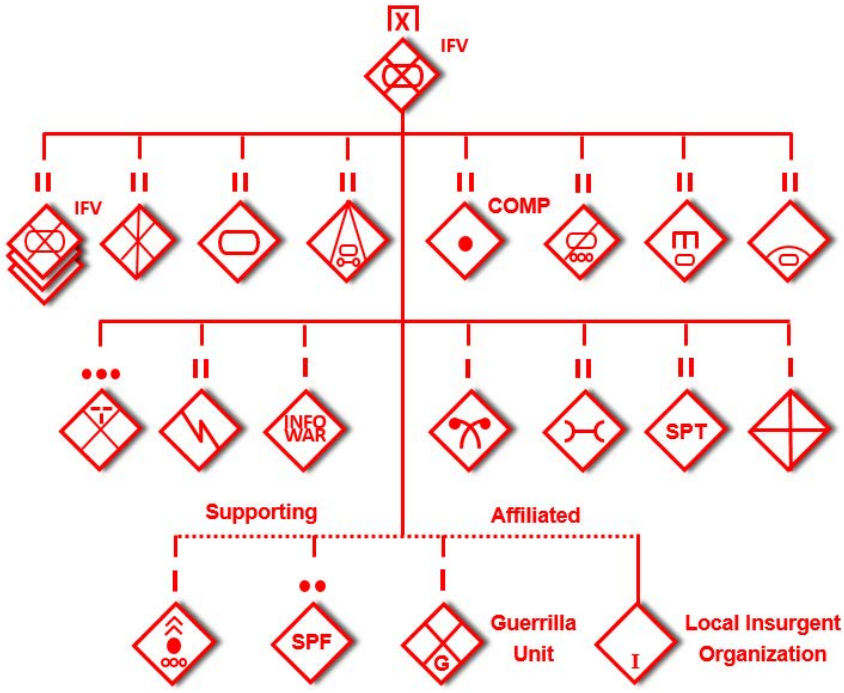


Figure 1. Threat brigade tactical group task organization (vignette example)

In this article, a threat BTG commander is assigned an area defense mission as a supporting effort to his higher headquarters' mission. The BTG area of responsibility (AOR) is a geographical area and associated airspace within which a

commander has the authority to plan and conduct combat operations. The AOR is normally described with three mission-oriented areas: a disruption, battle zone, and support zone. The AOR is bounded by a limit of responsibility (LOR) beyond which the organization may not operate or fire without coordination through the next-higher headquarters. The BTG commander also incorporates a zone of reconnaissance responsibility (ZORR) in his mission.[1] The ZORR is a combination of a unit's AOR and the area outside of that AOR that can be observed or monitored by the unit's technical sensors.[2]

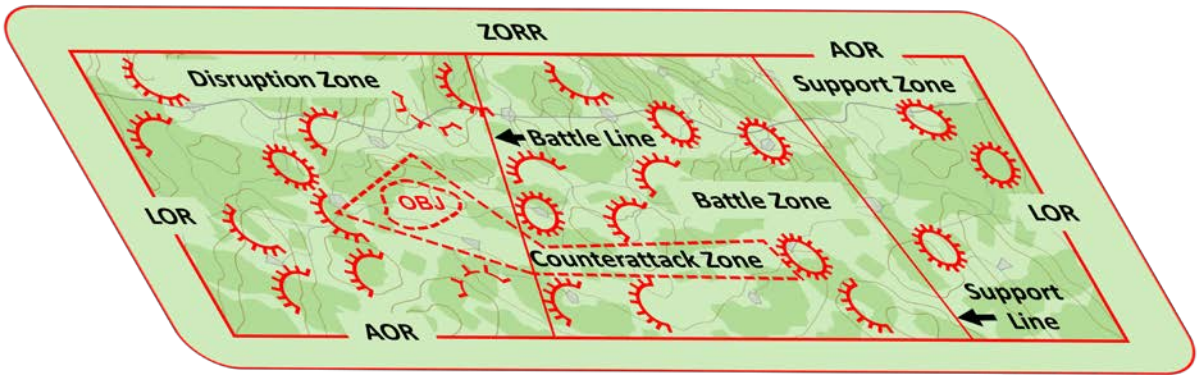


Figure 2. Terrain appreciation and control measures for an area defense (generic example)

The BTG commander prepares for tactical opportunities with intelligence reports of probable or known enemy forces approaching his defensive AOR. He is willing to accept risk, use initiative, and deviate from orders in order to achieve his assigned mission objective. His plans and orders consider contingencies that might emerge unexpectedly and options to exploit, which can include a counterattack. In a BTG area defense mission, an offensive mission area can include a *counterattack zone* assigned to a subordinate unit commander with an on-order mission purpose and intent. Attack zones are often used to control offensive action by a subordinate unit inside a larger zone or operation.[3]

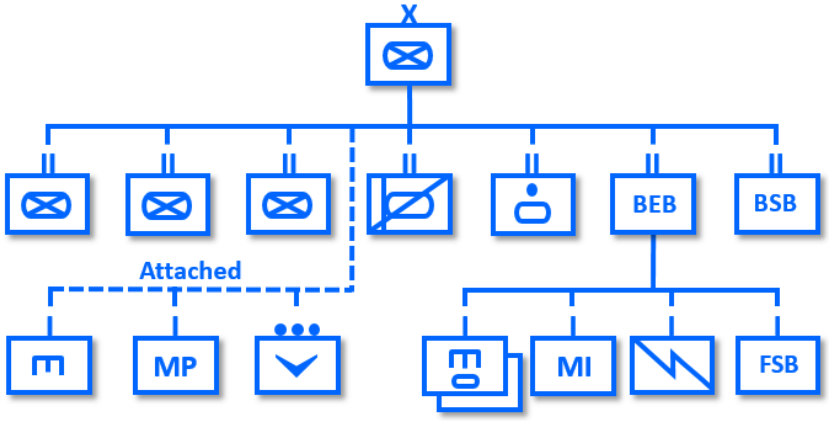


Figure 3. Enemy armored brigade combat team organization (vignette example)

The BTG maintains the initiative in threat operations and conducts tactical actions that create opportunities to transition to offensive operations. Causing unacceptable enemy casualties can be a specified task with the intent of degrading enemy resolve or ability to continue his attack. Information warfare (INFOWAR) is critical to the execution of an area defense. The capabilities of INFOWAR elements, applied in various combinations, create threat tactical advantages not typically available in a numerical force-on-force confrontation. Elements such as deception, electronic warfare (EW), computer warfare, and information attack can manipulate or disrupt enemy data and accurate understanding of an operational environment by an enemy commander. In addition, perception management is a key combat multiplier to executing an area defense.

Area Defense

Area defense retains terrain or denies enemy access to specified areas. Defenses can also be directed to protect friendly forces and/or areas and infrastructure. The threat is willing to accept significant casualties if this commitment supports a main effort in other areas of a higher headquarters AOR. The delay, commitment, and decisive engagement of enemy forces created by an area defense often facilitates the action of threat maneuver forces in a larger offensive operation.

Tactical disruption of enemy forces occurs deep in the enemy rear or consolidation zones with support of threat operational reconnaissance, intelligence, surveillance, and target acquisition (RISTA) and fires available from higher headquarters.[4] Threat forces in an area defense and in the disruption zone identify and attack an enemy's command and control, combat support, and combat service support systems at designated times to destroy critical components and subsystems. Effective enabling offensive and defensive actions in the disruption zone disaggregate enemy forces and cause them to attack into the battle zone at a significant disadvantage. Threat forces in an area defense intend to slow the momentum or disrupt the tempo of an enemy attack, canalize enemy forces into kill zones, and defeat or destroy the enemy with fires and maneuver.

Battle Positions

The decisive action in an area defense typically occurs with main defense forces in the battle zone. The fundamental structure for a defense is the *battle position* (BP)—also called a *simple battle position* (SBP)—as a defensive location oriented on a likely enemy avenue of approach. Area defense forces occupy and fortify a *complex battle position* (CBP) network throughout the disruption zone, battle zone, and support zone. Each CBP is comprised of multiple integrated SBPs. The location and construction of a BP is positioned to best accomplish the mission tasks assigned to the threat forces occupying the particular defensive position.[5]

The threat employs two types of complex battle position. A CBP can be a defensive location oriented on a likely enemy avenue of approach. Threat forces employ as much engineer effort and/or camouflage, concealment, cover, and deception (C3D) measures as time allows in preparing a defensive position. Improving defensive positions never ceases.[6] The other type of CBP may appear very similar in form, but has a distinctly different purpose. A CBP can be a defensive location designed to employ a combination of complex terrain, C3D, and engineer effort to protect threat forces and capabilities within the CBP from detection and attack.[7]

The location of a CBP site is not always oriented on an enemy avenue of approach. The exact opposite orientation may be directed to preclude identification while being able to observe or recognize an enemy approach to a location. This CBP purpose for protection is a form of sanctuary for forces, equipment, and/or materiel, and is typically not located along or in a probable enemy avenue of approach.

This is quite different from the concept of a CBP used as a strongpoint to anchor a defensive area or deny key terrain to an enemy. The threat uses the defensive nature of CBPs to preserve combat power until conditions permit threat offensive action. Defenses of a SBP or CBP are integrated for 360-degree weapon systems coverage, and can include integrated defenses for air defense and fires. In both SBP and CBP defensive concepts, an approaching enemy will be exposed to coordinated fires to cause substantial losses in systems and personnel.[8] The threat often uses cultural shielding in populated areas to prevent an enemy from employing precision standoff attack means against a CBP. While C3D is always important, deception efforts to hide a CBP may limit how engineer countermobility, survivability, and other supporting actions are employed that could reveal this type of CBP location.

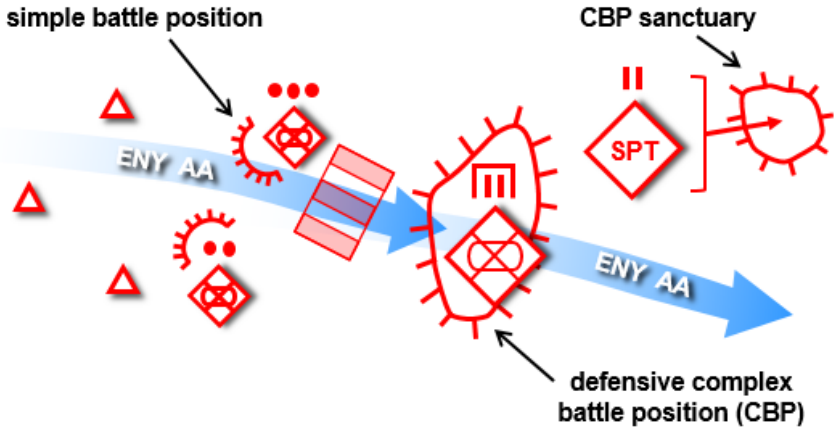


Figure 4. Complex battle position purposes to primarily defend or provide sanctuary

An area defense reinforces or creates complex terrain and can accommodate decentralized logistics in support of threat forces that may be bypassed by attacking enemy forces and/or are intentionally planned to fight in the defense as isolated

forces. Logistics caches are prepositioned in designated CBPs and sites throughout the AOR. This rationale of a CBP as sanctuary can also be used as a site from which to launch local offensive actions, which can include ambushes, assaults, and raids in an area defense. These types of defensive and offensive enabling actions force the enemy into continuous operations and degrade enemy combat power while the threat is able to sustain the initiative in its defensive mission. Within an overall area defense, the BTG commander might also direct some forces to conduct maneuver defense tactics.

Figure 5. Antitank ambush battle position being prepared in the battle zone

The BTG can also conduct a counterattack to cause enemy offensive actions to culminate and enhance threat ability to regain or sustain the initiative. A counterattack is a form of attack by part or all of a defending threat force against an enemy attacking force, with the general objective of denying the enemy his objective. The counterattack shifts actions from a defensive posture and transitions to an offensive action. A fixing force in a counterattack engages that part of the enemy to prevent designated enemy forces from moving from a location for a specified period of time. Threat forces also destroy enemy reconnaissance or counterreconnaissance forces and other enemy forces that may have penetrated the threat area defense. An assault force in a counterattack can be assigned actions to force the enemy to commit his reserve. With the enemy force reserve committed to combat, the enemy commander has marginal remaining tactical agility, which enhances the threat ability to defeat or destroy the enemy attack.[9]

The threat can use an area defense to create opportunities to execute a spoiling attack—in conjunction with actions of a higher headquarters—during early phases of a defensive mission. A spoiling attack can preempt or seriously degrade an enemy offensive operation during its initial preparations, movements, and maneuver, and disrupt the timing and integration of enemy combat power.[10]

The threat commander retains a reserve force. A true reserve force is not a committed force until the BTG commander assigns it a mission task for execution. The reserve provides flexibility for the threat commander to preempt or respond to emergent expected or unexpected conditions in the area defense. A designated counterattack force is a committed force with a mission, and is not a reserve force.

Functional Organization for an Area Defense

An area defense employs multiple types of functional forces. The BTG commander assigns subordinate units and affiliated organizations with functional designations that correspond to their assigned roles and tasks. The two general types of functional forces are enabling forces and action forces.

Enabling Forces

Enabling forces are structured or task-organized to create the conditions that allow the action force the ability to operate and accomplish the primary mission task. Enabling actions can be sequential, parallel, and/or simultaneous in execution, and continue throughout the entire mission timeframe. Enablers that perform fixing and/or isolation actions may be required to set the conditions for defensive forces to transition to a counterattack in order to destroy a designated enemy force. In order to create conditions for a defensive action force to succeed, an enabling force may be required to operate at a high degree of risk and may sustain substantial casualties to accomplish its mission task. However, an enabling force may not even make contact with the enemy, but instead conduct actions such as a demonstration to distract or disrupt. Functional titles for enabling forces in an area defense can include:

- Disruption force;
- Security force;
- Deception force;

- Fixing force;
- Assault force;
- Support force; and/or
- Reserve force.

Disruption Force. In an area defense, enabling forces operating in the disruption zone are described as a disruption force. Forces may have a designation change as the defensive mission progresses through a disruption zone and into the battle zone. A disruption force can have subordinate forces with specified titles such as deception, security, fixing, or assault force. Enabling actions include, but are not limited to, tasks of deception and security assigned to designated forces.

Support Force. A support force provides combat support and combat service support to the area defense, C2 functions for BTG actions, and any other enabling functions required to sustain and maintain the defensive mission.

Figure 6. Multiple rocket launcher reloading rockets for a subsequent fire mission

Reserve Force. The BTG commander in an area defense designates one or more reserve forces of varying size and capabilities. The reserve typically occupies an assembly area and defensive posture, but is prepared to move and maneuver immediately upon alert by the BTG commander. The reserve is not a committed force until the threat commander assigns it a mission task. However, a reserve force commander may be provided with several contingency tasks by the BTG commander for planning and possible execution. One of these mission tasks can be to counterattack.

The threat identifies two types of forces with "reserve" in their title that are forces committed to a mission task and cannot be considered an uncommitted reserve. The BTG can designate an antitank reserve (ATR) to counter armored threats; this force is typically an antitank unit and often operates in conjunction with an engineer obstacle detachment.[11] Another force the BTG commander can designate is an antilanding reserve (ALR) to counter actions if the area defenses are vertically enveloped by enemy airborne or heliborne attack.[12]

Action Force

Main Defense Force. The most common type of action force in an area defense is the *main defense force*. The SBPs and CBPs in the main defense area must be able to defeat, through its capabilities or positioning relative to the enemy, the attacking enemy formations. The main defense force executes the primary functions of defense that accomplish the threat mission.[13] The BTG commander can assign a particular action force with a more specific designation to clearly identify the function it is to perform; two examples of this are fixing forces and blocking forces.

Counterattack Force. When the BTG commander decides that a counterattack is necessary to success of the area defense, he commits a force to counterattack that then becomes the action force of the BTG. It can be the BTG reserve, another force already designated for the counterattack task, or a newly task-organized force within the BTG. Once the force is committed to the counterattack, other main defense forces enable the success of the counterattack, as do all disruption forces and support forces.

Disruption Force in an Area Defense

In an area defense, the disruption zone is the area surrounding the battle zone(s) where the threat plans to disrupt enemy attack formations and momentum. Disruption forces include RISTA assets and counterreconnaissance forces tasked to destroy enemy reconnaissance and security forces. The BTG often operates with affiliated forces such as insurgent organizations and cells, guerrilla units, and/or criminal organizations. These types of paramilitary forces can assist

disruption forces by providing reconnaissance and surveillance, performing force protection, controlling the civilian population, and conducting specified deception operations and small-unit offensive tactics. The BTG directs continuous defensive actions in the disruption zone that support the area defense, and coordinates for the integrated fires and air defenses of the disruption zone with the integrated fires of higher headquarters.

Reconnaissance-Fire Complex

A *reconnaissance-fire complex* can be described as an integrated system of RISTA; fires command, control, and communications; and designated weapon systems into a closed-loop, automated fire support system that detects, identifies, and destroys critical targets in real-time execution. The integrated fires command (IFC) of the threat exists at division or higher headquarters, from which the BTG receives integrated fires support.[14] Reconnaissance fire is designed primarily to attack and destroy key enemy capabilities and set conditions for operational missions and support to the operational/tactical battle.

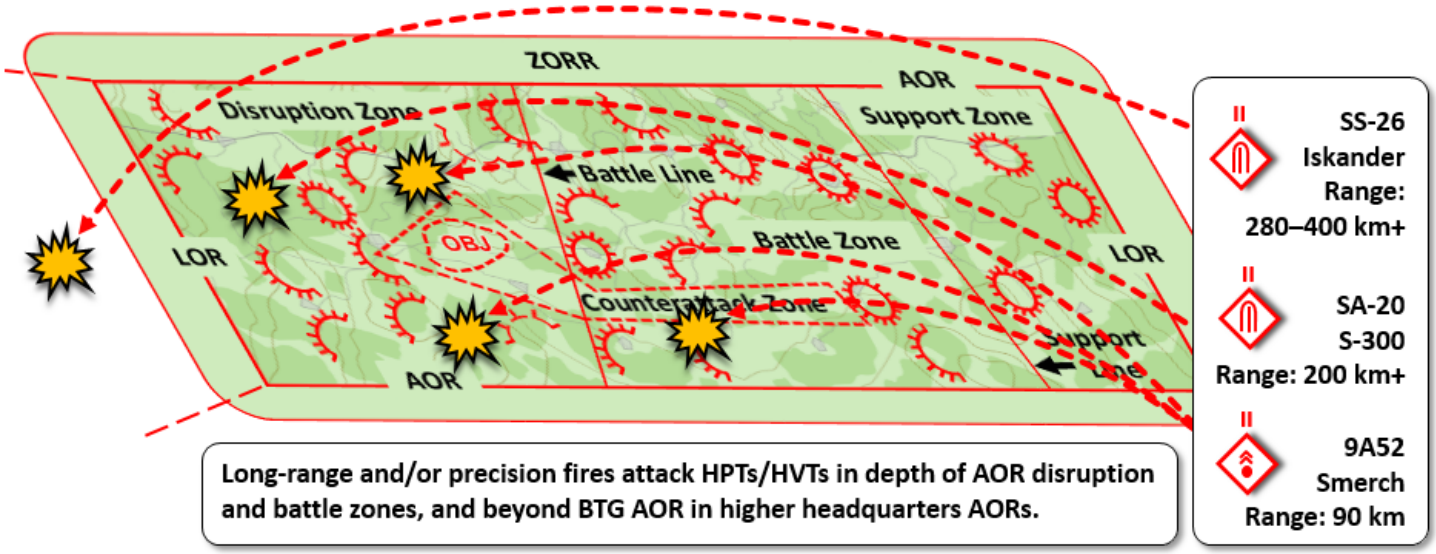


Figure 7. Integrated fires command possible support to BTG AOR (example)

Reconnaissance fire enables the threat to deliver the most effective fires—typically with tube artillery and multiple rocket launcher artillery, but they can include rotary-wing air, surface-to-surface missiles, cruise missiles, and area or precision artillery fires within a very short time after target acquisition.[15] These types of fires, designated to complement reconnaissance fires already in the BTG task organization, can be mission-tasked by the commander of the IFC with IFC control for centralized planning, analysis, and evaluation of RISTA data and execution support of the reconnaissance fires.[16]

The IFC commander selects and establishes the target priority and target damage criteria for high-payoff targets (HPTs) and the combat system components to be attacked. The HPTs are those high-value targets whose acquisition and disablement/destruction are critical to the success of the threat mission. A high-value target (HVT) is a target that an enemy commander requires for the successful completion of his mission, and whose loss would be expected to seriously degrade important enemy functions throughout the threat AOR and ZORR.[17]

The IFC staff and fire support component commanders develop a fire support plan designed to conduct the reconnaissance complex fires necessary to create the desired favorable conditions that support threat operations. This type of C2 allows assets to execute other missions until higher-priority targets are detected and confirmed. Additional long-range and precision threat fires that may typically be employed against operational or strategic targets can be directed on targets within or near the BTG AOR.

Battle Position Defenses

The disruption force occupies and defends from battle positions throughout the disruption zone. The size and capability of battle positions span small unit/cell locations to report or harass enemy progress within the disruption zone, combat security outposts up to platoon/company size, or company/battalion complex battle positions to defend and/or delay. While some threat forces retain terrain, other disruption forces may be directed to conduct maneuver defenses through

successive battle positions that defend and delay enemy forces in order to shape the axes direction allowed to the enemy. In these types of defensive tactics, the distance between battle positions has the intention of causing the enemy to displace the majority of his systems and fires in order to continue the attack.

Figure 8. Combat security outpost in the battle zone

Other disruption forces may be directed to break contact after conducting assaults, ambushes, and/or raids, and reorient to subsequent battle positions for defense or reorganization and resupply. Some disruption forces could be designated as stay-behind forces with orders not to engage initial echelons of the enemy attack. The disruption forces can conduct significant countermobility and obstacle efforts that support the area defense ability for fires and maneuver. Engineer support in the disruption zone also provides mobility support to selected disruption forces intended for maneuver options, such as support to a spoiling attack by the higher headquarters or a BTG-directed counterattack in its AOR.

The mission tasks typical of a disruption force include but are not limited to:

- Destroy enemy reconnaissance forces;
- Detect enemy axes of attack;
- Identify enemy command and control nodes and locations;
- Deceive enemy as to the location and configuration of main defense force battle positions;
- Delay enemy momentum with continuous assaults, ambushes, and raids;
- Conduct information warfare actions to include electronic warfare;
- Cause enemy to prematurely deploy his lead maneuver echelons and supporting fires;
- Identify enemy main effort;
- Fix designated enemy forces;
- Isolate designated enemy forces;
- Identify enemy critical logistics groupings and locations;
- Attack high-payoff targets;
- Canalize enemy into designated threat kill zones;
- Conduct battle handover to battle zone forces as enemy forces cross the battle line; and
- Conduct defensive/offensive mission tasks in the disruption zone to support decisive actions in the battle zone.

Some disruption forces may be directed to defend and accept decisive engagement as an integral component of the BTG main defenses in the battle zone. Actions in the disruption zone disrupt the momentum of an enemy attack. This disaggregating of enemy formations can reduce the speed, alter the tempo, or otherwise change the pace of attack, and can even halt the enemy advance. Typical targets for attack in the disruption zone include:

- C2 systems;
- RISTA assets;
- Precision fire systems;
- Aviation assets in the air and on the ground;
- Logistics support areas and lines of communications;
- Mobility and countermobility assets; and
- Casualty evacuation routes and means.

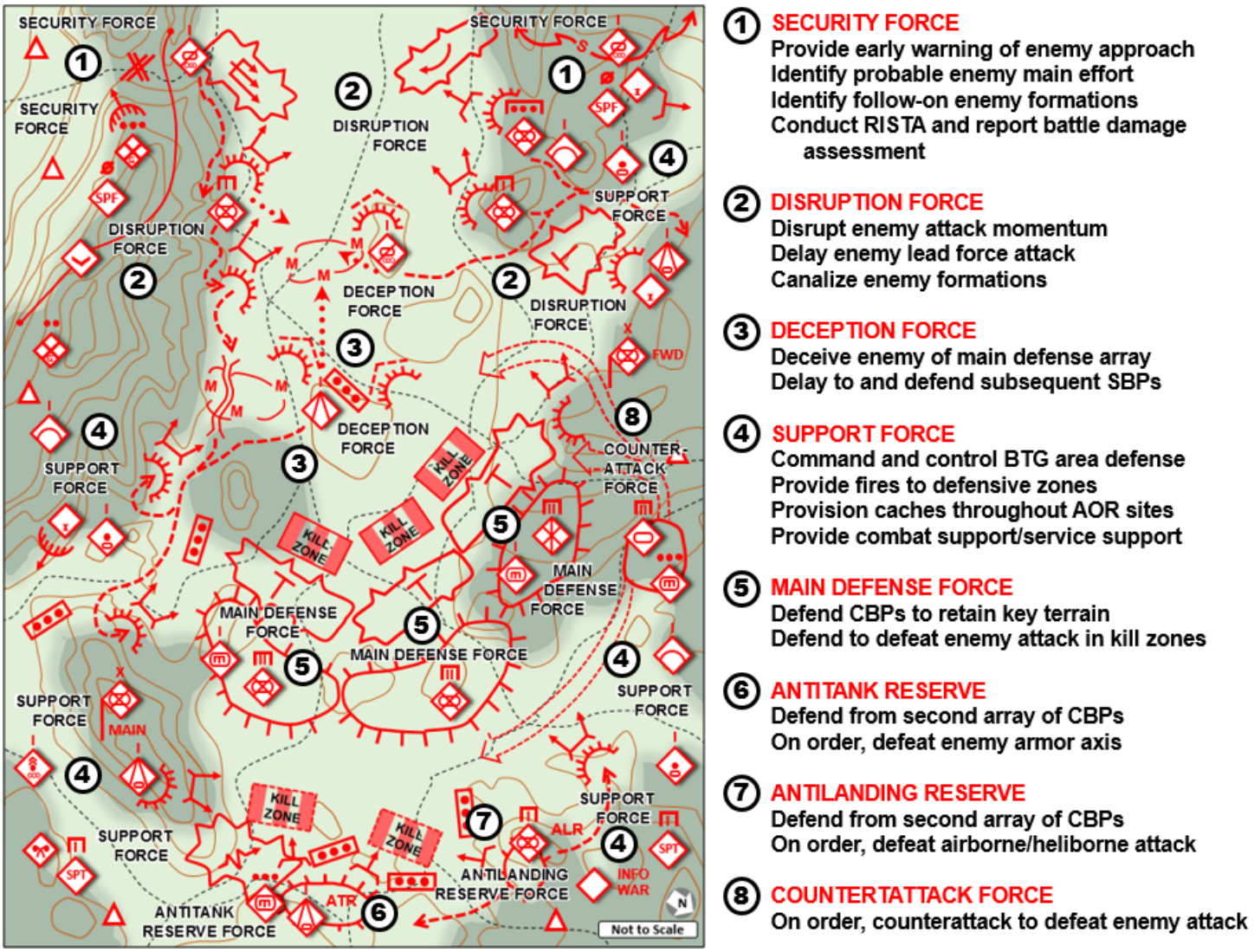


Figure 9. Initial area defensive array and intent

Main Defense Force in an Area Defense

The main defense forces continue defensive operations in the battle zone in a network of coordinated complex battle positions. These CBPs use terrain, fortification of survivability positions, and extensive obstacles to defend and defeat enemy offensive actions. As enemy forces enter the battle zone already degraded by disruption force actions, effective C3D measures obscure enemy understanding of the threat's actual main defensive positions. Decoy BPs in CBP networks deceive the enemy commander on where and when to mass his combat power.

Figure 10. Main battle tank in hull defilade overwatch position

The all-around defensive coverage of CBPs provides a threat force with the ability to rapidly shift orientation of fires and defenses if or when unexpected attacks or temporary penetrations of a defensive perimeter occur. The coordinated

positioning of multiple SBPs and/or CBPs interlock fields of fire and indirect fire concentrations in conjunction with countermobility and major obstacle efforts that support the area defense.

Actions in the battle zone can appear very similar to ongoing actions in the disruption zone. Threat main defenses can have specified units retain terrain while other units use maneuver defense within a battle zone to guide enemy forces into kill zones, where threat fires and obstacles cause significant damage to enemy combat power. Designated threat forces fix the enemy in kill zones while these and other forces attack by direct and indirect fires or support by fire. Other forces may be directed to maneuver on fixed enemy forces until the threat defeats them. The BTG employs *close support fires* to defeat enemy forces approaching and in kill zones, and uses *counterfire* to neutralize or destroy enemy indirect fires attempting to support enemy attacks and assaults into the threat defensive array. If necessary, *final protective indirect fires* complement CBP direct fires and demolitions to defeat enemy forces forward of the CBP perimeter.

Figure 11. Multiple rocket launcher battery engaging a high-payoff target

Designated forces in defensive positions—such as antitank forces or a BTG reserve—coordinate mobility avenues or routes in order to rapidly reposition mobile direct fire systems to block a penetration or reinforce an area of the defense. Integrated air defense and fires throughout the AOR prevent enemy aircraft and fires from effectively supporting the enemy attack into and in the battle zone. The main defense force benefits from reconnaissance fires and interdiction fires occurring in the depth of enemy attack formations, while the BTG concentrates on close support fires and counterfire near enemy maneuver forces, and prepares for final protective fires of CBP networked defenses.

Tactical Vignette Overview

In this tactical vignette, the BTG commander conducts an area defense to defeat an attack in his AOR by a US Army armored brigade combat team (ABCT). An analysis of the terrain indicates the main east-west corridor in his AOR as the only feasible enemy ground maneuver option to access the open plains to the east. The ridgelines on each side of the corridor severely limit lateral mounted movement to gaps with heavily wooded slopes and winding trails. Another corridor feeds into the main corridor from the northwest. As a supporting effort to his higher headquarters main effort, the BTG commander selects a main defense of key terrain that denies access to the eastern plain.

Disruption Zone

The BTG commander uses the time available to extend his reconnaissance, surveillance, intelligence collection, and target acquisition to the full depth of his ZORR, and to coordinate his tactical actions with higher headquarters RISTA, which is already disrupting the enemy with integrated long-range and precision fires on high-payoff targets.

As lead enemy forces enter the disruption zone, regular forces initiate recurring limited ambushes and assaults to break apart the momentum of the attack formations. Guerrillas block the gaps through the southern ridges and prepare ambushes for any approaching enemy forces. Insurgents emplace multiple obstacles in the northwestern corridor and coordinate for fires with their supporting special-purpose forces (SPF) team and planned reinforcement by BTG regular forces.

BTG reconnaissance forces identify enemy axes of attack with ground and aerial maneuver assets, engage lead enemy forces with antitank guided missile fires, and report damage assessment of observed indirect fires. One security force delays along the southern slope and supports other security forces in deception positions. This center security force coordinates with disruption forces to delay along the northern slope. A third security force orients in the northwestern

corridor to provide early warning of any enemy approach and prepares to defend in conjunction with the local insurgent organization.

Two mechanized company detachments (CDETs) with indirect close fire support defend a group of simple battle positons in the main corridor and are prepared to delay, on order, to successive battle positions. Guerrillas and SPF in stay-behind observation posts focus on probable areas that enemy close support artillery may occupy. The BTG disruption forces degrade critical C2 systems in the ABCT attack formation with EW and fires, reduce combat power tempo of lead attacking forces, and disrupt immediate resupply of enemy fuel and ammunition. Enemy artillery forces are firing at reduced rates and must constantly reposition to fire and survive. The disruption zone CDETs and BGT security forces are not to become decisively engaged.

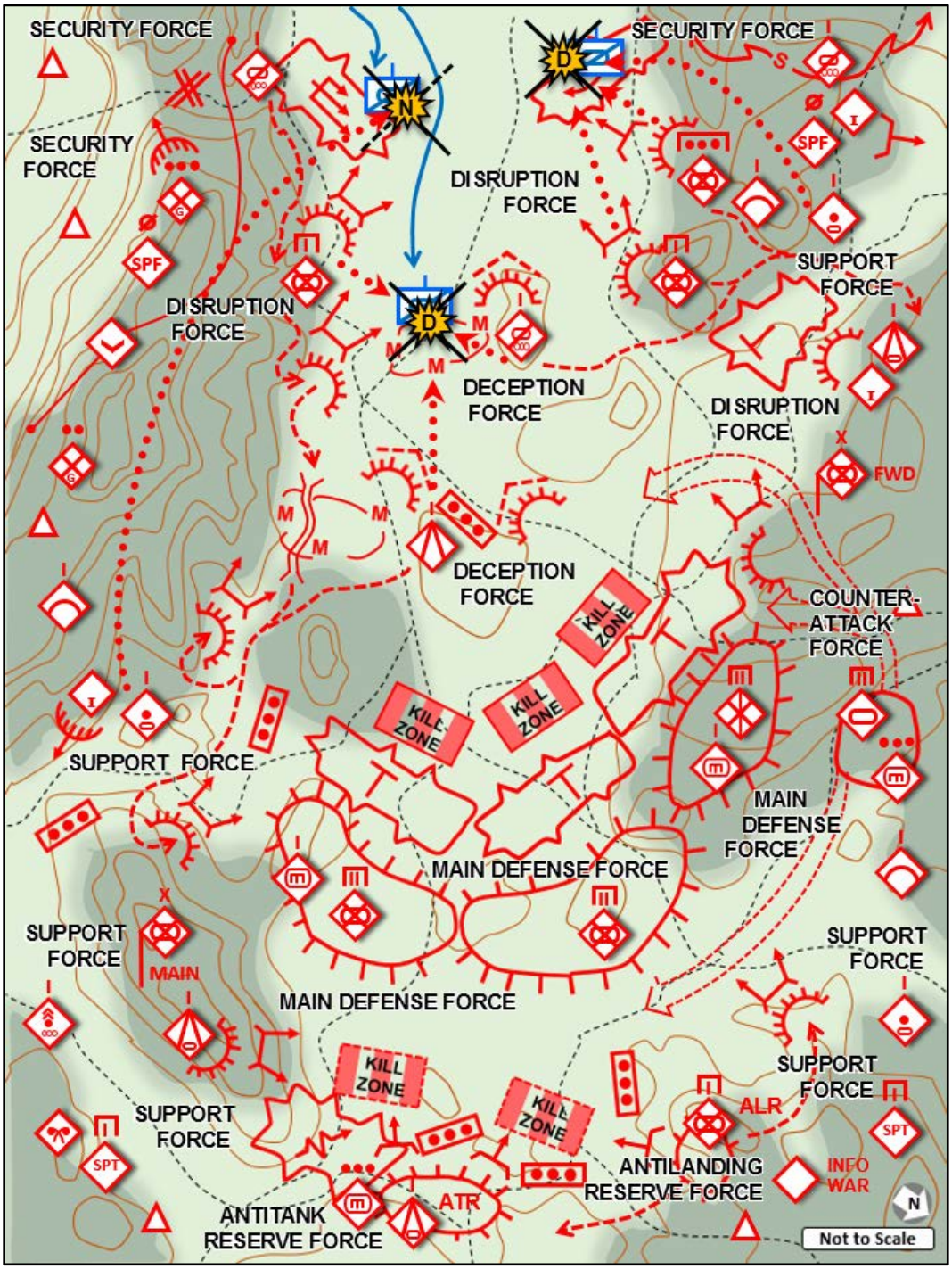


Figure 12. Security forces and disruption force actions in BTG area of responsibility (1 of 3)

The BTG commander uses his detailed understanding of the terrain and recommendations of local insurgents to best establish his main defensive array. Indiscernible from maps or photography, two intervisibility lines in the main corridor allow disruption and battle zone forces to physically mask SBPs and CBPs from attacking enemy forces. The combined INFOWAR capabilities, such as cyber attack, EW, and C3D, degrade any effective understanding by the enemy commander of the BTG main defenses. Although INFOWAR promotes the possibility of military-grade chemical warfare in regional and global media releases, military-munition chemical attacks are not used in this battle.

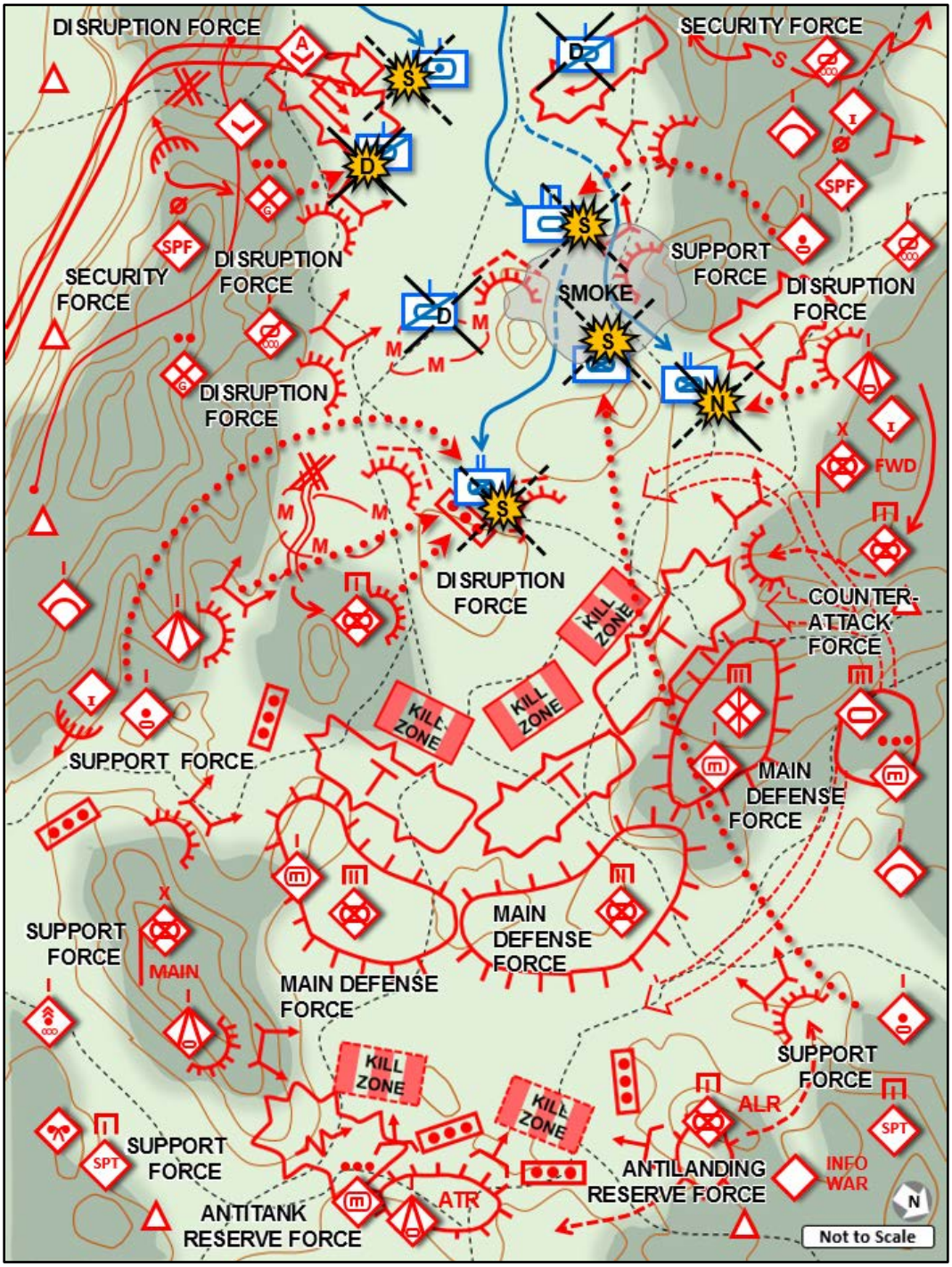


Figure 13. Area defense actions in BTG area of responsibility (2 of 3)

The disruption force uses the western intervisibility line and direct and close support indirect fires, obstacles, smoke, and decoy battle positions to deceive the lead enemy forces as to the location of the actual main defensive array in the battle zone. The BTG commander orders the two CDETs to initially defend from prepared battle positions situated among a group of decoy positions forward of the battle zone.

Support Zone

Engineer forces place major effort on countermobility support to the defenses in primarily the main defenses and augmented disruption activities in the disruption zone. Mobility capabilities are allocated to the counterattack force to ensure the ability to move and maneuver rapidly on any of three possible counterattack routes. Numerous stationary defenses have logistics caches that are protected in underground reinforced positions. Other caches located throughout the AOR provided flexibility for forces if enemy actions cause shifts in defensive orientation or forces become isolated. Sustainment actions such as medical treatment, maintenance, and other service support are in dispersed CBPs in the support zone.

Redundant secure and integrated communications add to BTG agility in quickly distributing intelligence updates and mission orders. Commanders and key leaders position themselves in the AOR to ensure an accurate sense of decisions and actions during critical points of the battle. BTG C2 locations include a mobile forward command post with functional support from a main command post and connectivity to an integrated fires command. The BTG commander, along with several key subordinates, operates from a command observation post during the battle in order to maintain a keen understanding of the tactical situation and when to issue orders that shape and support the successful conduct of his tactical group mission.

Battle Zone

The ABCT commander is unsure if his lead forces are still fighting BTG security forces in a delay, or if he has reached the BTG main defenses. As he continues the attack, substantial countermobility actions and fires slow lead forces as they attempt to breach obstacles and mined areas, which causes follow-on ABCT forces to bunch up behind the lead forces. The cumulative effect creates lucrative targets for BTG indirect concentration and interdiction fires. These fires allow the CDET in the south to pass through an open lane in the mined area, close the lane, and occupy SBPs in the disruption zone. The CDET in the north repositions to different SBPs to continue flanking direct fires and provide a capability to respond to any approach of enemy forces from the northwestern corridor. Both CDETs have mobile obstacle detachments attached to assist in defensive actions.

Breaching operations eventually create lanes through some of the obstacles and mined areas, but ABCT forces receive flanking direct fires from antitank forces along the southern and northern slopes in prepared BPs. The successful actions in the disruption zone disaggregate the massing of ABCT combat power.

The BGT commander employs most of his combat power in the first defensive array of his battle zone. Combat security outposts near the northern intervisibility line support the three battalion detachments (BDETs) in CBPs focused into a central kill zone area with interlocking sectors of responsibility for each BDET. Significant countermobility actions canalize the ABCT forces toward the east and into the primary kill zones of the battle zone. Antitank forces positioned in the south and north initiate long-range flanking fires.

As the lead ABCT forces appear over the intervisibility line, the BTG executes concentration fires on targets behind the attacking formations by artillery and multiple rocket launchers. The coordinated direct fires of the BDET CBPs blunt and fix the lead attacking forces in the kill zone, but have not defeated the ABCT attack. Some ABCT forces are attempting to maneuver out of the kill zones and assault into the defensive positions. Simultaneously, follow-on ABCT forces have cleared through the lanes breached in the obstacles and are headed toward the BGT main defenses. EW and related INFOWAR capabilities block or disrupt enemy C2 and fires at this critical time.

Tactical RISTA forces keep the BTG commander informed on maneuver of follow-on ABCT forces. He orders the BTG counterattack force to execute the western axis contingency to defeat the intermixed mechanized and armor forces. Previous key-leader reconnaissance and rehearsals prove invaluable, as counterattack routes have been cleared and prepared and coordination confirmed between liaison officers in the CBPs. The counterattack complements the main defense effects with an assault into the ABCT flank and rear by the tank-heavy BDET.

The BTG commander and his fires coordinator lift and shift fires to support the counterattack, as well as continuing fires on ABCT forces in the kill zones. Disruption forces report no follow-on force formations approaching east down the main corridor. The BTG area defense is successful in defeating an ABCT in the battle zone.

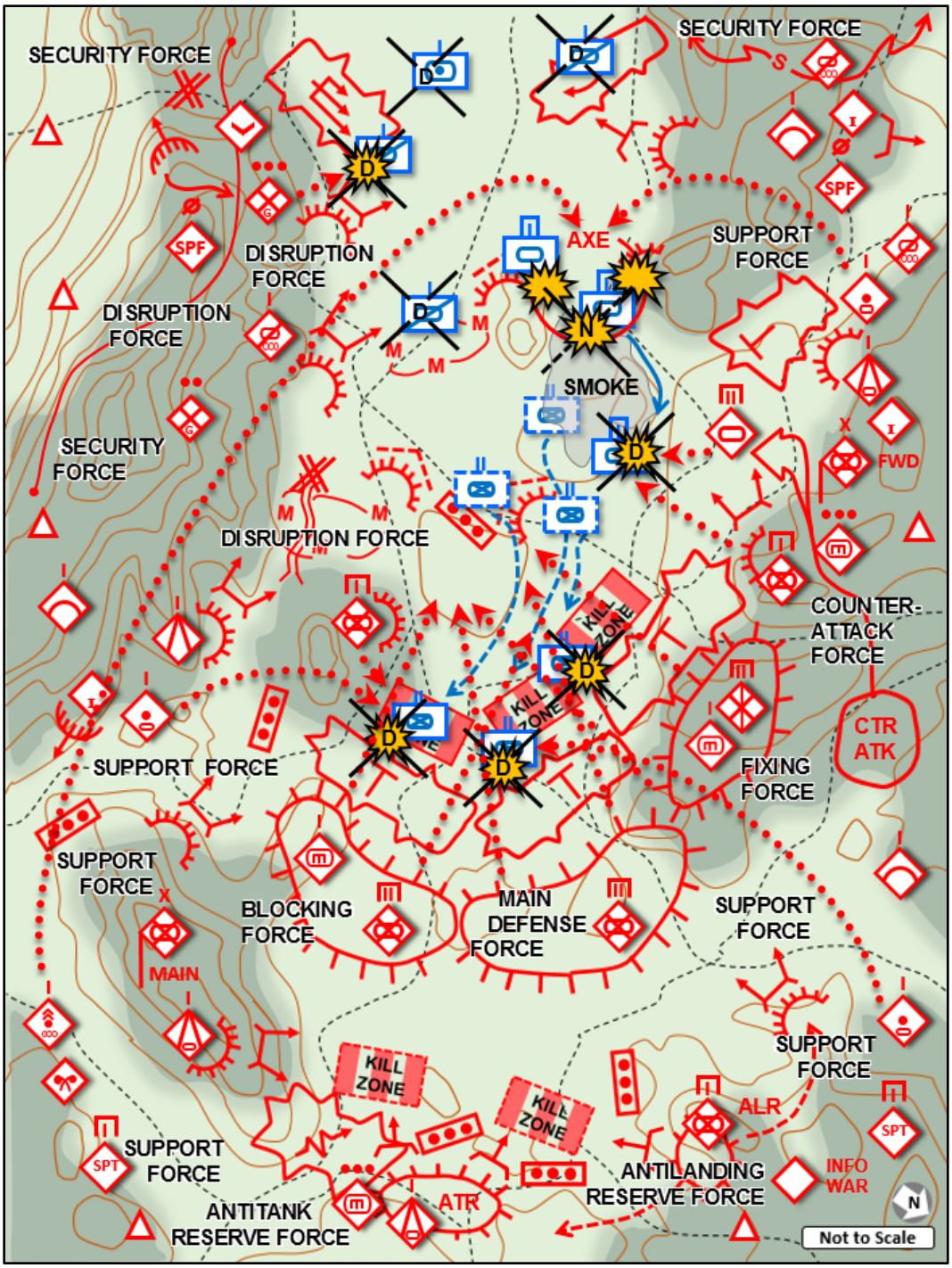


Figure 14. Counterattack force actions in BTG battle zone (3 of 3)

As the BTG commander reflects on this mission success, he realizes he decided to accept risk in having a weakened secondary defensive array in order to bolster his primary array with its combat power oriented laterally and into a central kill zone area. The antilanding reserve—a mechanized CDET—was one of only two forces in his secondary defensive CBPs. However, his antitank reserve company was ready to react against southern and central enemy axes. Knowing the counterattack force was a committed mission force, he had alerted the counterattack force commander of several contingencies that could occur within the battle zone.

The BTG commander conducts reorganization to improve the combat effectiveness of his tactical group forces. The BTG commander provides priorities of effort for improving defensive arrays, and states a warning order of possible offensive operations in the near future.

Summary and Training Implications

This tactical vignette describes key actions of a successful BTG area defense. The BTG commander obtained early disruption of enemy forces approaching his AOR based on integrated RISTA and fires command coordination at higher headquarters, and eyes-on confirmation of high-payoff targets by long-range reconnaissance forces and SPF operating deep in the enemy rear and consolidation areas.

Affiliated irregular forces and SPF added to disruption zone direct actions with small unit/team assaults, ambushes, and raids on critical command and control nodes and sustainment systems. Unmanned aerial vehicles and attack aviation forces supported RISTA and fires coordination of the BTG forces. The BTG and higher headquarters coordinated for EW and other INFOWAR capabilities to support deception, target acquisition and tracking, and electronic attack. Other actions unseen by BTG maneuver forces but critical to successful deception efforts included satellite-link jamming and disruption, and spoofing of enemy unmanned aircraft systems and global positioning systems by higher headquarters forces.

The BTG disruption force degraded the enemy attack, identified the enemy main effort, and conducted battle handover to main defense forces as the ABCT entered the battle zone. Engineers were task-organized to support maneuver forces in the disruption zone and battle zone for countermobility and mobility measures. Engineer effort was also apportioned and allocated to forces in the support zone for C3D and survivability of logistics nodes.

Disruption forces identified and tracked critical enemy systems in lead enemy formations, and reported movement and maneuver progress that cued when to attack selected high-payoff targets for best effects. These continuous actions disrupted the enemy's combat systems, with particular attention against enemy command and control. Targeting enemy combat support and combat service support was similarly critical to degrading enemy capabilities. Without the sustainment and support of these systems, enemy forces in direct contact with the BTG attack quickly became vulnerable to destruction or defeat.

The BTG commander ordered some disruption forces to defend or provide security actions, while others were ordered to reposition to support the BTG main defenses and shape the AOR for decisive actions in the battle zone. The BTG masked the actual main defenses of the battle zone with decoy battle positions and countermobility actions, such as smoke and other obscurants. Although the threat had release authority for use of chemical weapons, this capability was not employed in this defense. However, effective INFOWAR convinced the enemy commander to operate in an increased mission-oriented protective posture that decreased the level of agility and stamina in his personnel.

The enemy commander was deceived and prematurely committed his lead formations. The unmasked locations of supporting fires accompanying the attacking forces were degraded with threat counterfires. Timing of fire-mission execution was critical to effectively massing threat combat power, as was threat expert knowledge of the terrain, coordination with the relevant civilian population, and tactical experience of regular and irregular forces operating in close coordination. The BGT commander identified the correct moment to exploit the stalled enemy attack with a counterattack into the enemy rear echelon, which led to ultimate destruction of enemy force combat effectiveness.

The BTG commander accomplished his mission. The BTG used combined arms task organization and support from higher headquarters to optimize the combat systems of its mechanized infantry, tank, antitank maneuver, and fires forces. Logistics prepositioned multiple caches to support actions in the disruption, battle, and support zones. These sites anticipated defenses that may have to remain in a defensive position or resupply once repositioning to a successive position. Tactical actions of fires and air defense in depth, as augmented from higher headquarters, provided an integrated approach to massed fires and effective maneuver of ground and aerial forces in the BTG AOR.

Understanding the complex tactical environments and challenges of a prepared area defense requires deliberate and detailed analysis. Rehearsals and cogent critiques improve effective actions to apply adaptive techniques in order to achieve mission tasks in the attack. Realistic and robust conditions in Army learning events—which could or will be used against capabilities and potential vulnerabilities of US armed forces and supporting organizations in contemporary operational missions—must be the norm in training, professional education, and leader development venues in order to achieve and sustain readiness in Army operations. Plans and orders issued prior to mission execution will require adjustments and adaptation during the emergent conditions and actions of an actual tactical operation. The US Army commander must be expert in understanding the current capabilities witnessed during recent or ongoing persistent conflicts in order to prepare for and counter probable threat tactical actions.

Notes

[1] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 2-33–2-35 and 8-38–3-39.

[2] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 8-39.

[3] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 2-33, 2-36, and 2-47.

[4] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 4-87 and 9-95–9-97.

[5] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-106.

[6] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-146.

[7] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-145.

[8] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 4-105–4-106.

[9] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 3-98–3-100.

[10] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 3-90–3-91.

[11] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-33.

[12] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 4-34.

[13] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 2-52.

[14] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Para 2-14.

[15] Milan Vego. Recce-Strike Complexes in Soviet Theory and Practice. Soviet Army Studies Office. June 1990. Pgs ii and 2. See also: Michael J. Sterling. Soviet Reactions to NATO's Emerging Technologies for Deep Attack. RAND Note N-2294_AF. August 1985; and Larry A. Brisky, "The Reconnaissance Destruction Complex: A Soviet Operational Response to Airland Battle." The Journal of Soviet Military Studies. Volume 3. Issue 2.

[16] Headquarters, Department of the Army. Training Circular 7-100.2, Opposing Force Tactics. TRADOC G-2 Analysis and Control Element (ACE) Threats Integration. 9 December 2011. Paras 9-95–9-97.

[17] Headquarters, Department of the Army. Field Manual 3-09, Field Artillery Operations and Fire Support. 4 April 2014. Para 1-23.

———————

LOITERING MUNITIONS IN THE OPERATIONAL ENVIRONMENT

by Jerry England, TRADOC G-2 ACE Threats Integration (DAC)

A report by the monitoring group Conflict Armament Research revealed the possibility of irregular forces possessing and using explosive-laden unmanned aerial vehicles (UAVs) for operations in the Yemen theater of operations.[1] Loitering munitions, also known as suicide drones or "kamikaze" drones, are a capability typically representative of more advanced regular threat actors. Examples include the Harpy guided missile system and its successor, the Harop. Both systems have the ability to loiter over a suspected target and engage when the conditions for engagement are met. In the case of the Harpy, the radio frequency signature of early warning target acquisition radar will key the system to engage the source of the radiation. The Harop represents an evolution of the Harpy in that not only does it have the same radio-seeking capability of the Harpy, but it also includes electro-optical sensors that are controlled by the operators. These sensors provide visual cues and allow the operator to engage targets based on observations.[2] While some emerging threat forces do not possess the same kind of radio-honing technology found in the Harpy and Harop, the electro-optical capability is a technology that is accessible worldwide and can be used as a simple guidance system for loitering munitions.

Figure 1. Wreckage from an Ababil-type drone

Development and Proliferation of Loitering Munitions

Loitering munitions have a dual-use capability that combines tactical surveillance with the destructive effects of a guided missile. The fielding of these systems is expected to steadily increase as miniaturization of precision-guided munitions and micro unmanned aircraft (UAs)[i] continue to improve.[3] China has developed its own loitering munition, possibly using Israeli technology.[4] Another example of the use of loitering munitions comes from a report saying that a Harop was used as part of an offensive operation by Azerbaijan in the Nagorno Karabakh region.[5] Hybrid threat forces are greatly adapting commercial off-the-shelf systems to provide offensive abilities in combat zones in the Middle East and elsewhere: The adaptation of surveillance drones for strike purposes is an evolutionary process to achieve overmatch or a niche advantage.

Iran's UAV program is one of the oldest in the world. Started in the 1980s during the Iran-Iraq War, the program has developed a number of innovative unmanned systems despite heavy sanctions on military equipment.[6] The Ababil-T UAV is a loitering munition that uses an all-purpose tactical UAV to deliver an explosive payload. By merging the full-motion video and global navigation satellite system of the Ababil II, it is capable of operating at a range up to 100 kilometers.[7] A rail launched platform, the Ababil has been a mainstay of the Iran Aircraft Manufacturing Industries Corporation since the UAV was redesigned in 1991, and is offered as a multirole platform providing surveillance and retransmission services.

Iran is producing UAVs for not just its own military's use, but for an increasing number of foreign customers as well, from Syria to Russia. Analysts at the Center for Strategic and International Studies commented on the similarities between Russia's new Orion UAV and the Iranian version, implying that the Russians are benefitting from Iranian research and development.[8] Exports of technology not only to Russia, but also to Venezuela and Sudan are further examples of the demand for Iranian drones.[9] In 2006, an Israeli press report stated that an F-16 shot down a Hizballah loitering munition, known as Mirsad, illegally flying into Israeli territory during hostilities.[10] The Mirsad was described by Hizballah leaders as having the ability to be "laden with a quantity of explosives 40 to 50 kilograms, and can hit any target, be it water or power

[i] UAV is the title given to platforms used by adversaries of the US—to include the opposing force (OPFOR). When these platforms are discussed in general, without regard to ownership, they are referred to as unmanned aircraft (UAs).

plant, a military base or airport."[11] Other examples of the use of Iranian loitering munitions by its proxies are the discovery of an Ababil variant in Yemen known as the Qasef.[12] Both the Mirsad and the Qasef appear to be variants of the Iranian Ababil II. Use of these weapons against high-value and civilian targets could have implications for air defenders' ability to track small low- and slow-flying drones in the area. An example of this happened in July 2017 when an Israeli Air Defense unit failed to engage a UAV from Syrian airspace. Reasons for the apparent failure ranged from the air defense radar's inability to positively identify UAVs made of certain composite materials, to a procedural failure of the unit in question.[13]

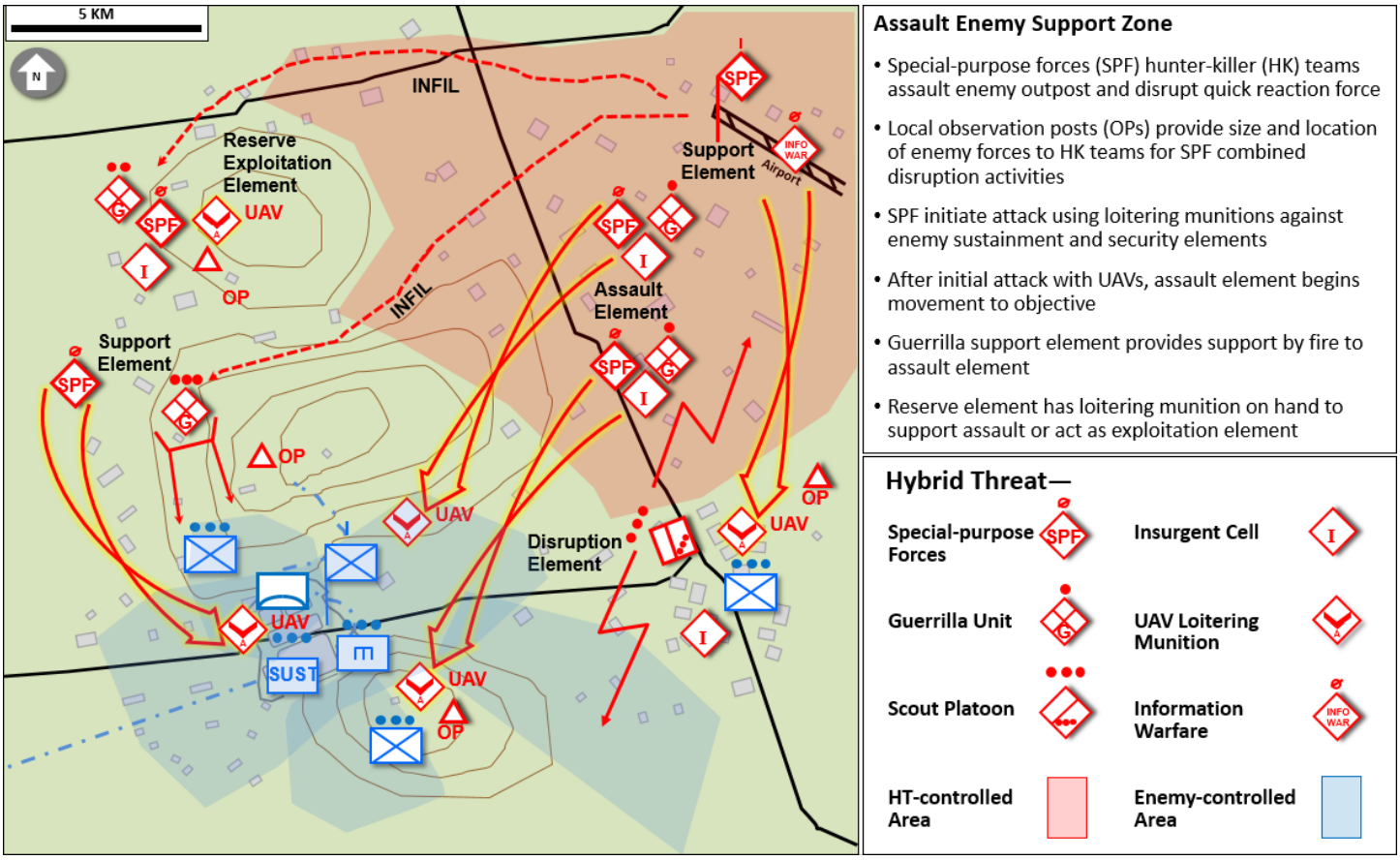


Figure 2. Diagram of an assault with loitering munitions for support

Loitering Munitions in Support of Hybrid Threat Operations

Loitering munitions are used to support both offensive and defensive hybrid threat operations. The ability to target high-value military and civilian targets, especially in urban areas or in other highly congested airspaces, could challenge friend or foe air identification systems. This lack of situational awareness could cause air defenders to expend munitions against friendly unmanned systems while failing to engage other, more capable, manned or unmanned systems. The use of a swarming attack against a single target could overwhelm target acquisition and engagement systems and increase the likelihood of a successful attack. In an urban environment, the ability to use buildings as concealment against electronic early warning systems further threatens the security of high-value targets. It is unclear whether multiple threat loitering munitions can be flown by a single operator; however, a coordinated attack with a relatively low number of platforms could have an advantage in an anti-access/area denial situation, especially in a congested areas.[14]

Loitering munition technology also helps to protect troops establishing a security zone. The ability to engage mobile targets at an extended range means more time to exploit windows of opportunity to transition from defense to offense. Applications include protection of concentrations of troops and equipment, breaching of fighting positions, establishment of a security zone, and provision of close air support.

The tactical strike capability of loitering munitions makes them ideal for supporting offensive operations, such as an integrated attack in dense urban terrain. The ability for loitering munitions to blend in with other UAVs in the area of operations will challenge enemy air defenses, especially in an urban environment. Loitering munitions launched in a dense

urban environment from behind terrain features such as buildings can enable a swarming attack in which a number of platforms converge on a single target within a short timeframe.

Loitering munitions can improve security for enabling elements by extending the disruption zone via denying enemy reconnaissance assets through active targeting by counterreconnaissance elements. By giving assault elements a dual-use surveillance and strike capability, the ability to gain an operational advantage through a surprise attack or deception operations could increase freedom of maneuver as enemy forces react to a loitering munition strike as part of an assault. Loitering munitions can enable a reconnaissance attack and serve as an initiation for the transition from reconnaissance to offense. Loitering munitions that have the ability to hone in on frequencies or possibly communications devices could be used as part of a perception management campaign designed to reduce the influence of enemy leaders and facilitators.

Ababil II Technical Characteristics

The Ababil II, along with the Mohajer, is one of Iran's most proliferated UAV system. It is advertised as a tactical surveillance and communications relay platform. All Ababil II variants have a cylindrical fuselage, a large rear wing, and a shorter front wing.[15] The Ababil is controlled by a single operator and can be transported by a medium truck. Its 40-kilogram payload consists of flight controls, optics, and 16-liter fuel tank, leaving approximately 17-kilograms for an explosive charge.[16] The explosive charge could cause damage to field-expedient and reinforced fighting positions.[17] It could destroy unprotected ammunition storage areas or large fuel containers. The threat to troops in the open is considered low due to lack of shrapnel.

Training Implications

UAVs are becoming more accessible, easier to operate, and more capable for a wide range of military uses, including strike capabilities. As a result, the need to detect small UAs, determine their identity, and engage them with an appropriate response will become increasingly important—especially in urban areas and heavily congested airspaces such as combat zones.[18] In summary, the following are ways hybrid threats could use loitering munitions:

- A large number of loitering munitions conducting a saturation attack could overwhelm air defenses.
- Targeted strikes against high-value targets such as command nodes, ammunition storage facilities, and civilian targets can cause significant operational damage.
- Small units enabled with dual-use surveillance and strike capable will enable offensive operations throughout the area of operation.
- Loitering munitions can enable security operations by extending the disruption zone around hybrid threat units in the defense.

Notes

[1] Kelsey Atherton. "Report: Iran built a guided missile in a drone's body for rebels in Yemen." Popular Science. 31 March 2017.
[2] Newsweek. "Israel tests 'Suicide Drones' for secret foreign buyers." 6 August 2015.
[3] Larry Friese, N.R. Jenzen-Jones, and Michael Smallwood. Emerging Unmanned Threats: The Use of Commercially-Available UAVs by Armed Non-State Actors. Armament Research Services. 2016. Pg 30.
[4] David Hambling. "China's Mini-Drone Packs a Heavyweight Punch." Popular Mechanics. 5 May 2016.
[5] Thomas Gibbons-Neff. "Israeli-Made Kamikaze Drone Spotted in Nagorno-Karabakh Conflict." Washington Post. 5 April 2016.
[6] Michael Rubin. "Iran Says Russia Desperate for UAV Technology." American Enterprise Institute. 16 November 2016.
[7] Don Rassler. Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology. Combating Terrorism Center. October 2016. Pg 55.
[8] John Kester. "Russian Drone Tech May Include Help From Iran." Foreign Policy. 5 October 2017.
[9] Michael Rubin. "Iran Says Russia Desperate for UAV Technology." American Enterprise Institute. 16 November 2016.
[10] David Isby. "Hizbullah uses UAVs as missiles." Jane's. 25 October 2006.
[11] Associated Press. "Hezbollah Says It Has the Ability to Bomb Israeli Targets From Air." Haaretz. 14 November 2004.
[12] Kelsey Atherton. "Report: Iran Built a Guided Missile in a Drone's Body for Rebels in Yemen." Popular Science. 31 March 2017.
[13] Barbara Opall-Rome. "Syrian-Launched UAV Evades Israeli Air Defenses." Defense News. 17 July 2017.
[14] Defense Advanced Research Projects Agency . "Keeping a Watchful Eye of Low-Flying Unmanned Aerial Systems in Cities." 13 September 2016.
[15] Galen Wright. "Ababil UAV." Arkenstone. 5 February 2011.
[16] Galen Wright. "Ababil UAV." Arkenstone. 5 February 2011.
[17] Galen Wright. "Ababil UAV." Arkenstone. 5 February 2011.
[18] Defense Advanced Research Projects Agency . "Keeping a Watchful Eye of Low-Flying Unmanned Aerial Systems in Cities." 13 September 2016.

What ACE Threats Integration Supports for YOUR Readiness

- **Determine Operational Environment (OE) conditions for Army training, education, and leader development.**
- **Design, document, and integrate hybrid threat opposing forces (OPFOR) doctrine for near-term/midterm OEs.**
- **Develop and update threat methods, tactics, and techniques in HQDA Training Circular (TC) 7-100 series.**
- **Design and update Army exercise design methods-learning model in TC 7-101/7-102.**
- **Develop and update the US Army *Decisive Action Training Environment (DATE)*.**
- **Develop and update the US Army *Regionally Aligned Forces Training Environment (RAFTE)* products.**
- **Conduct Threat Tactics Course resident at Fort Leavenworth, KS.**
- **Conduct Threat Tactics mobile training team (MTT) at units and activities.**
- **Support terrorism-antiterrorism awareness in threat models and OEs.**
- **Research, author, and publish OE and threat related classified/unclassified documents for Army operational and institutional domains.**
- **Support Combat Training Centers (CTCs) and Home Station Training (HST) and OE Master Plan reviews and updates.**
- **Support TRADOC G-2 threat and OE accreditation program for Army Centers of Excellence (CoEs), schools, and collective training at sites for Army/USAR/ARNG.**
- **Respond to requests for information (RFIs) on threat and OE issues.**

ACE Threats Integration POCs

DIR, ACE Threats Integration	Jon Cleaves	
jon.s.cleaves.civ@mail.mil	913-684-7975	
Dep DIR & DATE	DAC Angela Williams	
angela.m.williams298.civ@mail.mil	-7929	
Intel OPS Coordinator	DAC Nicole Bier	
nicole.n.bier.civ@mail.mil	DSN:552 -7907	
UK LO to ACE-TI	WO2 Danny Evans	
daniel.j.evans92.fm@mail.mil	-7994	
Threats Officer	LTC Bryce Frederickson	
bryce.e.frederickson.mil@mail.mil	-7930	
Threats Officer	MAJ James Andersen	
james.r.andersen20.mil@mail.mil	-7952	
Threats Officer	MAJ EJ Kesselring	
emil.j.kesselring.mil@mail.mil	-7898	
Threat Models	DAC Jerry England	
jerry.j.england.civ@mail.mil	-7934	
Threat Tactics Course	DAC Kris Lechowicz	
kristin.d.lechowicz.civ@mail.mil	-7922	
Threat Doctrine	DAC Dr. Jon H. Moilanen	
jon.h.moilanen.civ@mail.mil	-7928	
Training-Edu-Ldr Dev	DAC Walt Williams	
walter.l.williams112.civ@mail.mil	-7923	
Threat Analysis	CGI Brian Allen	
brian.d.allen44.ctr@mail.mil	-7948	
Threat Analysis	IDSI Dr. Jim Bird	
james.r.bird.ctr@mail.mil	-7919	
Threat Analysis	BMA Rick Burns	
richard.b.burns4.ctr@mail.mil	-7987	
Worldwide Eqmt Guide	BMA John Cantin	
john.m.cantin.ctr@mail.mil	-7899	
Thr Analysis & Editing	CGI Laura Deatrick	
laura.m.deatrick.ctr@mail.mil	-7925	
Threat Analysis	CGI Jay Hunt	
james.d.hunt50.ctr@mail.mil	-7960	
ACE-TI LO to MCTP	BMA Pat Madden	
patrick.m.madden16.ctr@mail.mil	-7997	
Threat Analysis	CGI Mike Marsh	
michael.g.marsh3.ctr@mail.mil	-7897	
Threat Analysis	CGI Brad Marvel	
bradley.a.marvel.ctr@mail.mil	-5963	
Threat Analysis	CGI Dave Pendleton	
henry.d.pendleton.ctr@mail.mil	-7946	
ACE-TI LO to JRTC/JMRC	CGI Mike Spight	
michael.g.spight.ctr@mail.mil	-7974	
Threat Analysis	CGI Jamie Stevenson	
james.e.stevenson3.ctr@mail.mil	-7995	
Threat Analysis	CGI Wayne Sylvester	
vernon.w.sylvester.ctr@mail.mil	-7939	
ACE-TI LO to NTC	ThreatTec Marc Williams	
james.m.williams257.ctr@mail.mil	-7943	