

Need Authorities For The Gray Zone?

Stop Whining. Instead, Help Yourself to Title 10. 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, cooperation, 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 authorities¹ 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 authorities² 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 inter-agency 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 United 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 sow 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 assess 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

directing. In those negotiations, you will often be a junior partner, or a bit player. In this environment, it is all about building and maintaining your credibility as a reliable and self-effacing player. You will need to check your ego (and, in all likelihood, your weapons) at the door, and recognize that the special operations culture from which you come is all too often viewed with skepticism and suspicion, rather than the awe and deference you have come to believe it deserves.

You will be working to shape decisions which you can't direct. This requires a soft touch and finesse, high emotional intelligence, excellent body language reading skills, and an ability to create trust and good will at a table where you usually have been dealt a pretty weak hand in terms of the actual resources you can offer, and the power of your position. But

let's be positive and assume that you have built a consensus for action in the Embassy and that the country team is prepared to orchestrate the use of each other's authorities and resources to go after Gray Zone bad guys. You will have mastered the orchestration of Title 100, added Title 10 to the mix, and built your skills in the "politocracy" of the U.S. Government.

How can we use Title 100 Against Bad Guys who are not Terrorists?

Let's consider how we can leverage this process to go after Gray Zone threats (other than AUMF-able terrorists) that threaten partner nations. The concept is to employ the partner's equivalent of Title 100—in other words, guide the partner to orchestrate its own authorities. Although many of our partners talk a good "whole of government" game, when it comes



SFC Anthony L. Taylor, U.S. Army

Special Operations Forces and civilian and military leaders from the United States and European and African nations meet to discuss military cooperation, an example of Title 200 authority.

to operationalizing their authorities, they face many of the same challenges that we do. Among these are jealousies about prestige and resources, divided authorities within their constitution or political landscape, and preferences of the political leadership. Additionally, there are often tribal or family alignments along agency lines, regional divisions, and other unhelpful groupings within military, police, security, intelligence, and other security organizations. Finally, graft and corruption may undermine government competence and legitimacy across the board.

Scanning the partner's authorities as well as the assignment of roles and missions across its interagency landscape is essential to understanding what is within the realm of the possible. This review will also help guide our capacity- and capability-building efforts, and will enable us to guide the partner in use of its own "Title 100." The combination of our "100" plus the partner's "100" gives us the Title 200 concept.

Title 200? I was Still Struggling with 100.

To leverage Title 200, the SOF element, in cooperation with its USG partners, must develop an in-depth understanding of the distribution of authorities across the partner's intergovernmental bureaucratic and legal structures. Once this understanding has been mapped and assessed, the USG interagency team can help the partner—element by element, and in combinations—to apply the F3EAD targeting process to the malign actors threatening the partner's sovereignty.

Right off the bat, you can see this will clearly require a deep understanding of both the threats the partner faces, and the legal code under which it operates. Of course,

accomplishing this will take time, access, and expertise—bound together with excellent bilateral trust between the USG and the partner ministries and institutions. In addition, an in-depth assessment of the partner nation's legal framework and specific codes will be required so as to assess what enemy actions are already illegal, and which could be made illegal.

By employing Title 200, we may be able to overcome many of the constraints that limit our ability to act directly on our own against Gray Zone non-terrorist threats. We must recognize that in most cases, these threats will not rise to a level where the United States has the legal authorities to intercede, much less invoke war fighting authorities.

It is also true that in the majority of state actor cases, the United States will have a wide array of competing interests with that state sponsor. Many of these will be of greater strategic importance to the overall relationship than the hard to prove, non-attributable nasty games the sponsor is conducting against the partner in the Gray Zone. In such cases, gaining Washington's approval for a direct U.S. response is highly unlikely.

However, there is a good possibility that some aspect of the malign Gray Zone actor's activities will constitute a local crime. Thus, they could be arrested by host nation security or law enforcement authorities, imprisoned, and tried for these offenses. On the other hand, there will be cases for which the partner may also lack the authorities necessary to interdict the Gray Zone malign activities. In this event, the advisors should recommend subtle, but important enabling legal changes that will criminalize the actions of the Gray Zone threat actors, without undermining basic civil protections and human rights.

Gray Zone malign activities executed by enemy state or nonstate actors can create great instability, political or economic turmoil, paramilitary or inter-tribal violence, or other direct and indirect pressures which seek to undermine the credibility, legitimacy, and ability of the partner nation to govern.

When the malign conduct does not constitute a crime in the partner's existing legal framework, I recommend that the Legatt (and, when necessary, Department of Justice experts) review the legal code of the host nation and carefully advise host nation officials on how to criminalize key aspects of the malign actor's conduct. Through this process, the host nation law enforcement apparatus can then arrest the malign actors for their criminal activity—and curtail their Gray Zone actions.

In some cases, the criminal activity may not rise to the level of a national security threat. For these, we might recommend to the partner that they take a page from the U.S. experience dealing with the mafia and other organized crime syndicates. Partner law enforcement can charge the bad actors with lesser crimes, much like the actions many U.S. jurisdictions have taken to prosecute organized crime enterprises by initially charging crime bosses with “no visible means of support,” then “discovering” their huge tax evasion schemes, and finally convicting them of tax evasion and/or tax fraud, as was the case with Al Capone.¹¹

This indirect approach in many instances has added benefits. It may outflank the political support or protection that the criminal organization may have built within the host nation's governmental structure, or key leadership. It also avoids the challenges of trying to prove a more complex or serious set of criminal activities.

Using the local law enforcement approach has many advantages. First, many of the Title 100 agencies in the Embassy have training and equipping capacity-building authorities that can be used to strengthen both the host nation unit's capabilities, as well as its backbone. Next as we employ the F3EAD model, we can share intelligence and law enforcement information to help the partner with the Find and the Fix stages. Employing various “advise and assist” authorities, USG Title 100 players can frame, shape, and guide the partner's Finish operation. After the Finish, the partner and the United States can leverage the “take” from the target, including his records and electronic media, to close out the cycle with joint Exploitation, Analysis, and Dissemination.

A second advantage of this approach is that it empowers the partner to re-establish governance on his own territory, using his own authorities. If the United States were conducting these operations in lieu of the partner, the partner government would be open to charges from Gray Zone (and other) opponents that the government is incapable of governing, has sold out to the Americans, and therefore is illegitimate and unworthy of popular support.

However, none of these accusations apply when the partner is enforcing its own laws, on its own territory, with its own forces. In fact, its legitimacy is likely to increase as a result of its directly confronting the enemy shadow forces. Its population may, in fact, applaud government efforts to rid them of the nefarious malign actor pressure.

In these endeavors, as in many others with partners, we would be wise to heed the following words from T.E. Lawrence: “Do not try to do too much with your own hands. Better the Arabs do it tolerably than that you do it

perfectly. It is their war, and you are here to help them, not to win it for them."¹²

So, help the partner understand the threat and develop the wherewithal to confront it on its own terms. Effectively leveraging the partner's authorities (and our own) to ensnare and prosecute Gray Zone criminals is core work for 21st century SOF.

In many ways, we should consider this the new approach to Foreign Internal Defense (FID). Whereas the original FID doctrine was developed to confront Soviet encroachment on partner sovereignty, we may be able to reformat the concept and employ the orchestrated authorities of Titles "100" and "200" to address the threats Gray Zone enemies present to our partners today.

The bottom line is please stop whining about inadequate authorities and start schmoozing our interagency and international partners to better leverage the authorities we do have. It is all about building relationships. You will need to build consensus inside the USG country team, and with host nation partner agencies. If you can bring your team (and your authorities) together with their team (and their authorities) into a cohesive and coherent whole of government campaign, you (and more importantly they) can go after Gray Zone threats with persistence and vigor.

The first step is to increase costs to Gray Zone adversaries and their sponsors by arresting key actors and successfully prosecuting them. Secondly, holding a public trial will expose both the criminals and their state sponsors to the light of international scrutiny and broad condemnation. At trial, some of the arrested operatives will incriminate their state sponsor bosses, particularly when they seek lesser penalties during sentencing. Additionally, some of the testimony may

permit charges against sponsoring government officials, either in national or international venues such as the International Criminal Court.

Finally, such an approach strengthens the partner nation's legitimacy by enabling it to demonstrate to its population, and to the world, that it is capable of coherent action in defense of its nation, even when the enemy is hiding his operations in the shadows of the Gray Zone.

Because of the United States' conventional (and nuclear) military overmatch against any near peer competitor for the foreseeable future it is likely that state competitors will continue to employ and refine their non-attributable Gray Zone capabilities for the next several decades. Malign nonstate actor enterprises will do the same. So far, democratic governments and their partners have not found good countermeasures to these illegal, clandestine methods that undercut legitimacy and create opportunities for their sponsors, while avoiding the imposition of costs that would likely be instituted, were the sponsoring government to attempt to conduct the same activity overtly.

This article describes some initial actions that could be taken today by the United States and our allies and partners to start imposing costs against a variety of malign actors exploiting Gray Zone shadows and ambiguity to their advantage. I have argued that we can make our current authorities work, despite the various challenges that our interagency processes and funding mechanisms present.

Nevertheless, I encourage the U.S. national security community to continue to pursue new, more flexible authorities at the same time. We need more flexible authorities and funding mechanisms to defeat Gray Zone threats. The measures I recommend in this

article allow us to accomplish some of what is needed today. However, as enemy actors evolve further, and hone their Gray Zone doctrines, our interagency national security mechanisms will continue to require longer term, flexible, and rapidly adaptable authorities and capabilities. **PRISM**

Notes

¹ Title 10 of the U.S. Code establishes the authorities of the Department of Defense, outlining the role, mission, and organizational structure of the U.S. military under the authority, direction, and control of the Secretary of Defense. Title 10 is organized into five subtitles, which include provisions on force structure, personnel, training, education, service, supply, and procurement.

² Title 50 of the U.S. Code outlines the procedures governing “War and National Defense,” describing how the United States declares and conducts war. Within its 43 chapters, Title 50 discusses intelligence operations, espionage, military equipment and assets, emergency powers, and other defense-related issues. Title 50 is primarily known for the powers it confers to the Intelligence Community through the Director of National Intelligence.

³ In covert missions and special operations, there is continuous conflict between Title 10 (the Department of Defense) and Title 50 (the Intelligence Community). For more information on the debate between Title 10 and Title 50, see: Andru E. Wall, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” 2011, <<http://www.soc.mil/528th/PDFs/Title10Title50.pdf>>.

⁴ United States Code: Title 22, Section 4865, *Security Requirements for the United States diplomatic facilities*, <[http://uscode.house.gov/view.xhtml?req=\(title:22%20section:4865%20edition:prelim\)](http://uscode.house.gov/view.xhtml?req=(title:22%20section:4865%20edition:prelim))>.

⁵ Title 28 of the U.S. Code establishes the authorities of the Department of Justice (including the FBI) and outlines the organization of the courts, the procedures of the U.S. legal system, and the responsibilities of court officers and employees.

⁶ Karen DeYoung, Greg Miller, and Greg Jaffe, “U.S. indicts Somali on terrorism charges,” *Washington Post*, July 5, 2011, <https://www.washingtonpost.com/national/national-security/us-indicts-somali-on-terrorism-charges/2011/07/05/gHQA-8bbfzH_story.html>.

⁷ Ernesto Londoño, “Alleged al-Qaeda operative captured in Libya was among terrorist organization’s early elite,” *Washington Post*, October 7, 2013, <<https://www.washingtonpost.com/world/national-security/alleged-al-qaeda-operative-captured-in-libya-was->

among-terrorist-organizations-early-elite/2013/10/07/386340dc-2f83-11e3-8906-3daa2bcde110_story.html>.

⁸ In a press release, President Obama stated, "The fact that he [Ahmed Abu Khatallah] is now in U.S. custody is a testament to the painstaking efforts of our military, law enforcement, and intelligence personnel." This statement is a testament to the effectiveness of interagency cooperation. For the full text, see: "Statement by the President on the Apprehension of Ahmed Abu Khatallah," The White House, June 17, 2014, <<https://www.whitehouse.gov/the-press-office/2014/06/17/statement-president-apprehension-ahmed-abu-khatallah>>.

⁹ General officer speaking not for attribution at the National Defense University in January 2016.

¹⁰ Robin Sage is the end of course exercise for Green Berets that focuses on unconventional warfare. During the exercise, the Green Berets meet with a "local guerilla chief" who usually asks them something along the lines of, "Why don't I just kill you and your team, and take your guns and money now?"

¹¹ A document released by the FBI stated, "In the end, it took a team of federal, state, and local authorities to end Capone's reign as underworld boss. Precisely the kind of partnerships that are needed today as well to defeat dangerous criminals and terrorists." For the full document, see: "How the Law Finally Caught Up With Al Capone," Federal Bureau of Investigation, March, 28, 2005, <https://archives.fbi.gov/archives/news/stories/2005/march/capone_032805>.

¹² T.E. Lawrence, "The Evolution of A Revolt," Combat Studies Institute, reproduced on December 4, 2000, available at <<http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/lawrence.pdf>>.