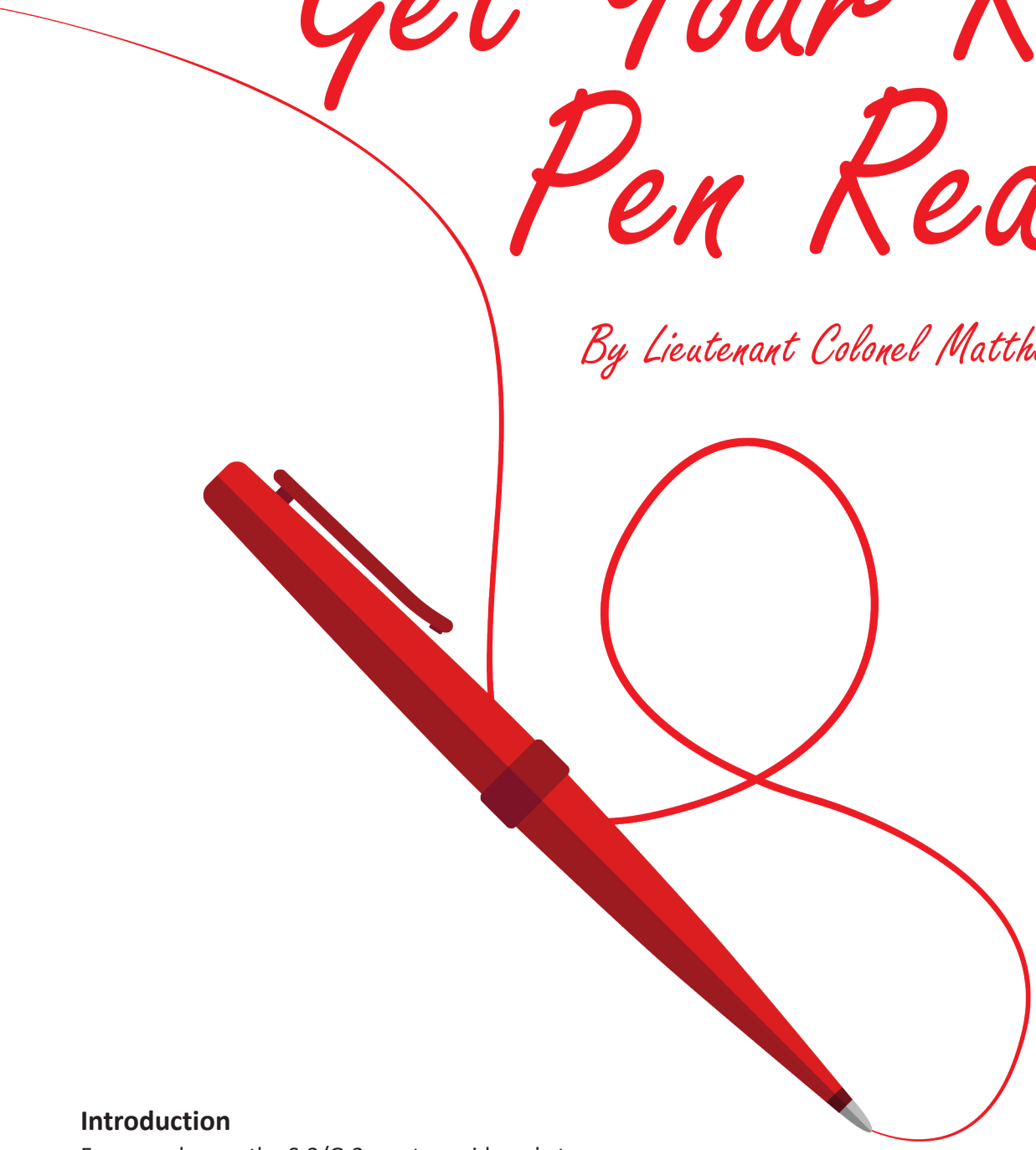
Get Your Red Pen Ready.

By Lieutenant Colonel Matthew J. Fontaine



Introduction

Everyone knows the S-2/G-2 must provide only two enemy courses of action (COAs) during the mission analysis brief, and it is a job well done. These two COAs, the most likely and most dangerous, provide the commander and staff with everything they need to know about how the threat will fight against friendly actions throughout the execution of a complex operation, right? Sure, we know that doctrine asks us to "identify the *full* set of courses of action available to the threat,"[1] but who does that?

The intelligence cell should do that, of course. This article recommends that intelligence cells continuously develop and refine three categories of enemy COAs, instead of the two standard most likely and most dangerous enemy COAs, to better account for the tactical and operational options available to a thinking enemy in large-scale combat operations.[2] Better enemy COAs result in better friendly plans. Better plans result in friendly forces more likely to seize opportunities or avoid disaster during the execution of operations. So, get your red pen ready! The three enemy COA categories are:

- Operational enemy COAs.
- Critical event enemy COAs.
- Transition enemy COAs.

Now, don't get me wrong. The intelligence cell must still designate the most likely and most dangerous enemy COAs, but they must do so for *each category*. Identifying the most likely and most dangerous enemy COAs is essential because they enable the commander to develop optimized friendly plans in environments that are often time constrained.[3] The staff then develops contingency options (think branches, sequels, or alternate COAs) should the enemy execute any other *valid COA* available to the threat for each category.[4] (I will discuss the value of the most likely and most dangerous designations in the context of the three enemy COA categories again near the conclusion of this article.)

In this article, I will explain why the typical enemy COAs drafted by many intelligence cells do not meet the challenges of large-scale combat operations. I will then describe each enemy COA category in detail. I will then conclude with a discussion on developing logical priority intelligence requirements (PIRs) to detect any valid enemy COA selected by the threat.

The Problem with "Two and Done"

The standard two enemy COAs typically developed by intelligence cells often do not provide the complete conceptual narrative and details the commander and staff need to create an effective plan. Effective plans posture the unit to overcome the current enemy challenge *and* execute critical future transitions, like branches or sequels, without unnecessary risk.[5]

Enemy COAs often come up short because they try to provide too much information from the start but do too little to support the development of effective plans. This tendency is especially true for enemy COAs developed for command post exercises, large-scale combat operations scenarios at the division and higher echelons, or the initial COA a brigade creates before an Army combat training center rotation. Here is what I mean: the typical command post exercise or initial combat training center enemy COA often focuses on how the threat will achieve its operational or strategic end state from start to finish. I dub this enemy COA the *operational enemy course of action* (OECOA, pronounced OH COA); it is an essential COA.[6] However, an operational enemy COA only tells part of the story to the commander and staff. The intelligence cell uses the operational enemy COA to portray how the enemy could achieve its overall mission and end state. It has limited utility for developing effective plans for two primary reasons.

First, an operational enemy COA cannot provide the necessary details for good staff work because it must cover so much ground, literally and figuratively. It is not uncommon for an operational enemy COA in a typical large-scale combat operations scenario to describe how an enemy division, corps, or even army will execute an entire operation—from invasion to the destruction of the friendly forces over hundreds or even thousands of square kilometers! Intelligence cells often describe an operational enemy COA using a single paragraph or PowerPoint slide. How valuable can this analysis be in supporting detailed, friendly planning?

Second, the intelligence cell drafts operational enemy COAs during mission analysis before developing friendly COAs. Given this arrangement, operational enemy COAs only consider opposing forces in the most general sense, as the detailed, friendly plan does not yet exist. From its inception, an operational enemy COA is of limited value because the intelligence cell did not construct it in relation to friendly actions.

But we know war, particularly large-scale combat operations, must be considered from both friendly and enemy perspectives. Carl von Clausewitz imagined war as a match between two wrestlers: "Each [wrestler] tries through physical force to compel the other to do his will; his *immediate* aim is to *throw* his opponent in order to make him incapable of further resistance."[7] Clausewitz's analogy evokes an image of a violent fight. One sees two competitors locked in a fierce back-and-forth struggle to gain advantage before one side imposes its will in a final tremendous effort to emerge victorious.

Our enemy COAs should account for this dynamic nature of war–but often, they do not. Instead, many intelligence cells develop operational enemy COAs without understanding the friendly plan. And how could this not be the case? S-2s/G-2s present enemy COAs during mission analysis before friendly COA development. Look at many operational enemy COAs (and friendly COAs, for that matter) to see how little we take our opponent's actions into account. Most enemy COAs have a few blue opponent icons or tasks at the end of a sequence of enemy steps as if the friendly forces were just along for the ride. Some include no friendly icons or tactical tasks at all!

Developing a friendly COA with just an operational enemy COA is akin to a wrestler preparing for a live opponent based solely on a session with a wrestling dummy.[8] Like wrestling against a dummy, typical operational enemy COAs provide no sense of the dynamic reactions and counteractions necessary to spur commanders' and staffs' thinking on how best

to design a friendly operation considering the complete set of options available to a threat. The limited utility of operational enemy COAs becomes readily apparent after being briefed during mission analysis. The S-2/G-2 receives a deluge of "how" questions from the commander and staff: how will the enemy react to a particular aspect or critical event of a friendly COA? How long will an enemy transition take? And so on.

I know what you think; the war game will address many of these questions. After all, the purpose of the S-2/G-2 during the war game is to project how the enemy will react to the friendly COA, including its constituting critical events.[9] But do they always? And how far do staff get during war gaming in time-constrained environments or under demanding conditions (if the war game even happens)? If a war game does occur, is the S-2/G-2 prepared to execute the basic war-gaming "action, reaction, and counteraction methods of friendly and enemy forces interaction"[10] for *every* critical event described in doctrine, armed with only a most likely and most dangerous operational enemy COA? I am not convinced based on my experience. Many of us have been guilty of using the same enemy COA paragraph or PowerPoint we initially showed during mission analysis for the operations order at the end of the military decision-making process (MDMP). We all agree that this should not occur if the command and staff truly wrestle with the problem presented by the enemy.

Suppose you are an S-2 or G-2 that comprehensively updates the intelligence preparation of the operational environment products at the end of war-gaming. (There should be significant changes, correct?) In that case, you are ahead of the game!

Whether or not you update your products, don't you wish you had more depth in your enemy COAs before the war game so as not to provide shallow responses or, to put it politely, baloney? Or that you had better enemy COAs during mission analysis to give the commander and staff a better starting point for developing more comprehensive friendly COAs, branches, and sequels, with the idea that better input—both friendly and enemy—will result in a better war game output?

One thing is sure: no G-2 or S-2 wants to find themselves at a war game considering for the first time the enemy's reaction to some critical event, like a wet gap crossing! The enemy fights to win in large-scale combat operations and will use every technically and tactically ingenious method to prevail. We must think deeply to beat these opponents, so broad enemy COAs alone will not cut it. The solution to providing better enemy COAs—and better friendly COAs as a result—is to start with the big picture.

Operational Enemy Courses of Action

The first set of enemy COAs to develop are the operational enemy COAs. Even though I just seemingly maligned them, creating quality operational enemy COAs is essential to understanding the threat from a complete narrative perspective. Operational enemy COAs describe how the enemy might achieve its desired operational or strategic end state from start to finish, arranged along a line of operation (LOO). It is a conceptual product that lets the staff visualize how an enemy operation could evolve holistically. Operational enemy COAs are also essential to anticipating how enemy forces can enter and exit the unit's deep area or flanks (a vital aspect for targeting and intelligence handover line coordination). The intelligence cell derives the operational enemy COAs from the enemy COAs developed by its higher headquarters.[11]

For example, a division's analysis and control element derives its operational enemy COA from the corps enemy COAs, with a *slight* emphasis on the forces templated in the division's area of operations (AO). I say slight because the purpose of the operational enemy COA is to gain a holistic understanding of the big picture, so focusing just on one's own AO misses the point, potentially obscuring how the enemy in one's area of interest (AOI) could present a risk to the mission or forces. Operational enemy COAs are the first enemy COAs presented during mission analysis and serve as the foundation for all future enemy COA development.

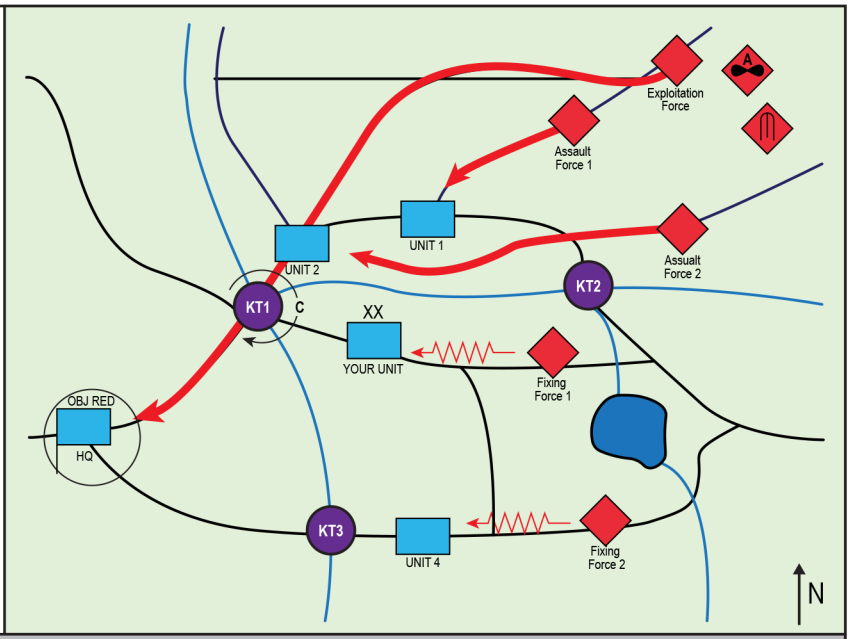
Importantly, if an intelligence cell has no higher enemy COAs on which to base its operational enemy COAs, that cell must produce them. If a unit disagrees with the enemy COAs of the higher team, it cannot simply change or ignore them. To do so would contravene the necessity of having a common understanding of the threat. Instead, every intelligence cell must collaborate through both staff and command channels to arrive at a common understanding of the threat with their higher headquarters before moving on with planning.

Figures 1–5 provide simplified examples of higher echelons' enemy COAs and associated operational enemy COAs developed by the fictional YOUR UNIT. Ideally, the intelligence cell would produce multiple operational enemy COAs, each nested within the higher echelon's read of the situation.

Operational enemy COAs frame the possible range of valid enemy COAs to include the most likely and most dangerous available to the threat based on the friendly's understanding of the enemy's mission, intent, key tasks, and end state within the AO and AOI. As mentioned, this is usually as far as intelligence cells get at the start of any large-scale combat operations scenario, but we know more is needed. Therefore, the next step is to develop more detailed enemy COAs. Key to this is understanding the likely critical event of a given LOO.

Mission: Enemy forces attack to seize OBJ RED (friendly capital city) to install a politically favorable regime.
Enemy Commander's Intent: Gain rapid control of OBJ RED while minimizing the loss of combat power.
End State:
Enemy: Friendly forces cleared in OBJ RED.
Friendly: Combat effectiveness above 60% with an established area defense at OBJ RED to defeat the HIGHER FRIENDLY RESERVE.
Terrain: River crossing sites at KT 1, 2, 3, are intact.

LEGEND	
COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective

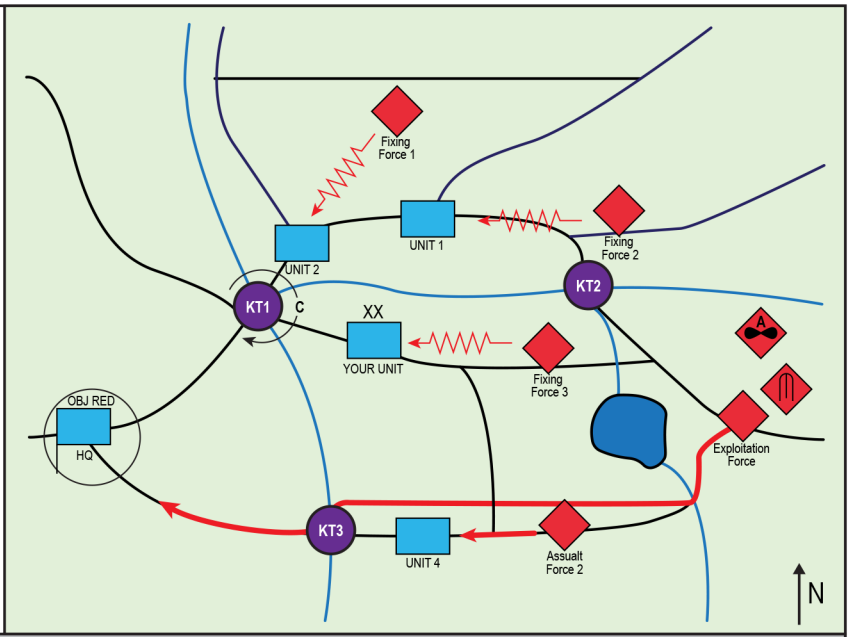


This figure is a simplified representation of an ECOA YOUR UNIT may receive from its higher echelon. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the northern axis in this COA. The higher echelon designates this ECOA, ECOA 1 - HEAVY NORTH.

Figure 1. Higher Echelon Enemy Course of Action One: Heavy North[12]

Mission: Enemy forces attack to seize OBJ RED (friendly capital city) to install a politically favorable regime.
Enemy Commander's Intent: Gain rapid control of OBJ RED while minimizing the loss of combat power.
End State:
Enemy: Friendly forces cleared in OBJ RED.
Friendly: Combat effectiveness above 60% with an established area defense at OBJ RED to defeat the HIGHER FRIENDLY RESERVE.
Terrain: River crossing sites at KT 1, 2, 3, are intact.

LEGEND	
COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective



This figure is a simplified representation of a second ECOA a unit may receive from its higher echelon. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the southern axis in this COA. The higher echelon designates this ECOA, ECOA 2 - HEAVY SOUTH.

Figure 2. Higher Echelon Enemy Course of Action Two: Heavy South[13]

Mission: Fixing Force 1 attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the northern axis.

Enemy Commander's Intent: Rapidly fix YOUR UNIT with limited infrastructure damage.

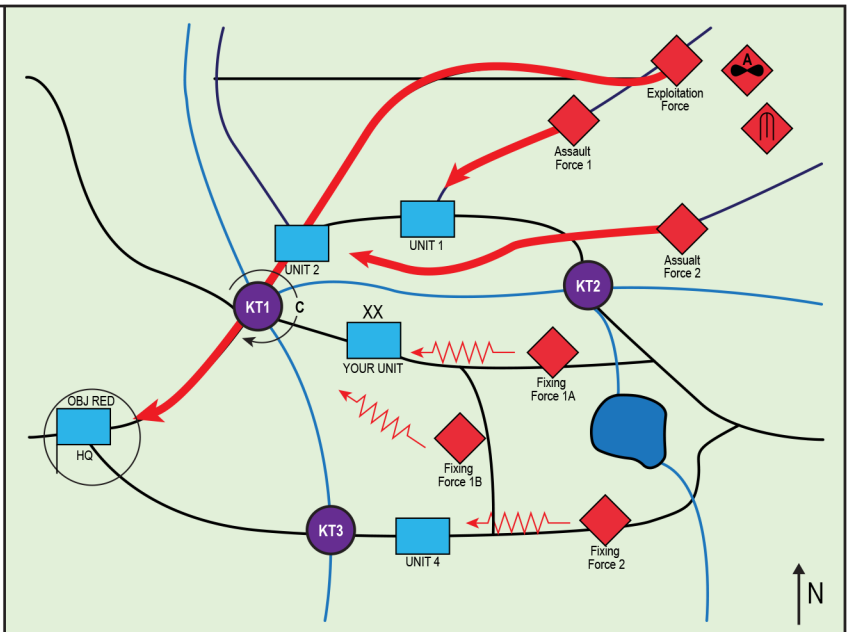
End State:

Enemy: Friendly forces unable to interfere with the seizure of OBJ RED.

Friendly: Combat effectiveness above 60% and postured to conduct wet gap crossing.

Terrain: The river crossing site at KT 1 is intact.

LEGEND	
AO	area of operation
COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OECOA	operational enemy course of action



This figure is a simplified representation of an OECOA YOUR UNIT developed. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along a northern axis in this COA. In the YOUR UNIT AO, Fixing Force 1 attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the northern axis. YOUR UNIT designates this ECOA, OECOA 1 - HEAVY NORTH, SOUTHERN FIX. YOUR UNIT adds additional detail to OECOA 1, represented here by the delineation of Fixing Force 1 into Fixing Force 1A and 1B while ensuring OECOA 1 is nested within the higher echelon's ECOA 1.

Figure 3. Operational Enemy Course of Action One: Heavy North, Southern Fix[14]

Mission: Fixing Force 3A attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the southern axis.

Enemy Commander's Intent: Rapidly fix YOUR UNIT with limited infrastructure damage.

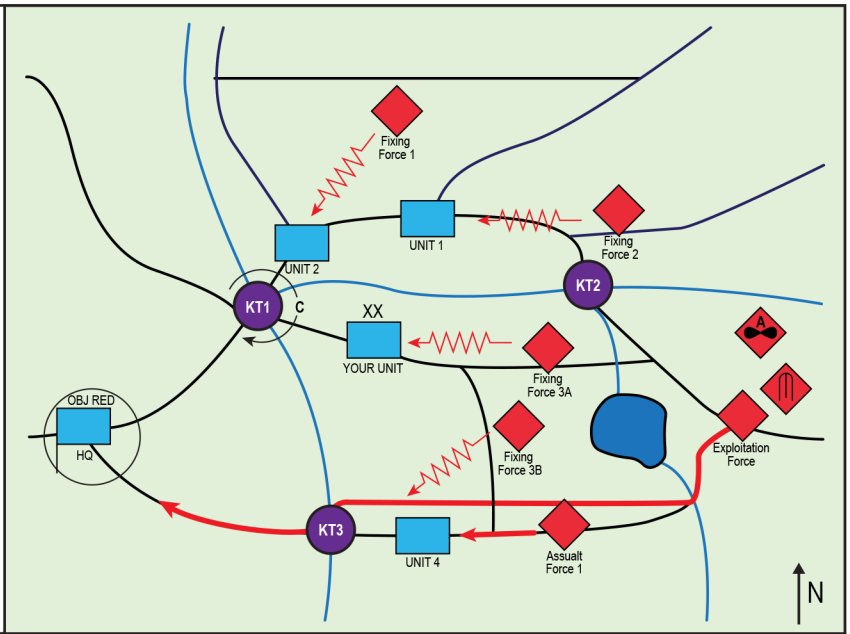
End State:

Enemy: Friendly forces unable to interfere with the seizure of OBJ RED.

Friendly: Combat effectiveness above 60% and postured to conduct wet gap crossing.

Terrain: The river crossing site at KT 1 is intact.

LEGEND	
AO	area of operation
COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OECOA	operational enemy course of action



This figure is a simplified representation of a second OECOA YOUR UNIT developed. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the southern axis in this COA. In the YOUR UNIT AO, Fixing Force 3A attacks to fix YOUR UNIT to prevent the massing of combat power on the Exploitation Force in the northern axis. YOUR UNIT designates this ECOA, OECOA 2 - HEAVY SOUTH, SOUTHERN FIX. YOUR UNIT adds additional detail to OECOA 2, represented here by the delineation of Fixing Force 3 into Fixing Force 3A and 3B while ensuring OECOA 2 is nested within the higher echelon's ECOA 2.

Figure 4. Operational Enemy Course of Action Two: Heavy South, Southern Fix[15]

Mission: Assault Force 1 attacks to defeat YOUR UNIT to enable the Exploitation Force seizure of OBJ RED in the southern axis.

Enemy Commander's Intent: Rapidly defeat YOUR UNIT with limited infrastructure damage.

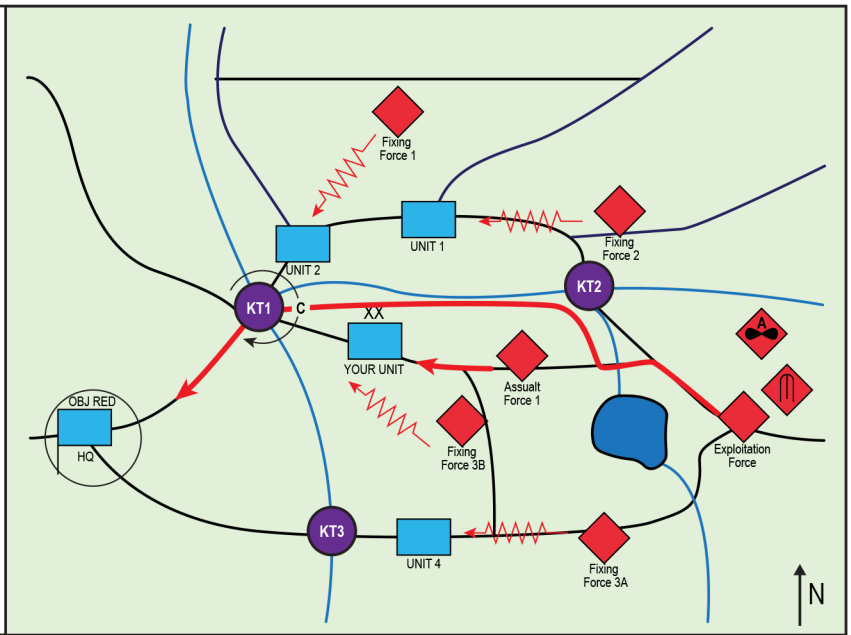
End State:

Enemy: YOUR UNIT unable to interfere with the seizure of OBJ RED.

Friendly: Combat effectiveness above 60% and postured to conduct wet gap crossing.

Terrain: The river crossing site at KT 1 is intact.

LEGEND	
AO	area of operation
COA	course of action
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OECOA	operational enemy course of action



This figure is a simplified representation of a third OECOA YOUR UNIT developed. Enemy forces attack to seize OBJ RED, a friendly capital city. The enemy weights its efforts along the southern axis in this COA. In the YOUR UNIT AO, Fixing Force 3B attacks to fix YOUR UNIT. Once fixed, Assault Force 1 attacks to defeat YOUR UNIT to enable the seizure of OBJ RED by the Exploitation Force. YOUR UNIT designates this ECOA, OECOA 3 - HEAVY SOUTH, SOUTHERN DEFEAT. YOUR UNIT modifies OECOA 2, represented here be shifting the avenue of approach of the Exploitation Force within the southern axis, to account for the possibility of the main attack against YOUR UNIT.

Figure 5. Operational Enemy Course of Action Three: Heavy South, YOUR UNIT Defeated[16]

Critical Event Enemy Courses of Action

The second set of enemy COAs to develop is what I will dub *critical event* enemy COAs (CECOA, pronounced "SEE COA"). Critical event enemy COAs are like the "snapshots in time" situation template described in doctrine that represent a "potential threat COA as part of a particular threat operation."[17] Like a situation template, a critical event enemy COA describes how the enemy might achieve its desired *tactical* end state in pursuit of its *operational* end state. The difference between a critical event enemy COA and a situation template is that a critical event enemy COA emphasizes the anticipated enemy COA's *relationship* to the anticipated friendly COA or action during a specific critical event. Critical event enemy COAs are detailed products that enable the staff to visualize the separate ways (actions, reactions, and counterreactions) the enemy will seek to gain the advantage (win) during a particular portion of a LOO given a friendly action.[18] Critical event enemy COAs ensure we approach enemy COA development from the back-and-forth perspective of Clausewitz's wrestlers.

For example, imagine the LOO in figure 6 (on the next page) associated with a simple operational enemy COA and a *failure* operational enemy COA (more on failure COAs later). The example LOO has three critical events with these possible friendly actions and enemy counteractions:

- Critical Event 1.
  - Friendly Action: Seize OBJECTIVE ONE (Capital City).
  - Enemy Counteraction: Defend OBJECTIVE ONE.

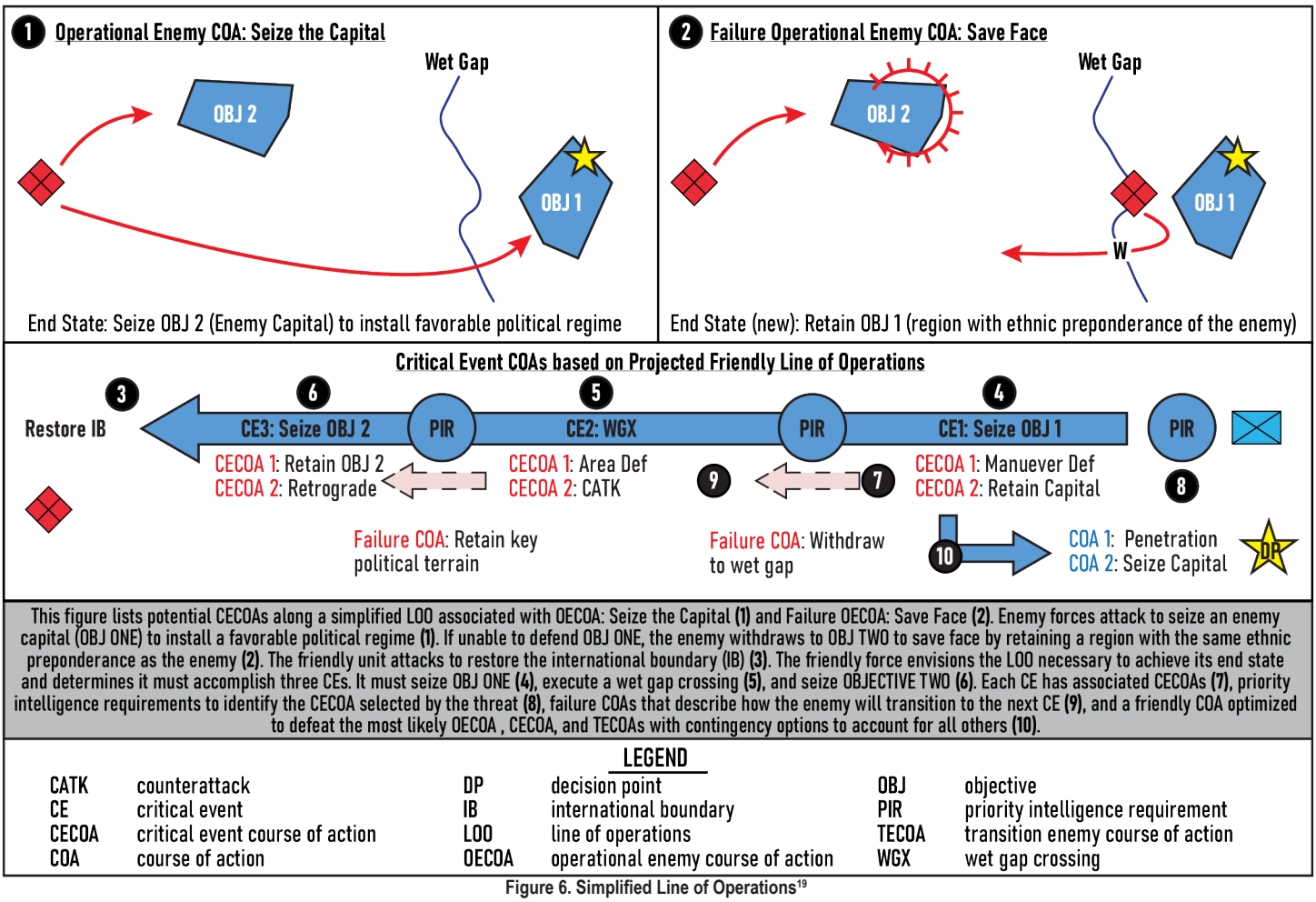
The enemy can defend OBJECTIVE ONE broadly via a maneuver defense (CECOA 1 for CE 1) or an area defense to retain the capital (CECOA 2 for CE 1).

- Critical Event 2.
  - Friendly Action: Execute Wet Gap Crossing.
  - Enemy Counteraction: Defeat Wet Gap Crossing.

The enemy can defend key crossing sites of the wet gap via an area defense (CECOA 1 for CE 2) or, broadly, via a maneuver defense (CECOA 2 for CE 2).

- Critical Event 3.
  - Friendly Action: Seize OBJECTIVE TWO.
  - Enemy Counteraction: Defend to retain OBJECTIVE TWO. (CECOA 1 for CE 3) or retrograde (CECOA 2 for CE 3).

This is simple stuff. The intelligence cell develops multiple *initial* critical event enemy COAs for each critical event to present during the mission analysis brief that they refine throughout the MDMP. The S-2/G-2 designates each critical event enemy COA as the most likely, most dangerous, or some other valid enemy COA for that critical event. The result is that the S-2/G-2 will develop the most likely and most dangerous critical event enemy COAs (and other valid critical event enemy COAs) for the most likely operational enemy COA, and the same goes for the most dangerous critical event enemy COA (and other valid operational enemy COAs). Given the already high demands on an intelligence cell for the mission analysis brief, this is a tall order, but it will pay dividends. If not possible, the intelligence cell should begin developing or refining critical event enemy COAs immediately after the mission analysis brief as the friendly plan takes form. The enemy critical events will likely be a mirror image of the friendly anticipated critical events.



This figure lists potential CECOAs along a simplified LOO associated with OECOA: Seize the Capital **(1)** and Failure OECOA: Save Face **(2)**. Enemy forces attack to seize an enemy capital (OBJ ONE) to install a favorable political regime **(1)**. If unable to defend OBJ ONE, the enemy withdraws to OBJ TWO to save face by retaining a region with the same ethnic preponderance as the enemy **(2)**. The friendly unit attacks to restore the international boundary (IB) **(3)**. The friendly force envisions the LOO necessary to achieve its end state and determines it must accomplish three CEs. It must seize OBJ ONE **(4)**, execute a wet gap crossing **(5)**, and seize OBJECTIVE TWO **(6)**. Each CE has associated CECOAs **(7)**, priority intelligence requirements to identify the CECOA selected by the threat **(8)**, failure COAs that describe how the enemy will transition to the next CE **(9)**, and a friendly COA optimized to defeat the most likely OECOA , CECOA, and TECOAs with contingency options to account for all others **(10)**.

LEGEND

CATK	counterattack	DP	decision point	OBJ	objective
CE	critical event	IB	international boundary	PIR	priority intelligence requirement
CECOA	critical event course of action	LOO	line of operations	TECOA	transition enemy course of action
COA	course of action	OECOA	operational enemy course of action	WGX	wet gap crossing

Figure 6. Simplified Line of Operations[19]

How can the S-2/G-2 recognize friendly actions during mission analysis to develop the initial critical event enemy COAs when COA development has not started? My advice is not to overthink the initial critical event enemy COAs. If a piece of key terrain is essential enough for the enemy to defend it, friendly forces will likely have to seize it. If a large river flows through the AO, both sides may have to cross it. Therefore, it becomes necessary for the intelligence cell to describe how enemy forces would react to friendly actions at that objective if the staff is to build an effective plan. Hopefully, in their initial planning guidance, the higher echelon's order or the unit commander will identify or at least indicate likely critical events for the unit. If not, ask the commander and staff to get thinking!

If prepared correctly, the critical event enemy COAs will supercharge friendly COA development after mission analysis. The staff will better understand the risk to the mission and force during critical aspects of the overall operation from the start within the context of the general enemy's operation, thanks to the operational enemy COA. Critical event enemy COAs also focus on the detailed planning of all warfighting functions in more concrete situations within the larger enemy and friendly picture. For example, given a particular critical event enemy COA, a member of the protection cell will have to think deeply about how to shield forces during a wet gap crossing while staying nested within the general scheme of protection for the overall friendly COA, which itself is designed to account for the most likely operational enemy COA. Detailed planning like this is essential to understanding and mitigating risk.

Critical event enemy COAs are the intelligence cell's primary input to the war game; the war game refines them. Providing draft critical event enemy COAs during mission analysis ensures that the staff has already had an opportunity to think deeply about the valid, serious problems the unit will likely encounter during different portions of the operation, including the most likely and most dangerous ones. Quality critical event enemy COAs ensure that the COA analysis of the MDMP includes a genuine war game instead of what can be a series of ad hoc responses to inch-deep tactical dilemmas.

The next step is to consider what happens if the threat fails (or succeeds) in achieving its objectives.

Transition Enemy Courses of Action

The third set of enemy COAs to develop is what I will dub the *transition* enemy COA (TECOA, pronounced "TEE COA"). A transition enemy COA anticipates what actions the enemy might take initially if unable to achieve a critical event on its LOO. Or, a transition enemy COA might envision how an enemy could seize an opportunity because the enemy completed

its assigned objectives at costs below what was anticipated for factors such as time or battle damage. First, I'll discuss a *failure* transition enemy COA and second, a success transition enemy COA.

Failure transition enemy course of action. The failure transition enemy COA describes how the enemy will attempt to regain the conditions necessary to achieve the current end state described in the operational enemy COA or a modified end state based on the new battlefield realities.[20] Stated another way, the failure transition enemy COA describes how the threat will *transition* from a state of relative disadvantage to a situation of relative advantage to the friendly force.[21] The Save Face COA in figure 6 is an example of a transition enemy COA at the operational level. The enemy sought to seize OBJECTIVE ONE but transitioned to retaining OBJECTIVE TWO when it could not. Remember: the enemy constantly fights to win, and our enemy COAs must always reflect this.

Failure transition enemy COAs are issued with their respective operational enemy COA or critical event enemy COA. They enable the commander and staff to develop success *branches and sequels* to exploit the threat's momentary failure before they shift to a failure transition enemy COA.

Figures 7 and 8 (on the next page) provide simplified examples of transition enemy COAs developed by the fictional YOUR UNIT. Ideally, the intelligence cell would produce multiple transition enemy COAs for each operational enemy COA and critical event enemy COA while also designating the most likely and dangerous instances.

Consider a wet gap crossing for another example of the power of sequel planning thanks to a quality transition enemy COA. A high-performing intelligence cell presents an initial wet gap crossing critical event enemy COA during mission analysis to kick off detailed, friendly planning for this event. At this point, staff typically do one of three things.

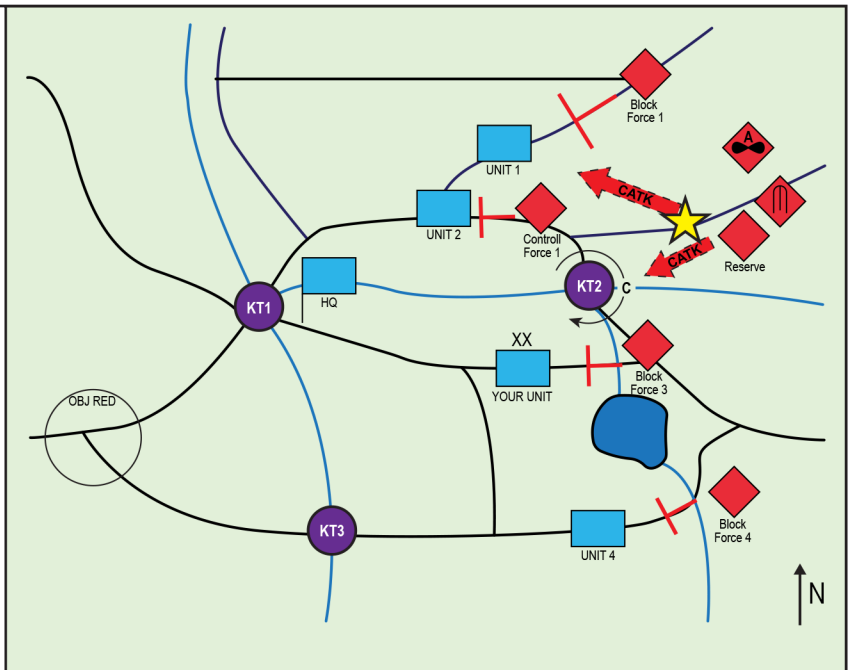
One staff only designs a plan for crossing the wet gap against the threat described in the critical event enemy COA. This isn't bad; it's certainly better than only planning against an operational enemy COA or only planning for the critical event enemy COA after publishing the base operations order. But, as we will see with the following staff scenario, a critical event enemy COA only improves a friendly plan by so much.

The second staff war-games the critical event enemy COA and identifies the possibility of a sequel, which leads to the creation of a new decision point. Something like, *Decision Point 1: conduct sequel after wet gap crossing*. Unfortunately, little detailed planning goes into the sequel to increase the odds of success because the enemy situation becomes too murky at this point. As a result, the unit culminates after crossing the river during execution and watches as the enemy retrogrades, unable to exploit their initial success. In other words, even with a decision point, this staff mainly reacts to the enemy situation as it emerges. It cannot effectively sequence its actions to maintain pressure on the enemy.

Here is where things get interesting. A third staff receives a wet gap critical event enemy COA and a *failure* transition enemy COA. The commander and staff listen with great interest

Mission: Block Force 3 defends to block YOUR UNIT west of the wet gap along the southern axis to enable the control of KT 2 by Control Force 1.
Enemy Commander's Intent: YOUR UNIT freedom of movement is restricted east of the river. Conditions set for a favorable political settlement.
End State:
Enemy: YOUR UNIT is unable to interfere with the control of KT 2.
Friendly: Combat effectiveness above 40%.
Terrain: The river crossing site and road junction at KT 2 are controlled and intact.

LEGEND	
AO	area of operation
CATK	counterattack
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
TECOA	transition enemy course of action



This figure is a simplified representation of a Failure TECOA YOUR UNIT developed at the operational level. Enemy forces withdraw to control KT2, a critical river crossing site and road junction. In the YOUR UNIT AO, Block Force 3 defends to block YOUR UNIT to enable the control of KT 2 by Control Force 1. YOUR UNIT designates this ECOA, TECOA 1 – KT 1 AND WET GAP DEFENSE.

Figure 7. Failure Transition Enemy Course of Action One: Key Terrain One and Wet Gap Defense[22]

Mission: Crossing Site Force defeats YOUR UNIT at KT 1 to enable the destruction of the HIGHER RESERVE by the Exploitation Force.

Enemy Commander's Intent: YOUR UNIT is unable to interfere with the Crossing or Exploitation Force freedom of movement across the river. Conditions for the defeat of friendly forces set.

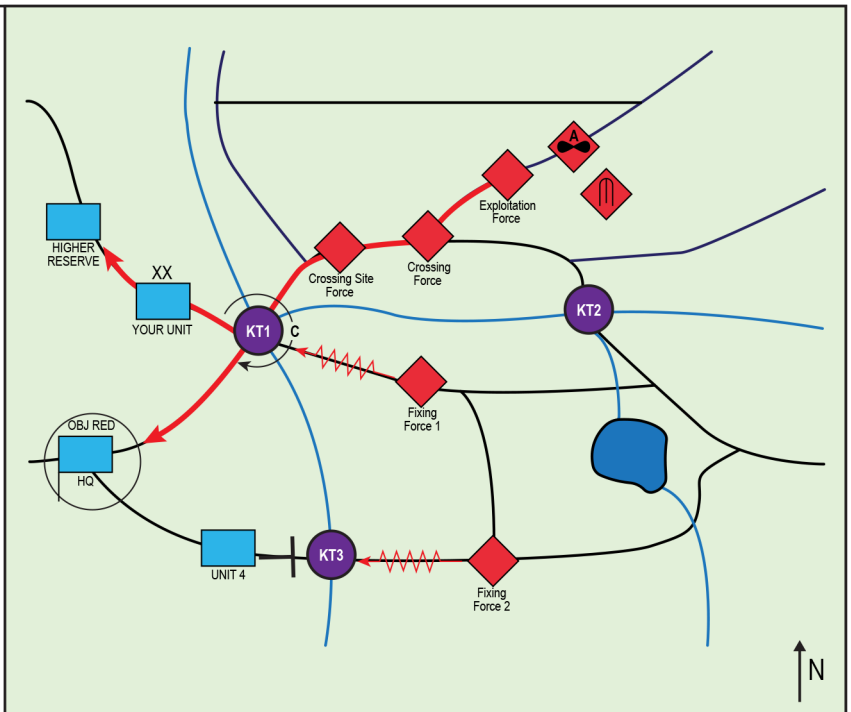
End State:

Enemy: YOUR UNIT is unable to restrict freedom of movement.

Friendly: Enemy forces postured to defeat HIGHER RESERVE and seize OBJ RED.

Terrain: OBJ RED seized and KT 1 infrastructure intact.

LEGEND	
AO	area of operation
ECOA	enemy course of action
HQ	headquarters
KT	key terrain
OBJ	objective
OECOA	operational enemy course of action
TECOA	transition enemy course of action



This figure is a simplified representation of a Success TECOA YOUR UNIT developed at the operational level. Friendly forces withdraw to control KT 1 and retain OBJ RED after being defeated east of the river. In the YOUR UNIT AO, Fixing Force 1 attacks to fix YOUR UNIT at KT 1. Once fixed, the Crossing Site Force attacks to defeat YOUR UNIT to enable the seizure of OBJ RED by the Crossing Force and the destruction of the HIGHER RESERVE by the Exploitation Force. YOUR UNIT designates this ECOA, Success TECOA 2 – FRIENDLY RIVER DEFEAT. The Success TECOA is distinguishable from the OECOA 1– HEAVY NORTH, SOUTHERN FIX, as Enemy Forces can seize OBJ RED and defeat the HIGHER RESERVE offensively.

Figure 8. Success Transition Enemy Course of Action Two: Friendly River Defeat[23]

as the S-2/G-2 explains how, if provided the opportunity and with sufficient remaining combat power, the threat will withdraw (transition) to new defensive positions if defeated at the wet gap and immediately dig in to establish a deliberate defense in as little as 24 to 36 hours. The commander tells the operations officer that the unit cannot allow the enemy to establish a deliberate defense. As a result, the staff designs a detailed sequel that prevents the unit from culminating after the wet gap crossing and disrupts enemy defensive preparations in the unit's deep areas. The proactive friendly plan prevents the enemy from regaining the advantage during execution.

Success transition enemy course of action. The success transition enemy COA (figure 8) describes how the enemy will exploit unanticipated success to achieve its current end state, as described in the operational enemy COA, or a modified end state based on the improved battlefield realities for the threat. Stated another way, the *success* transition enemy COA describes how the threat will *transition* from a state of relative advantage to a situation of *greater* relative advantage to the friendly force.

As with failure transition enemy COAs, success transition enemy COAs are issued with their respective operational enemy COA or critical event enemy COA. They enable the commander and staff to develop failure branches and sequels to mitigate or completely head off the friendly unit's momentary disadvantage (failure) before the threat fully executes its success transition enemy COA.

Consider again the third staff in our failure transition enemy COA wet gap critical event enemy COA. After getting a pat on the back from the commander for their insights on the enemy failure transition enemy COA, the S-2/G-2 asks to brief one more slide. Again, the command and staff listen with great interest to how the threat may commit additional ground, fires, and aviation assets to defeat the wet gap crossing in the unit's AO. The S-2/G-2 then demonstrates how the threat could exploit this opportunity to transition to the offense with the enemy's operational reserve in a follow-and-support role to *defeat* the unit. To mitigate this worst-case scenario, the staff designs a more robust COA with enhanced levels of protection and combat power at the crossing sites, coordinates for higher echelon fires to disrupt the movement of the operational reserve in the AO, and designs a whole new sequel COA that rapidly transitions the unit to a deliberate defense.

Quality transition enemy COAs ensure that a friendly unit can seize opportunities and weather setbacks. The next step is to ensure the team has a collection plan to detect these operational enemy COAs, critical event enemy COAs, and transition enemy COAs.

Priority Intelligence Requirements Development

We know that uncertainty and ambiguity are unavoidable qualities of war.[24] Returning to the wrestler analogy, no wrestler goes into a match believing they know precisely how a contest will play out. Sure, a wrestler has a plan, given what they know about their own and their opponent's strengths and weaknesses, but if their plan is off track, they change

their approach if they want to win. The wrestler expects their opponent to do the same. Notably, some wrestlers may only commit to an initial approach once the match begins, when both opponents first receive cues about what the other might do. However, as a rule, we expect those wrestlers who have planned and prepared for alternate approaches to win more matches.

We can draw three simple points from the wrestling analogy to inform the development of PIRs. First, planning and preparation are essential even in uncertain environments.[25] Second, the uncertain nature of war is partially due to the sometimes unpredictable outcomes resulting from the clash or posturing of forces. We cannot predict with 100 percent accuracy how we or our opponent will react or counteract in a situation. Third, because both sides approach war knowing that they select COAs based on many friendly, enemy, and environmental factors, it would be foolish to assume that our opponent has already determined what they will do from the start. Instead, the enemy may keep their options open for as long as possible. In other words, we cannot tell what COA our opponent will pick with complete certainty from the get-go because the enemy may still need to commit to a decision or may transition to an alternate COA partway through execution. Because forces react unpredictably and can make decisions based on a wait-and-see attitude, units must develop collection plans that constantly scan the environment for multiple enemy COA possibilities. Commanders and staff cannot simply pick one enemy COA and ignore the rest–or they do so at their peril.

Staff must design PIRs to determine what the enemy is doing now (critical event enemy COA), next (transition enemy COA), and within the big picture (operational enemy COA) to reduce the unavoidable uncertainty of war. PIRs ensure units use their scarce collection assets to answer the commander's most important questions.[26] What else would be worth prioritizing our limited collection assets against than determining what COA the enemy is undertaking or will undertake (besides support to targeting to enable our selected COA)? Nothing in my mind.

The description of a PIR offered in FM 3-0, *Operations*, supports this reasoning. FM 3-0 states that PIRs "identify information about the threat and operational environment that a commander considers most important to making decisions in a specific context."[27] Certainly, the set of enemy COAs described in this paper qualifies as requiring friendly decisions!

However, the straightforward process of drafting PIRs to identify which enemy COAs the enemy selects breaks down too often. Many PIRs (even well into execution) often say nothing of enemy COAs at all and instead use generic or unhelpful statements like:

- PIR 1: Where will the enemy employ its reconnaissance?
- PIR 2: Where will the enemy employ its fires?

Knowing where the enemy reconnaissance or fire assets are located is beneficial, but why? Read on.

Let's return to our wet gap crossing example. Recall that our third staff worked through the whole gamut of enemy COAs. The intelligence cell prepared critical event enemy COAs for the threat's anticipated defense: a failure transition enemy COA if the threat could not defeat the friendly crossing operation and had to withdraw, and a success transition enemy COA if the enemy defeated the crossing operation and transitioned to the offense.

To provide support for the commander's decision making, a better set of simplified PIRs for this phase of the friendly operation might look like this:

- PIR 1: Will the enemy conduct an area defense (critical event enemy COA 1) or maneuver defense (critical event enemy COA 2) to oppose a friendly wet gap crossing? Friendly Decision: Execute a COA to defeat the most likely critical event enemy COA 1 option with a contingency option should the threat adopt the second, less likely COA. (This PIR may be broken into two separate requirements).
- PIR 2: Is the enemy transitioning to defensive operations east of the wet gap (failure transition enemy COA)? Friendly Decision: Pursue withdrawing forces and disrupt defensive preparations in depth (success sequel COA).
- PIR 3: Is the enemy transitioning to offensive operations west of the wet gap (success transition enemy COA)? Friendly Decision: Execute a defense west of the wet gap (failure sequel COA).

Instead of looking for reconnaissance or fires assets as the sole purpose of collection as we did in the first sample set of PIRs, these examples focus collection efforts to broadly identify what the enemy is doing (enemy COA). Collection still looks for fires and reconnaissance assets, in addition to other critical systems and activities, but now they serve as indicators to support the assessment of which COA the enemy is executing. Next (or concurrently, if possible), the unit focuses collection via additional PIRs to target assets on the high payoff target list, which enables the execution of the optimized friendly COA. Too often, the tendency is to jump right into targeting without understanding what the enemy is trying to do as a combined arms team, both operationally and tactically.[28] The collection approach represented in the second set of PIRs fixes that.

For any operation, a generic PIR framework that considers the uncertainty inherent to large-scale combat operations would look like figure 9 (on the next page). While seemingly complicated, it has clear advantages over the standard two-and-done enemy COAs often generated at the start of many large-scale combat operations scenarios. Figure 10 (on the next page) suggests how to keep the number of PIRs more manageable throughout an operation's execution.

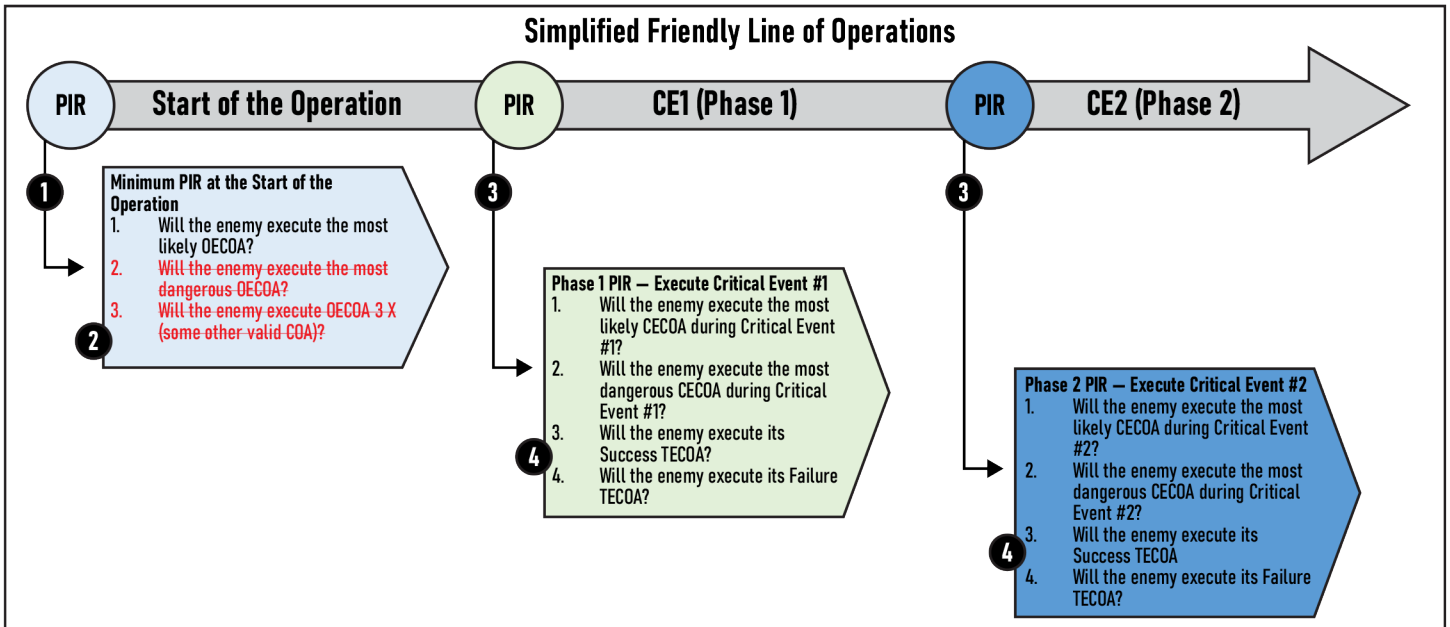
PIR	Most Likely OECOA	Most Dangerous OECOA	Other Valid OECOA
Step 1: Determine the OECOA the enemy will execute			
#1	Will the enemy execute the most likely OECOA—or-	...the most dangerous OECOA —or-	...some other valid OECOA X (as necessary)
Step 2: Determine the CECOAs the enemy will execute nested within each OECOA			
#2-X (X is critical events)	Will the enemy execute the most likely, most dangerous, or other valid CECOA for the most likely OECOA	Will the enemy execute the most likely, most dangerous, or other valid CECOA for the most dangerous OECOA	Will the enemy execute the most likely, most dangerous, or other valid CECOA for all other valid OECOAs
Note: *Some CECOAs may be the same or similar across the Most Likely, Most Dangerous, and other Valid OECOAs*			
Step 3: Determine the TECOAs the enemy will execute at the operational level (OECOA) and by critical event			
#X+1	Will the enemy execute a failure or sequel TECOA during the most likely OECOA	Will the enemy execute a failure or sequel TECOA during the most dangerous OECOA	Will the enemy execute a failure or sequel TECOA during all other valid OECOAs
Note: *S-2 and G-2s should prioritize TECOA development at the operational level (OECOA) and work TECOAs by critical event as they can because the operational TECOA will likely be associated with enemy failure or success at some critical event*			

This figure demonstrates a PIR framework that takes the most likely, most dangerous, and all other valid ECOAs of the three categories into account (OECOA, CECOA, and TECOA). This framework ensures an intelligence cell has considered the complete set of ECOAs available to the threat. Each OECOA will have its unique set of most likely, most dangerous, and other valid CECOAs and TECOAs that may or may not overlap with those of the other OECOAs. S-2s and G-2s must carefully prioritize how much planning and collection resources are devoted to each category and their nested CECOAs and TECOAs while remembering that failing to consider a valid ECOA increases the risk to friendly forces and mission accomplishment.

LEGEND

CECOA	critical event course of action	OECOA	operational enemy course of action	TECOA	transition enemy course of action
ECOA	enemy course of action	PIR	priority intelligence requirement		

Figure 9. Priority Intelligence Requirement Framework[29]



This figure demonstrates how to keep the number of PIRs manageable during an operation by initially focusing on the OECOAs and phasing the PIRs. The minimum PIR set at the operation's start must determine if the enemy will conduct its most likely, most dangerous, or some other valid OECOA **(1)**. The S-2/G-2 scan the environment to determine the OECOA the enemy is likely selecting or is executing. Once the COA is *reasonably* determined, remove the other PIR related to OECOAs **(2)** to include their associated CECOAs and TECOAs (not shown). I say "reasonably determined" because intelligence cells can determine few assessments with 100% confidence due to the uncertainty inherent to war. Therefore, units must devote collection resources to scanning the environment for contradictory information. The S-2/G-2 present their team the CECOAs and TECOAs associated with the selected OECOA (in this example, the most likely OECOA) one phase at a time **(3)**. In the instances above, I correlated each critical event with a single phase, but an actual friendly operation may include more than one critical event per phase. Generally, each phase ends with the enemy executing a Failure or Success TECOA at the tactical or operational level **(4)**. Presenting the CECOAs and TECOAs associated with the selected OECOAs by phase ensures the unit is not overloaded with PIRs.

LEGEND

CE	critical event	COA	course of action	PIR	priority intelligence requirement
CECOA	critical event course of action	OECOA	operational enemy course of action	TECOA	transition enemy course of action

Figure 10. Managing Priority Intelligence Requirements by Phase[30]

Return to the Most Likely and Most Dangerous Enemy Course of Action

How do you position friendly planning efforts against all these enemy COAs? Here is where the most likely and most dangerous labels return to the picture. S-2s and G-2s evaluate and prioritize all valid enemy COAs within the three categories.[31] Prioritization is essential for two reasons. First, as discussed at the beginning of this article, prioritization ensures that most planning time is devoted to developing the most likely and most dangerous enemy COAs when time is limited.[32] Second, prioritization enables the staff to develop a *single* friendly COA "optimized to counter the most likely threat COA, while allowing for contingency options should the threat choose another COA."[33] So, if we do our enemy COA development correctly, we wind up with one very resilient friendly COA with the necessary number of contingency options to account for every valid enemy COA in our three categories over an entire operation. This optimized COA is far preferable to a friendly critical event COA that does not take the big picture into account or an operational COA that lacks the details of the tactical situation, with just a single contingency option to account for the most dangerous enemy COA.

Conclusion

Intelligence cells must commit to determining the complete set of valid enemy COAs to support effective decision making in the uncertain conditions of large-scale combat operations. Drafting operational enemy COAs guarantees we never lose sight of the big picture. Operational enemy COAs serve as the basis for all future COA development. Critical event enemy COAs ensure we execute detailed planning on the areas that matter most. Transition enemy COAs force us to consider what happens next and account for dangerous what-if scenarios. We leverage this understanding, gained during planning, to recover or gain an advantage in every valid situation during execution. The three enemy COAs acknowledge that the enemy *and* friendly have a vote and incorporate this dynamic into their narratives.

The inescapable result of the recommendations in this article is that the staff will make many enemy COAs and friendly branches and sequels. That's okay. Staff need to adopt the view that COA development is never finished. Once the team wrestles with one COA, they move to understand the operational, critical event, and transition enemy COAs tied to the next most likely or most dangerous situation–situations that large-scale combat operations are guaranteed to produce in abundance. As enemy COAs are updated, so are the PIRs prioritizing the unit's limited collection assets to determine which COA the enemy will select.

If all these COAs sound too intimidating, start small. Develop a failure transition enemy COA and a success transition enemy COA to go with the standard most likely and most dangerous enemy COA during the mission analysis brief. Move to critical event enemy COAs and additional permutations of the three enemy COA categories as your commander, staff, and you see the benefits that the three categories bring to planning and execution.

So, grab some red pens. You're going to need them!

Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: U.S. Government Publishing Office [GPO], 1 March 2019), 6-5. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024. (emphasis added).

2. Department of the Army, Field Manual (FM) 5-0, *Planning and Orders Production* (Washington, DC: U.S. GPO, 16 May 2022), 2-1. Please review the discussion cited here for the distinction between warfare's tactical and operational levels.

3. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7.

4. As with friendly courses of action (COAs), valid enemy COAs must be "feasible, acceptable, suitable, distinguishable, and complete." Ibid.

5. Many people from my daily duties and professional military education influenced my thinking for this article. I first gained an appreciation for the value of an enemy COA beyond the standard most likely and most dangerous during Intermediate Level Education at the Command and General Staff Officer Course. The curriculum exposed me to the value of the failure enemy COA. I developed and implemented those ideas as a brigade S-2. In my *Military Intelligence Professional Bulletin (MIPB)* article, "Enemy Course of Action Development," I captured how failure and operational enemy COAs helped my team keep pace in a time-constrained environment during a Joint Readiness Training Center rotation. This article builds upon those ideas along with conversations with my co-workers (notably Majors Kyle Ferguson, Zachary Lawson, Michael Lapadot, Michael Hoffman, and LTC Patrick Vogt) and lessons gleaned from my leadership, principally MG John Meyer's thoughts on transition points, the need for careful development of enemy COA indicators, and the need for detailed (effective) planning to understand the risk to the force and the mission. Of course, all errors are my own. You can access "Enemy Course of Action Development" at https://mipb.army.mil/articles/2020-1qtr/fontaine-15oct2019.

6. Matthew Fontaine, "Enemy Course of Action Development," *MIPB* (October-December 2019): 23-24, https://mipb.army.mil/articles/2020-1qtr/fontaine-15oct2019. I first use the term operational enemy COA in figure 1 of this article. The operational enemy COA's value, paraphrased in the current paper, is initially described in this article's text as the COA belonging to the next higher headquarters.

7. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 75. (emphasis original).

8. Full disclosure—I am not a wrestler. But wrestling dummies exist and are helpful in some situations (much as an operational enemy COA can be!). See Kase Nipe, "Wrestling Dummies in Wrestling: Top Options," Wrestle Love, https://wrestlelove.com/guides/wrestling-dummies-in-wrestling-top-options/.

9. Department of the Army, FM 5-0, *Planning and Orders Production*, 5-51.

10. Ibid., 5-36. The manual states, "each critical event within a proposed COA should be war-gamed."

11. Fontaine, "Enemy Course of Action Development," 24.

12. Adapted from author's original graphic. The figure is a simplified example of figure 6-8. Threat course of action statement example in Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-16.

13. Ibid.

14. Ibid.

15. Ibid.

16. Ibid.

17. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7.

18. Fontaine, "Enemy Course of Action Development," 24. Critical event enemy COAs are akin to the key terrain and population center microanalysis COAs described in my earlier *MIPB* article. I now prefer the term critical event enemy COA better because it encompasses a broader set of situations and includes a friendly plan to consider enemy counteractions at that event. Key terrain is still valuable, as it can be the starting point for the staff to identify critical events.

19. Adapted from author's original graphic.

20. Fontaine, "Enemy Course of Action Development," 24.

21. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 1 October 2022), 1-3. See this reference for a discussion on the term *relative advantage*.

22. Adapted from author's original graphic. The figure is a simplified example of figure 6-8. Threat course of action statement example in Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-16.

23. Ibid.

24. Clausewitz, *On War*, 80, 85.

25. *Public Papers of the Presidents of the United States: Dwight D. Eisenhower, 1957: Containing the Public Messages, Speeches, and Statement of the President, January 1 to December 31, 1957* (Washington, DC: Office of the Federal Register, National Archives and Records Service, General Services Administration, 1958), 818. President Eisenhower recalled this fact during a speech to the National Defense Executive Reserve Conference on November 14, 1957.

26. Department of the Army, FM 2-0, *Intelligence* (Washington, DC: U.S. GPO, October 2023), 6-7.

27. Department of the Army, FM 3-0, *Operations*, 3-9.

28. I benefitted from presentations by COL Blue Huber on the hazards of focusing solely on targeting at the expense of the bigger intelligence picture for this insight.

29. Adapted from author's original graphic, using information from Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7; and Clausewitz, *On War*, 80, 85. See also Department of the Army, Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. GPO, 31 July 2019), 3-7, for a discussion on "exceptional information" as the doctrinal broad category which "contradictory information" would belong to.

30. Ibid.

31. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, 6-7.

32. Ibid. Prioritizing planning time for the various enemy COA permutations is critical to success and requires judgment. Even at the division level with a fully staffed analysis and control element, it is difficult to truly *identify*, let alone *analyze*, each enemy COA available to the threat. In my experience, the teams I have participated in have successfully developed the most likely and most dangerous operational enemy COAs. It has also been possible for us to develop the most essential critical enemy COAs post-mission analysis. During mission analysis, we also successfully promoted the most likely transition enemy COAs for the operational enemy COAs. I share this to inform the reader that executing the ideal framework proposed in this article is no small feat! I am still striving for it. But, keep in mind, every added COA we developed brought value to the unit, and the other extreme alternative, only developing two broad COAs and being done, is far too hazardous for large-scale combat operations.

33. Ibid.

LTC Matthew J. Fontaine is the G-2 for the 1st Infantry Division, Ft. Riley, KS. He previously served as the G-2 for the U.S. Army Joint Modernization Command, Fort Bliss, TX. His deployments include two tours to Iraq and two to Afghanistan, serving as an executive officer, platoon leader, battalion S-2, military intelligence company commander, and analysis and control element chief. He holds two masters of military art and science degrees, one in general studies and the other in operational art and science, from the U.S. Army Command and General Staff College.

Reviewing Current Doctrine

ATP 2-01.3, *Intelligence Preparation of the Operational Environment*, provides current doctrine for conducting intelligence preparation of the operational environment (IPOE). Chapter 6, Step 4—Determine Threat Courses of Action, discusses how step 4 of the IPOE process identifies and describes threat courses of action (COAs) that can influence friendly operations.[1] Outputs from step 4 include situation templates, threat COA statements, event templates, and an event matrix. The following paragraphs are key take aways from the ATP.

During step 4, the intelligence staff identifies and develops possible threat COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat COAs to assist in developing and selecting friendly COAs during COA steps of the MDMP [military decision-making process]. Identifying and developing all valid threat COAs minimizes the potential of surprise to the commander by an unanticipated threat action.

Failure to fully identify and develop all valid threat COAs may lead to development of an information collection strategy that does not provide the information necessary to confirm what COA the threat has taken and may result in friendly forces being surprised and possibly defeated. When needed, the staff should identify all significant civil considerations (this refers to those civil considerations identified as OE [operational environment] significant characteristics) to portray the interrelationship of the threat, friendly forces, and population activities.

The most important element in determining threat COAs is understanding threat operational art and tactics. U.S. forces may encounter regular, irregular, and hybrid threats. The process for determining the COAs these threat forces may employ mirrors friendly COA development and consists of the following:

- Identify likely objectives and the end state.
- Determine threat battlefield functions.
- Determine threat capabilities available to perform each battlefield function.
- Identify the full set of COAs available to the threat.
- Evaluate and prioritize each threat COA.
- Develop each COA in the amount of detail time allows.
- Identify high-value targets for each COA.
- Identify initial collection requirements for each COA.

When determining a threat COA, the intelligence staff accounts for all relevant threat activity, including but not limited to the analysis of the following:

- Current threat situation and mission (includes task and purpose).
- Threat objectives, methods and functions, and end state.
- Commander's intent, purpose, and end state.
- Task organization, capabilities, vulnerabilities, and high-value targets.
- Decision points (essential in determining branches and sequels).
- Decisive points (source of strength, power, and resistance).
- Critical events, branches, and sequels.
- Intent for (includes task, purpose, method, and end state)—
  - Movement and maneuver.
  - Reconnaissance and surveillance.
  - Fires support.
  - Logistics.
  - Threat C2 [command and control].
  - Protection.
  - Information activities.
  - Denial and deception.
- How terrain and weather affect threat operations.
- How civil considerations affect threat operations.
- How displaced civilians and displaced persons affect threat operations.
- How the presence and actions of U.S. forces affect threat operations.

Endnote

1. Department of the Army, Army Techniques Publication 2-01.3, *Intelligence Preparation of the Operational Environment* (Washington, DC: Government Publishing Office, 1 March 2019), 6-1–6-24. Change 1 was issued on 6 January 2021. Change 2 was issued on 23 January 2024.