# Need Authorities For The Gray Zone?

## Stop Whining. Instead, Help Yourself to Title 100. Hell, Take Some Title 200 While You're At It

BY JAMES Q. ROBERTS

As we strive to confront enemies operating in the Gray Zone—the fog-filled twilight zone between war and peace, where state and non-state actors employ threats, coercion, cooption, espionage, sabotage, political and economic pressure, propaganda, cyber tools, clandestine techniques, deniability, the threat of the use of force, and the use of force to advance their political and military agendas—U.S. Department of Defense (DOD) forces are often frustrated by a lack of authorities to act. Short of war and beyond the parameters set by the 2001 Congressional "Authorization for the Use of Military Force" (AUMF) we may judge our Title 10 authorities[1] inadequate to the task, or at best a remarkably poor fit.

This article encourages U.S. special operations forces (SOF), and other DOD elements, that are seeking to contain, parry, or otherwise respond to Gray Zone threats to take full advantage of the authorities that do exist within the United States Code. By smartly leveraging the authorities that the special operations community and our interagency partners do have, the United States can, in fact, do a lot.

But to do so will require imagination, vision, stamina, salesmanship, guile and a keen understanding of our interagency partners, their cultures, authorities, and prejudices. Sounds like an environment and a task ready made for special forces types!

*James Q. Roberts is a part-time subject matter expert at the College of International Security Affairs, National Defense University. A 1970 graduate of the U.S. Army Special Forces Qualification Course, Mr. Roberts has spent 46 years—in both military and civilians capacities—seeking to advance Special Operations authorities and capabilities*

## Finding Title 100

A close follower of U.S. Code might be saying, "What do you mean? There is no Title 100 in the U.S. Code!" Not to worry, here is how you find this elusive tool box. As a SOF Gray Zone warrior you arrive (more often than not at the U.S. embassy) with a rucksack full of Title 10 authorities. These include the ability to engage with partners, and under most circumstances, to build their capabilities for special operations, combating terrorism, and general ministry of defense management. In some instances, they include execute orders that allow SOF to advise and assist partners in operations, subject to some peacetime (and interagency) constraints. In all cases, they include the right to self-defense, and the defense of U.S. interests when under direct attack.

But Title 10 is not "Title 100:" a powerful combination of authorities attained by blending the authorities of interagency partners. You may love them or you may hate them, but your Central Intelligence Agency brothers and sisters in the Station have a large basket of Title 50 authorities[2] that can be brought to bear on many Gray Zone phenomena. These include intelligence collection activities as well as authorities for equipping, training, engaging, advising, and conducting operational actions with partner intelligence, military, and security forces. So far so good—if we can just get along with the Station, we can employ, or help them employ, Title 50.[3]

Both SOF and the Station are beholden to the Chief of Mission (COM), usually an Ambassador, sometimes, a Charge d'Affaires. Either way, the COM reigns supreme in peacetime, empowered as the President's direct representative to the host nation, and per the Letter of Instructions to Posts, signed by the President, in charge of all U. S. Government (USG) activities, other than "those under the command of an area military commander."[4] He or she is also empowered by Title 22, which governs the Department of State (DOS) and describes USG diplomatic responsibilities. These include the management of diplomacy, but also an overarching responsibility for the entirety of the U.S. relationship with the host government in all its dimensions. Continuing our mathematical approach, SOF and the interagency team can now employ Title 72 (Title 50 plus Title 22), with a lot of good will and huge doses of the requisite schmoozing.

Finally, many County Teams today have a representative from the Justice Department or the Federal Bureau of Investigation, usually known as the Legal Attaché (Legatt), assigned to the Embassy. He or she is there to execute federal law enforcement activities under the guidance provided in Title 28.[5] The Legatt interfaces with the host nation Ministry of Interior and various other security forces, on liaison matters for U.S. law enforcement purposes. But they may also provide training and assistance to host nation law enforcement units and agencies. These activities are also fully coordinated (in theory) with the country team and approved by the Ambassador. Title 72 plus Title 28 from the Legatt gets us to Title 100. Be ready to repeat the requisite schmoozing throughout this stage as well.

I can hear all the naysayers already. "Will never happen!" "Too many people can say 'no,' while almost no one can say 'yes.'" "The agency cultures are too different to permit constructive interaction." "Who pays?" "Who is in charge?" On and on. I've heard it all. Please stay calm and listen (or read) for a few more minutes.

Despite the above complaints and many others (which we must not neglect), there have been instances (outside of war zones) where under the overarching leadership of an Ambassador a group of players from State, Special Operations Task Forces, the Intelligence Community (IC) and federal law enforcement have been able to get their acts together to employ Title 100 in the Gray Zone. In some instances, they have leveraged Title 110 by employing SOF's Title 10 alongside the other authorities. Their successful orchestration has been of great benefit to each other, the President, the USG, and our ultimate stakeholders, the U.S. taxpayers. The partner nations have benefited greatly as well.

The three cases that come to mind most readily are the successful captures of three terrorists in Africa; two in North Africa and one in transit, off the coast of Somalia. In each instance, the USG, at times working closely with partner forces and governments, was able to mix and match its authorities to successfully find, track, and capture important terrorists. The first case was the capture of Ahmed Abdulkadir Warsame in international waters en route from Yemen to Somalia.[6] The second was the capture of Abu Anas al-Libi in Libya.[7] The third was the capture of Ahmed Abu Khatallah, also in Libya.[8] In these examples, each target was a terrorist who fit within the parameters of the Authorization for Use of Military Force (AUMF). At different stages of each operation, the IC, SOF, the Department of State (DOS), and the FBI each played key, leading roles. But in none of these cases was the end result a SOF kill, or any agency's kill, for that matter. For each case, the end state was a prosecution in U.S. Federal Court, back in the United States. In the al-Libi case there was an outstanding indictment prior to the initiation of the operation; in the Warsame and Abu Khatallah cases, the suspects self-incriminated during questioning, after capture.

Although these successes were all against terrorist targets, the distributed and shifting roles within the country team, as different combinations brought various aspects of the combined authorities to bear, is what we should focus on. But first, a short review of a methodology that serves us extremely well for combating terrorism, but which I believe can (and must) be adapted for use against all manner of malign actors in the Gray Zone.

## Catching Bad Guys with F3EAD

Over the past 15 years we have developed and refined a targeting methodology now known as Find, Fix, Finish, Exploit, Analyze, and Disseminate. Of course, this wordy compilation just screams to become an acronym. And, of course, the acronym-enamored DOD has obliged: F3EAD has entered our lexicon.

As a result of our experiences in Afghanistan, and Iraq, and smaller more discreet efforts elsewhere, many within the interagency counterterrorism community (and beyond) have become adroit at implementing this targeting cycle. The cycle itself stresses the requirement to blend USG authorities, particularly outside of war zones. I will argue that it should not remain principally a counterterrorism skill set, but instead, could be used to address all manner of threats in the Gray Zone. We can envisage ways to combat both state sponsored and nonstate actor malign, illegal, and often clandestine enterprises using the F3EAD methodology, in close cooperation with our partners.

"Find" refers to the initial geographical locating of the target. "Fix" is the more intimate and timely locating and tracking of the

target, designed to eventually enable the next step. "Finish" can come in two forms; capture or kill. The former is far preferable to the latter, since the next phase is greatly enabled by capture options, and directly feeds the last two steps. "Exploit" refers to both the individual captured and all of the documents, electronics, and materials that may be captured with him. "Analyze" is the task of assessing and cross referencing all of the captured information, and placing it in context with the rest of what is known about the targeted individual, group, network, movement, or enterprise. Finally, "Disseminate" refers to making the analysis and raw information available back to the user and intelligence communities, with the view toward enabling a return to Phase One—to reset the cycle forward to another "Find."

To clarify, let me illuminate each phase a bit. The essential concept is that each phase (and each scenario) will require a tailored blending of the complement of authorities, with interagency roles and responsibilities adjusting accordingly.

As we further dissect the targeting cycle, we can see that the Find phase relies heavily on the intelligence community. The IC will leverage all source collection and analysis to scope the problem and locate the target. Bringing the U.S. intelligence and, in some cases, law enforcement information together into a seamless, cohesive whole is the first step in this task. Working with the partner in such a way as to leverage its information on the same subject is the second step.

For the Fix phase, the blend of authorities may shift. Some combination of IC resources, often augmented with or enabled by SOF, needs to get closer to the target and begin a pattern of direct observation and collection, including through technical means, that enables the development of the "pattern of life" of the target. Understanding the details of how the target is living and moving on a daily—and in some instances, on an hourly basis—allows for further assessment of his or her vulnerabilities and establishes the parameters of the options for the Finish phase. Of course, during this phase, operational security is perhaps the essential consideration for U.S. and host nation forces as secrecy is required to achieve the requisite surprise.

For the Finish phase the blend of authorities and capabilities will likely shift again. Since the Finish usually moves from a clandestine collection and observation phase to a direct action raid for the capture of the target, the role for SOF will likely increase, while the assets of the Fix phase maintain "eyes on target." For the Finish, if the goal of the operation is capture and extradition to the Unites States for trial, then incorporating some Title 28 resources into the capture phase is advisable, in order to maintain a legally sufficient "chain of custody" of the individual and any assets seized during his or her capture. Keeping the Title 28 players in the mix for movement back to the United States is also crucial to ensuring that no missteps occur along the way that might give defense attorneys an opening to sew doubt during any eventual trial.

The Exploitation phase usually involves most of the Title 100 (and Title 10) team, often dependent on language skills, technical expertise, an understanding of how this target fits into the rest of the malign organization, and the requirement to ensure proper chain of custody for those informational components crucial to a successful prosecution. Depending on the skills of the partner forces, they may also be extensively involved.

Analysis is definitely a broad effort, with some being done in the field by the Title 100 team on site, but much of it being done downstream by headquarters intelligence analysis staffs back at the various agency home offices. This phase of the effort may go on for months or years, depending on the scope and content of the sensitive information and equipment collected. If the partner has an analytic capacity, it may be fully engaged during this effort.

Finally, the Disseminate phase is also a broad effort. The initial outputs will come from the team in the field, but reports from the various intelligence and headquarters staffs involved may continue to publish finished intelligence long after the close of the operation. Again, heavy partner and international cooperation can be expected.

The key takeaway is that a skilled orchestration of the authorities and capabilities of the diplomatic, intelligence, military, and law enforcement tools resulted in impressive results against illegal, clandestine, dangerous Gray Zone targets. I contend that the same can be done against non-terrorist elements as well. It will just take a little more Special Operations "magic dust."

## A DIME is Not Enough

For Gray Zone threats there are a few other core considerations that should go into our recipe for success. First, the traditional diplomatic, informational, military, and economic description of the elements of national power (known as DIME) is too narrow. At a minimum we should expand our toolkit to include financial, intelligence, and law enforcement (FIL) capabilities. If we combine these two, we have the somewhat cumbersome acronym of DIMEFIL.

A few years ago, I was frustrated with this acronym, and asked one of my action officers to develop a less clumsy and more easily remembered term. He was a typical SOF Major, in the middle of a divorce and attempting to stay alive in the expensive Washington environment. He was back in 20 minutes with a new phrase: MIDLIFE. This has the advantage, and disadvantage at the same time, of listing the Military tool first—making it easier for DOD types to remember, but upsetting the diplomats and associated DIME traditionalists.

Its real disadvantage is that it can imply that these Gray Zone malign actors can be best confronted by military means—a perception to be absolutely avoided at all costs. Nevertheless, I prefer MIDLIFE to DIMEFIL and enjoy seeing MIDLIFE appear in national security papers or talks from time to time.

## The Environment is VUCA, at the Very Least

In addition to MIDLIFE, there is another War College acronym that is helpful to keep in mind as we asses this fog-filled Gray Zone environment. Many contend that the national security environment of today and tomorrow is increasingly volatile, uncertain, complex, and ambiguous. This gives us VUCA, with each of these characteristics playing off of the others to make assessment of a given situation more difficult, and placing decisionmakers in a space where it is becoming more the norm that a decision must be taken, absent all (or even most) of the information that the decisionmaker would like to have before deciding.

Recently, a senior leader speaking at the National Defense University, referred to this phenomenon by saying that the only way to cope is to "become comfortable with being uncomfortable."[9] Given Gray Zone opponents'

inclination to leverage unexpected capabilities and to see asymmetric advantage where we see status quo, VUCA thinking should definitely permeate our approach.

So, an appreciation of the VUCA environment and a well-developed set of MIDLIFE tools are additional core requirements as we prepare to go beyond combating terrorism with our interagency Title 100 or Title 110 enterprise. But, there is another major challenge for the special operator deploying to a "peacetime" embassy.

## You are not in Charge? So What. You can Still Make it Work.

The warrior diplomat, deployed to an embassy, will find himself (or herself) in an environment in which he has minimal authority, even over his own team. He certainly has no authority over the interagency group he is trying to influence; thus his task is to try to achieve unity of effort in the absence of unity of command. His first step is to scan the internal and external environments to determine the formal and (more importantly) informal power structures present in the country team. Who has access to whom? And who are the trusted (and despised) players in the zoo? Who actually makes the decisions and controls the game? Does anyone already understand Title 100, or Title 110? Can you partner with them?

As a SOF guy or gal you will need every ounce of your warrior diplomat skill set—to interact with the country team, before you ever get to say "Hi!" to a partner nation leader. You thought you were deploying to be a warfighter? Think again! Your real mission is to read and assess, to coopt and cajole, and generally curry favor with your embassy teammates to build a consensus about the Gray Zone and how to proceed therein.

Understanding that your most important role is to develop and nurture key relationships with the other interagency players on the country team is essential. Your task is to build a Title 110 cabal in their midst, where you are not in charge, but where you do have a major shaping voice in the way forward. Your goal is to have the ambassador (or his trusted agent) come to believe that this team, and the processes it will use, was his (or her) own brilliant idea.

This is political and informational warfare at the grass roots level. You have the necessary skills, but this work will require you to refocus them in an unending effort to build "coalitions of the willing and the able" to advance your agenda in the face of constant risk aversion, naysaying, and bureaucratic push back. Indirectly influencing those who you do not command, (and over whom you have but limited sway) should appeal to your core competencies as SOF. After all, for you Green Berets, when you first met your Robin Sage Guerilla Chief, you were in the same boat.[10]

Heretofore, you have lived (and thrived) in a relative meritocracy—work hard, be skilled, keep your eyes open and your mouth shut, be the best, play fair, and the "system" will reward you with prestige, promotions, and increased responsibilities. When you move into the interagency authorities game, you will leave the meritocracy and enter the "politocracy"—where your merit remains important, but will be neither adequate nor determinant.

Your political skills—including the ability to listen (not to respond quickly, but to actually understand), to know and cope with the cultures of the other agencies, and to mask your anger and frustration in pursuit of consensus—will be key to your success. Most of your gains will come by negotiating, not