The national and military strategies of the United States explicitly outline a strategic requirement for unified action to combat networked VEOs. Despite this strategic imperative, neither the U.S. military nor its “interagency” partners are adequately structured, resourced, or empowered to effectively conduct such operations. The concept of using SOF as a global CT network, captured in this paper under the label of “Global Pursuit” operations, addresses the incoherence of current U.S. CT efforts. To effectively conduct Global Pursuit operations, SOF must be armed with standing authorities and a streamlined approval process, and adopt a series of organizational changes. The result of these actions should allow SOF to lead a U.S. CT network capable of achieving “network overmatch” against globally networked VEOs.

**15. SUBJECT TERMS**

Special Operations Forces (SOF), Violent Extremist Organizations (VEO), counter-terrorism (CT), Global Pursuit
FUTURE WAR PAPER

TITLE:
Global Pursuit: Employing Special Operations Forces as a Counter-Terrorism Network

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

AUTHOR:
Major Mason Dula

AY 2011-12

Mentor: Dr. Wray Johnson

Approved: [Signature]

Date: 17 May 2012
DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.
Executive Summary

Title: Global Pursuit: Employing Special Operations Forces as a Counter-Terrorism Network

Author: Major Mason R. Dula, United States Air Force

Thesis: Employing U.S. Special Operations Forces (SOF) as a global counter-terrorism (CT) network has the potential to address the United States’ strategic requirement to “Disrupt, Dismantle, and Defeat” networked violent extremist organizations (VEOs), but would entail strategic risk and require broadened authorities, streamlined approvals, and structural changes to existing SOF organizations.

Discussion: The national and military strategies of the United States explicitly outline a strategic requirement for unified action to combat networked VEOs. Despite this strategic imperative, neither the U.S. military nor its “interagency” partners are adequately structured, resourced, or empowered to effectively conduct such operations. The concept of using SOF as a global CT network, captured in this paper under the label of “Global Pursuit” operations, addresses the incoherence of current U.S. CT efforts. To effectively conduct Global Pursuit operations, SOF must be armed with standing authorities and a streamlined approval process, and adopt a series of organizational changes. The result of these actions should allow SOF to lead a U.S. CT network capable of achieving “network overmatch” against globally networked VEOs.

Conclusion: Despite significant risks associated with adopting a counter-network strategy to combat VEOs, the use of SOF as a global CT network offers tangible benefits, at reasonable costs.
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISCLAIMER</td>
<td>i</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>ii</td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>iii</td>
</tr>
<tr>
<td>STRATEGIC REQUIREMENTS</td>
<td>1</td>
</tr>
<tr>
<td>CURRENT U.S. STRATEGY</td>
<td>3</td>
</tr>
<tr>
<td>EXISTING U.S. CAPABILITIES</td>
<td>4</td>
</tr>
<tr>
<td>GLOBAL PURSUIT</td>
<td>8</td>
</tr>
<tr>
<td>SPECIAL OPERATIONS FORCES (SOF) AS A GLOBAL COUNTERTERRORISM (CT) NETWORK</td>
<td>9</td>
</tr>
<tr>
<td>SOF AUTHORITIES IN THE “DIRECT” APPROACH</td>
<td>9</td>
</tr>
<tr>
<td>SOF APPROVALS IN THE “DIRECT” APPROACH</td>
<td>11</td>
</tr>
<tr>
<td>AN ARCHITECTURE FOR SOF-LED GLOBAL CT OPERATIONS</td>
<td>12</td>
</tr>
<tr>
<td>WORKS CITED</td>
<td>17</td>
</tr>
</tbody>
</table>
Shakespeare observed that "as many ways meet in one town, as many fresh streams meet in one salt sea, as many lines close in the dial's center, so may a thousand actions, once afoot, end in one purpose, and all be well borne without defeat." In confronting the challenge of global terrorism, the United States musters a host of often disjointed responses. Frequently lumped together under optimistic banners such as "whole-of-nation approaches," these attempts to counter violent extremist organizations (VEOs) tend to reflect the bureaucracies from which they hatched, rather than the common purpose ostensibly calling them into being. Despite a widely accepted strategic imperative to disrupt global terrorism and defeat the VEOs that employ terror as a tactic, the United States lacks unity of effort in its counter-terrorism (CT) efforts. Employing U.S. Special Operations Forces (SOF) as a global CT network has the potential to address the United States' strategic requirement to "Disrupt, Dismantle, and Defeat" networked VEOs, but would entail strategic risk and require broadened authorities, streamlined approvals, and structural changes to existing SOF organizations.

**Strategic Requirements**

The national and military strategies of the United States explicitly outline a strategic requirement for unified action to combat networked VEOs, both in today's security environment and in the future. The 2010 National Security Strategy (NSS) identifies security as one of four national interests, and includes the implementation of a multi-faceted and integrated campaign to counter VEOs under this rubric. The 2011 National Military Strategy lists "Counter[ing] Violent Extremism" as one of four National Military Objectives, elevating efforts to combat VEOs to the same level of importance as winning the nation's wars. In 2011, the United States released a National Strategy for Counterterrorism (NSCT), ostensibly an extension of the current NSS and not a radical restructuring of national security priorities. The NSCT acknowledges the
existence of multiple VEOs whose ideology and activities threaten U.S. interests, but deliberately focuses on the Al Qaeda network, its affiliates, and its adherents. Strategic intelligence estimates on future threats predict the continued use of irregular warfare and terror tactics by both state and non-state actors through the next decade and beyond. Whether deliberately focused on individual VEOs, or considering the challenge of defeating such organizations holistically, U.S. strategy clearly identifies effective efforts to counter VEOs as a national requirement.

While differing in scope and specificity, these attempts to codify U.S. CT strategy share a common vision of contemporary threats. National strategy identifies a networked organization, rather than hierarchal variants, as a defining characteristic of contemporary VEOs. The NSS alone uses variations of the term “network” over 25 times in describing both the nature of the VEO threat, and proposed U.S. responses. The NMS discusses the role of global illicit trafficking networks as an emerging source of VEO recruitment and funding. U.S. Joint doctrine for CT operations examines the cellular organization of networked VEOs in an attempt to identify exploitable vulnerabilities.

This notion of viewing globally active VEOs as networked “systems,” or even complex and evolving enemy “ecosystems,” anchors attempts by strategy and policy-makers to create a shared understanding of the nature of contemporary threats. A network-centric view of contemporary VEOs is therefore the dominant narrative informing strategic requirements, and debating the merits of such a paradigm lies beyond the scope of this paper. Regardless of the concept’s validity, the description of VEOs as networked entities in strategic literature and joint doctrine inform the creation of global CT strategies. The implications of viewing networked
VEOs as the primary CT threat facing the U.S. are best illuminated by examining the military aspects of current U.S. CT strategies.

**Current U.S. Strategy**

Contemporary U.S. strategy envisions a strategic campaign to create a "stabilized global environment" resistant to the actions and ideologies of VEOs. This campaign focuses on both enemy networks themselves and U.S. and partner nation CT efforts to disrupt them. Along with actions taken to directly defeat VEOs and their adherents, U.S. strategy calls for a host of sweeping initiatives, including the strengthening of effective governance in threatened areas across the globe, and bolstering U.S. government capabilities to assist partner nations in gaining and maintaining popular legitimacy.

Central to this strategy is the concept of "indirect" and "direct" approaches to CT operations, as displayed in Figure 1. The "indirect" approach involves a variety of different operations and activities, including unconventional warfare, foreign internal defense, civil-military operations, stability operations, counterintelligence, information operations, and psychological operations. These activities comprise the means by which U.S. and partner nations may attempt to shape the global environment in which VEOs thrive and operate. The
“direct” approach seeks to neutralize and dismantle VEOs themselves and prevent the re-emergence of such organizations after they are attacked. While the resiliency of modern VEOs may render the “direct” approach’s long-term impact questionable, the requirement to kill or capture terrorists exists and must be addressed in any comprehensive CT strategy. This paper will primarily focus on the implications of the “direct” approach for SOF as a global CT force, but many of the issues presented will apply to “indirect” approaches as well.

Both direct and indirect approaches focus on the creation of a U.S. CT network capable of achieving “network overmatch” against VEO networks. In developing such an enterprise, joint doctrine outlines the creation of a Global Combating Terrorism Network (GCTN). From a purely military perspective, all joint forces are directed “to provide a versatile mix of tailorable and networked organizations” to combat contemporary threats. The addition of foreign military expertise as well as that of U.S. agencies and non-governmental organizations would create a friendly network capable of creating “a critical mass of capabilities that enable both direct and indirect approaches.”

Ideally, this friendly network would adopt a “flattened,” decentralized organizational structure, enabling it to operate at speeds that networked VEOs cannot match. In advocating for the creation of a GCTN, joint doctrine attempts to fashion unity of effort from amongst disparate organizations with equities in global CT operations. The creation of such a network is hampered by the structure of contemporary national security organizations.

Existing U.S. Capabilities

The synchronized efforts of U.S. intelligence, law enforcement, and diplomatic agencies should constitute the opening gambit in any U.S. campaign to combat VEOs. U.S. strategy is explicit in calling for such a “whole of government” approach to the challenge of contemporary
CT operations.\textsuperscript{18} Synchronizing the efforts of increasingly ponderous aspects of the U.S. government involved in ensuring national security is a herculean task, however, and one for which current organizational models are woefully inadequate.

Many contemporary observers agree that the national security system of the U.S. is “increasingly misaligned with a rapidly changing global environment” and the diverse challenges presented by threats like networked VEOs.\textsuperscript{19} Despite frequent appeals for cooperation amongst “interagency” partners involved in global CT efforts, the U.S. struggles to effectively focus disparate elements of national power. Specifically, advocates for major national security reform charge that the U.S. achieves “suboptimal, and occasionally... damaging” results when confronted by complex challenges like global VEO networks, which require the simultaneous application of military, diplomatic, and economic power.\textsuperscript{20}

Rather than achieving unity of effort against networked VEOs, contemporary U.S. national security institutions frequently produce redundant or duplicative capabilities. Since the terrorist attacks of September 11, 2001, the Central Intelligence Agency (CIA) has shifted ten percent of its workforce to operate its Counter-Terrorism Center, and converted 20 percent of its intelligence analysts into “targeteers” focused on identifying targets for lethal drone strikes and paramilitary operations. Rather than focus on providing policy makers with strategic insight, formerly the CIA’s raison d’etre, critics claim that the agency is becoming a quasi-military organization, operating without the constraints and oversight normally associated with uniformed armed forces.\textsuperscript{21}

Recent drone strikes targeting high profile VEO leaders in Yemen illustrate a “convergence between the CIA and the nation’s elite military units” conducting CT operations. These operations were so seamless that it remains “unclear whether a drone supplied by the CIA
or the military" conducted the actual strikes. The CIA’s development of lethal ground and air forces, though demonstrably successful in disrupting VEO operations, represents a clear duplication of capabilities normally confined to the U.S. military forces.

Binding U.S. legislation and prevailing interpretations of the military instrument of national power dictate that Geographic Combatant Commands (GCCs) should command, control, and plan military activities directed against VEOs. Both the Goldwater-Nichols legislation of 1986 and a succession of Unified Command Plans suggest that any globally-focused CT campaign involving U.S. military forces should support GCC-directed strategies to advance U.S. national interests. Despite a clear mandate from policy makers to direct worldwide U.S. military activity, contemporary GCCs “struggle with how best to apply force outside theaters of combat.”

Theater Security Cooperation (TSC) is emerging as a primary means for GCCs to bolster international CT efforts outside theaters of combat. In 2003, the Department of Defense directed GCCs to produce annual TSC plans in an attempt to link bilateral and multilateral defense activities with U.S. strategic objectives, including global CT efforts. TSC plans complement the indirect approach described in current U.S. strategic campaign guidance for CT. While necessary, these plans are GCC specific and tend to focus narrowly on activities within a given GCC’s area of operations. Such an approach is ill-suited to combating networked VEOs whose activities ignore organizational and jurisdictional boundaries and ignores the disparity in forces assigned to different GCCs across the globe.

To execute TSC plans, or any localized military operations, expeditionary assets complement the organic military forces assigned to the GCCs. Forces capable of rapidly deploying from garrisons in the U.S., however, are also ill-suited to conducting global CT
operations in support of either direct or indirect activities. Forces based in the U.S. lack the prolonged exposure to indigenous cultures necessary to optimize TSC plans and long-term indirect strategies. Expeditionary assets such as U.S. Marine Expeditionary Units also have relatively large "footprints" when measured against dispersed and networked VEOs. While eminently capable of conducting operations to kill or capture VEO high-value targets while in theater, expeditionary assets are also far too slow to react to fleeting intelligence on transient VEO targets when alerted from bases in the U.S.

As a functional, rather than geographic combatant command, U.S. Special Operations Command (SOCOM) coordinates and synchronizes U.S. global CT efforts. Designated the supported command to plan, organize, and, when directed, execute strategy and operations in support of the Global War on Terror, SOCOM's strategy to conduct global CT operations is captured in a series of classified Concept Plans and Operations Plans. While SOCOM has aggressively pursued a portion of this mandate, it largely avoids conducting or directing global operations across GCC boundaries. Senior SOCOM leaders actively reject the notion of SOCOM-led global CT operations, claiming that SOCOM's dual mission is confined to providing SOF to other GCCs and synchronizing U.S. planning.

SOCOM's reluctance to lead and conduct operations across GCC boundaries likely stems from the GCC's resistance to cede control of military assets in their areas of responsibility (AOR). GCCs are responsible for all military activity in their AORs and most either control access through a formal clearance process or require notification of any military personnel transiting their boundaries on official business. The notion of SOF transiting their AOR without falling under their authority--particularly if pursuing lethal operations along the direct approach--is anathema to most GCCs.
The complex web of overlapping jurisdictional boundaries across the GCCs and global organizations like the U.S. State Department and the CIA also hinder SOCOM's potential ability to control global CT operations. For example, National Security Decision Directive-38 is often interpreted as granting U.S. ambassadors control over the number and type of U.S. personnel inside their respective host nations, rather than the senior military officer in the region.

Similarly, CIA chiefs of station at various U.S. Embassies typically control the planning and execution of intelligence-gathering activities and often pursue priorities different than those envisioned by military planners. With potential friction points both inside and outside of the Department of Defense (DoD), it is unsurprising that SOCOM has mostly rejected the role of a "global GCC."

**Global Pursuit**

With the above context in mind, it is clear that, despite the strategic imperative to disrupt, dismantle, and defeat networked VEOs, neither the U.S. military nor its interagency partners are adequately structured, resourced, or empowered to effectively conduct such operations. The concept of using SOF as a global CT network addresses the incoherence of current U.S. efforts and establishes a clear node of integration for non-military U.S. instruments of power. This paper proposes the label of "Global Pursuit" for the use of SOF in a CT campaign targeting networked VEOs:

The concept of Global Pursuit implies a whole of government approach to disrupting VEO networks and recognizes that such networks are not contained in a single geographic area. Defeating these networks will require their interdiction through varied means at multiple points across the globe. While this paper focuses on the military implications of such a concept,
multiple entities of the U.S. government would participate in a global, long-term, and multi-dimensional series of irregular campaigns outside current theaters of war.

**SOF as a Global CT Network**

The bulk of SOF is already organized, trained, and equipped to execute indirect Global Pursuit operations to counter VEOs. Indeed, of the eleven SOF “core activities” detailed in joint doctrine, over half are well-suited to the low-profile, long-duration, partner-intensive strategies inherent in the indirect approach.\(^{29}\) SOF units and personnel, already positioned forward in the GCCs, are organized into Theater Special Operations Commands (TSOC) capable of performing indirect operations and could be augmented by SOF dispatched from the U.S. Though this paper will primarily address shortfalls and requirements to address direct lines of operation, it is important to note that existing SOF assets are trained for and postured to execute indirect strategies, if armed with the authorities, approvals, and organizational changes outlined below.

While certain SOF organizations are capable of executing direct Global Pursuit operations against networked VEOs, they lack critical authorities to do so and are hamstrung by antiquated national-level decision-making processes. Without consolidated authorities accepted by all facets of the U.S. government, and crafted in a manner protecting the equities of non-military U.S. government organizations, any SOF-led network will make little headway in a global CT campaign. Similarly, the risks attendant to direct Global Pursuit operations creates a perceived need for tightly controlled senior leader approval processes at odds with the speed required to achieve network overmatch against global VEOs.

**SOF Authorities in the Direct Approach**

Global Pursuit operations aimed at killing or capturing VEO leadership will likely require covert or clandestine military actions, and recent U.S. strategy illuminates such requirements.\(^{30}\)
Such claims have triggered a debate within the U.S. government, centered on whether the U.S. military is authorized to conduct covert operations, or whether such action is the sole province of the CIA. Such disagreement is significant, because statutory requirements require covert action be initiated by a Presidential finding and also mandate robust Congressional notification and reporting. Both of these time consuming processes are at odds with the network overmatch concept of an agile Global Pursuit force. Resolving this debate, often referred to as “DoD-led ‘Title 10 operations’ versus CIA-led ‘Title 50 operations’” requires a brief examination of the statutory, doctrinal, and policy definitions of covert action.

Bolstered by a narrow interpretation of Title 50 of the U.S. Code, some legal experts in both the U.S. military and intelligence communities argue that authorities to conduct covert action in sovereign nations are restricted to the CIA. Such authorities cite a 1991 amendment to the National Security Act of 1947 which defines covert action as activities of the U.S. government “to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. Government will not be apparent or acknowledged publically.” The law also cites four exceptions to this definition, including “traditional diplomatic or military activities or routine support to such activities.”

Doctrinal definitions, unfortunately, differ substantially from statutory definitions. Joint doctrine defines clandestine operations as those “conducted by governmental departments or agencies in such a way as to assure secrecy or concealment.” Such activities differ from covert operations in that the emphasis in clandestine operations “is placed on concealment of the operation rather than on concealment of the identity of the sponsor.” DoD definitions neglect the foreign policy element of the statutory definition and fail to cite the “traditional military activity” exception.
Despite entrenched and potentially parochial resistance, U.S. law appears to provide ample authority for SOF to conduct direct approach military operations, including both covert and clandestine actions. Advocates for military covert action cite the “traditional military activities” exception in asserting that any operation conducted under the direction and control of a military commander fails to meet the definition of covert action. Others point to different Title 50 legislation that appears to leave the choice of U.S. government agency to conduct covert action to the President, using language that does not exclude the DoD as an option. Under this interpretation of existing U.S. law, the reluctance to grant such authorities to the DoD becomes a matter of policy and not a legal dispute.

**SOF Approvals in the Direct Approach**

The approvals necessary to mount an effective Global Pursuit campaign against networked VEOs are narrowly concentrated at the national level and issued through an antiquated decision-making hierarchy ill-suited to the requirements of global CT operations. Approvals to conduct military or covert actions in sovereign nations are typically controlled by the Executive Branch of the U.S. government. While centers of power shift from one administration to the next, contemporary bodies capable of granting approvals for military or covert action include the National Security Council’s (NSC) Principals Committee, or the President of the United States. Potential military actions requiring approvals from the highest level of the U.S. Executive Branch emerge from the highly structured bureaucracy of DoD and then wind through a series of sub-committees, inter-agency policy committees, the NSC Deputies Committee, and the Principals Committee itself, before ever reaching the President.

Approvals necessary to conduct global CT operations are not constricted solely at the national level. Both indirect and direct Global Pursuit operations will almost certainly involve
military activity in sovereign nations with which the U.S. is not at war. The coordination of U.S. non-military efforts in such nations is normally the province of the U.S. Ambassador or Chief of Mission. Recent U.S. State Department guidance directing chiefs of mission to approve “changes in the size, composition, or mandate” of the personnel assigned to a given host country is often interpreted as tacit control over military operations.\(^{38}\) However, DoD policy holds that military personnel are not restricted by State Department authority and instead fall under a military chain-of-command terminating with the applicable GCC. In practice, military operations in sovereign nations often require Chief of Mission “concurrence,” resulting in de facto approval of military operations by non-military decision-makers.

**An Architecture for SOF-led Global CT Operations**

A well-resourced military force, armed with a fusion of the authorities currently outlined in Title 10 and Title 50 of the U.S. Code, could effectively wage “Title 60” covert actions against networked VEOs. Such authorities already exist and require only changes in the interpretation of existing law, not the adoption of new legislation, in order to enable Global Pursuit operations. Identifying a narrowly focused and specialized group of SOF to conduct direct approach operations, and empowering them with the requisite authorities, might limit concerns about the risks inherent to Global Pursuit operations.

SOF-led Global Pursuit forces might also require standing NSC approvals for military or covert action against a broad array of targets in disparate sovereign nations. These standing approvals might delegate authorities to conduct military actions to the GCCs, against various VEO networks identified as a clear threat and “mapped” enough to allow leaders to identify suitable targets. These standing approvals would require the GCCs to simply notify the NSC, rather than seek approval for operations when considering direct approach operations in response
to emerging intelligence. Streamlined, responsive approval processes for operations involving particularly high political risk could be leveraged by the GCCs and involve relatively immediate access to the NSC’s Principals Committee, or the President. Such a process likely already exists to enable the time-sensitive execution of drone strikes currently employed against high-value VEO targets.39

Command and control (C2) of Global Pursuit operations would require organizational changes to current SOF structures, but with minimal investment in additional SOF equipment or manning. To effectively manage global operations against networked VEOs, SOCOM must aggressively pursue its role as a “global GCC” and create the ability to command and control such operations. C2 systems capable of controlling military activity on a global scale already exist and SOCOM could exploit such systems to enable Global Pursuit. The operation of unmanned aerial vehicles from the continental U.S. and the C2 architecture for intercontinental ballistic missile systems provides two potential examples for modification. The realization of SOCOM’s role as a “global GCC” would create a standing global operating environment in which a SOF-led network could operate against VEOs, without jurisdictional boundaries. To enable global operations inside politically sensitive or denied countries, a permanently assigned Afloat Forward Staging Base (AFSB) would allow SOF to “forward stage” without producing an overt military signature on the ground.40

SOCOM’s relationship with standing regional GCCs might involve either supported/supporting relationships or the exercise of “concurrent operational control (OPCON).” Establishing a relationship with each GCC, in which SOCOM was the supporting element to GCC-supported regional campaign plans, might mitigate potential concerns over SOF operating without regional oversight. Alternatively, and a better approach for achieving rapid network
overmatch against global VEOs, SOCOM could retain COCOM of all SOF while ceding OPCON of SOF to multiple GCCs at the same time. “Concurrent OPCON” would allow SOF to transit GCC boundaries in pursuit of transient VEO targets without seeking approval, while ensuring GCC visibility and awareness.

SOCOM should also seek combatant command authority over the TSOCs currently assigned to the Pacific and European GCCs. While still capable of acting as a force provider for GCC SOF requirements, the exercise of COCOM over regional TSOCs would enable SOCOM to leverage the forward basing of SOF elements to conduct long-duration indirect Global Pursuit operations. The TSOCs might also serve as the foundation for Regional SOF Coordination Centers, which could act as fusion nodes in a friendly global CT network.

Shakespeare warned, in considering an enemy, to “[h]eat not a furnace for your foe so hot that it do singe yourself.”41 The creation and use of a Global Pursuit force risks the potential “militarization” of U.S. foreign policy and an over-reliance on military force at the expense of other instruments of U.S. power. These risks notwithstanding, the adoption of a counter-network strategy to combat VEOs and the use of SOF as a global CT network offers tangible benefits at reasonable costs: With broadened authorities, streamlined and clearly defined approval processes, and organizational changes reflecting SOCOM’s role as a “global GCC,” SOF have the potential to address the U.S. strategic requirement to “Disrupt, Dismantle, and Defeat” networked VEOs.


3 Ibid.


7 The White House, 2010 NSS, 1-52.

8 NMS 2011, 6.

9 Joint Chiefs of Staff, Joint Publication (JP) 3-26, Counterterrorism (Washington D.C.: Office of the Joint Chiefs of Staff, 2009), II-10. Attributing hierarchical organizations to legacy VEOs that leveraged political grievances in a Leninist or Maoist fashion, the Joint Publication explicitly claims that “[n]ewer groups tend to organize or adapt to the network model.”


11 JP 3-26, III-2.

12 Ibid., III-3.

13 Ibid., III-5.

14 Ibid. JP 3-26 implies that over time, the “indirect” approach constitutes the decisive line of effort in CT operations, claiming that “the resiliency of terror organizations and networks to reconstitute their forces and reorganize their efforts limits the long-term effectiveness of the direct approach as a sole means of countering terrorism.” While the concept of employing SOF as a global CT network should involve both “direct” and “indirect” approaches, this paper will largely focus on the capabilities needed to pursue the “direct” approach, and their implications for SOF.

15 This paper defines “network overmatch” as the construction and operation of a friendly network capable of reacting with greater speed, and more precisely, than an opposing enemy network.

16 NMS 2011, 18.

17 JP 3-26, III-3.

18 2011 NSCT, 7.


20 Ibid., 17.


22 Greg Miller, “Joint strike is latest example of CIA-military convergence,” Washington Post, 1 October 2011.


25 The source document, the 2004 Unified Command Plan, is classified. See United States Special Operations Command, United States Special Operations Command History, Headquarters, USSOCOM, 2007, 16.


29 Joint Chiefs of Staff, Joint Publication 3-05: Special Operations (Washington D.C.: Office of the Joint Chiefs of Staff, 18 April 2011), II-6. The 11 SOF “core activities” include direct action, special reconnaissance, counter proliferation of weapons of mass destruction, counterterrorism, unconventional warfare, foreign internal defense, security force assistance, counterinsurgency, information operations, military information support operations and civil affairs operations.


33 Joint Chiefs of Staff, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (Washington D.C., Office of the Joint Chiefs of Staff, 8 November 2010) (as amended 15 October 2011), 53.

34 Gross, Different Worlds, 12.


36 Schultz, Richard. “Showstoppers: Nine reasons why we never sent our Special Operations Forces after al Qaeda before 9/11.” The Weekly Standard, 26 January, 2004, 5; http://www.weeklystandard.com/Content/Public/Articles/000/000/003/613twavk.asp (accessed 23 October, 2011). Title 50, Chapter 15, Section 413b stipulates that when considering covert action, a Presidential finding “shall specify each department, agency or entity of the U.S. Government authorized to fund or otherwise participate in any way in such action.” This provision does not restrict such activities to the CIA.

37 The White House; Presidential Decision Directive 1: Organization of the National Security Council System, (13 February, 2009), 2-5. This PDD is characteristic of the NSC structure generally adopted by preceding Executive administrations.


40 Establishing an AFSB would involve temporarily detailing a U.S. Navy vessel to SOF control for sustained periods off the coast of sovereign nations. Such vessels should have the deck space to allow four to six rotary winged platforms to operate, and the connectivity to allow SOF forces to tie into GCTN intelligence nodes. The U.S. Navy recently announced plans to retrofit the USS Ponce, an amphibious transport dock, into such a platform. Christopher Cavas, “Floating Base Ships to Join US Navy,” Navy Times, 28 January, 2012, http://www.navytimes.com/news/2012/01/navy-aflot-forward-staging-base-ships-join-fleet-012812w/ (accessed February 01, 2012).

Works Cited


Headquarters, United States Special Operations Command, USSOCOM Strategic Appreciation, MacDill Air Force Base, 8 July 2011.


United States Code. *Title 10, Chapter 6, Subtitle A, 161*.

United States Code. *Title 50, Chapter 15, Subchapter III, 413b*.


