AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Saving Coalition Lives and Limbs:

Disrupting the Improvised Explosive Device Network in Iraq

with

Center of Gravity Analysis

and

Social Network Viral Targeting

by

Kofi Campbell, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of Graduation Requirements

Advisor: Dr. Gregory F. Intoccia
Maxwell Air Force Base, Alabama

21 December 2008

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States Government.

Contents

List of Illustrations

Preface

I first became interested in counter-improvised explosive device (C-IED) activities while preparing for my early 2004 deployment to Iraq. Despite my access to some of the most highly classified intelligence, I found very little information on IED networks; almost all available information pertained to countering or avoiding IEDs that insurgents had already emplaced. This was surprising, since disrupting, degrading, defeating, or destroying almost any type of network is usually more effective and efficient than trying to defeat that network's outputs. Additionally, during my 2005 deployment to the Central Air Forces (CENTAF, now AFCENT) Combined Air and Space Operations Center as a targeting officer, I again observed an inadequate focus on IED networks.

While most, if not all, military professionals now acknowledge that attacking the IED network gives the military more "bang for the buck" than attempting to defeat individual IEDs, the US military has allocated more resources to the latter. It is possibly no coincidence that neither US nor Coalition C-IED efforts lead to a decrease in IED attacks in Iraq until 2008 (in Afghanistan, IED attacks increased in 2008). But IEDs still killed 130 service members that year. The US military needs a new analytic approach to the IED threat and new method to defeat the IED network.

I would like to thank my friends and family for their support as I worked on this paper. I would also like to thank my instructor and advisor, Dr. Gregory F. Intoccia who provided great guidance and mentoring, and was exceedingly patient and understanding during my deployment to South West Asia while I wrote this thesis.

Abstract

Improvised explosive devices (IED) continue to inflict coalition casualties in Iraq, indicating the United States has not found an effective means of disrupting the IED network in that country. This thesis presents center of gravity (COG) analysis and social network viral targeting as a means of disrupting the IED network in Iraq. A COG is a physical or moral entity that is the primary component of physical and moral strength, power and resistance that allows victory in battles, operations, and wars. COG analysis identifies these COGs and their critical vulnerabilities that are susceptible to neutralization, degradation, or defeat. Social network viral targeting disrupts the human elements of networks by sowing social "viruses" such as animosity, disinformation, distrust, and humiliation. Disruptive, viral information is first planted into "carriers", or people associated in some way with those targeted. These carriers then spread the viral information via various "vectors", resulting in the dissemination of disruptive information throughout the targeted persons' social network.

This research paper uses a problem/solution framework to answer the question: how can the United States most effectively further disrupt the IED network in Iraq? It describes how COG analysis can help to identify critical vulnerabilities associated with the IED network's key people, facilities, and aspects of its support network. It then shows how viral targeting can disrupt the IED network by disrupting the human element around these critical vulnerabilities. Viral targeting can include planting derogatory information about specific bomb makers and their affiliations into "carriers" such as friends, acquaintances, associates, or rivals of those bomb makers. These carriers would then spread the viral information via word of mouth or via "vectors" such as phone text messages and computer e-mails. The ensuing distrust, increased

tensions, and resources expended on protecting IED cell members' reputations and prominence reduces the effectiveness of their IED cell.

The framework recommends that coalition forces routinely conduct COG analysis on the IED network, and also develop a strategic concept that institutionalizes the employment of social network viral targeting in conjunction with US Air Force and Navy air-to-ground bombing, and ground forces' direct action. It also recommends that once coalition forces refine this strategic concept, it be applied to the war in Afghanistan, where casualties from IED attacks in that conflict more than doubled in 2008.

Introduction

Between the increase in armor and the changes in tactics, techniques and procedures that we've employed, the number of attacks . . . that have been effective has gone down, and the number of casualties per effective attack has gone down.

--General Peter Pace
Chairman of the Joint Chiefs of Staff
November 2005

What General Pace did not say was that the number of IED attacks had roughly doubled from 2004 to 2005 and thus better tactics, techniques, and procedures had failed to reduce the overall number of fatalities stemming from the IED threat.

--Michael Goldfarb
Improvised Explosive Disaster:
An inside look at the Pentagon's inadequate response to the IED threat in Iraq
The Weekly Standard
4 May 2006
Referring to General Peter Pace's November 2005 comment

The first improvised explosive device (IED)-related coalition casualty in Operation Iraqi Freedom (OIF) occurred on 18 July 2003 in the city of Fallujah, Iraq.[1] Since then, 81,000 IEDs have killed over 1,800 coalition forces in Iraq, including 133 in calendar year 2008.[2] The Department of Defense (DOD) describes IEDs as weapons of strategic influence[3], and since fiscal year 2004, has spent over $12 billion to address the IED threat.[4] However, most counter-IED (C-IED) efforts have focused on countering or defeating IEDs that insurgents have already hidden, ready to be detonated (so called "emplaced" IEDs) instead of the IED network. For example, almost all Naval Postgraduate School (NPS) C-IED research initiatives that were cited in its 2005 IED research update pertain to defeating emplaced IEDs.[5]

This "weight of effort" is surprising, since disrupting, defeating or degrading almost any type of network is usually more effective and efficient than trying to defeat that network's outputs. For example, if attempting to take down a major drug ring, law enforcement officials

might opt to arrest the head of the drug ring, the drug suppliers, drug processors, and accountants. Taking these "right hand" accomplices with relatively rare skills off the street would have far greater impact in disrupting the drug ring than a campaign that relies predominantly on arresting drug users and low level drug dealers.[6]

The same reasoning can be applied to the insurgents, terrorists, and the IED problem. In fact, killing terrorists with rare skills is 60 percent more effective than randomly killing them.[7] Because human social organizations build and use IEDs, understanding this social context is vital for defeating them.[8] In its 2007 annual report, the Joint Improvised Explosive Device Defeat Organization (JIEDDO), which focuses the military's efforts to defeat IEDs,[9] explains that the recent decline in IED incidents in Iraq can be credited to local factions supporting coalition force efforts, the sustained presence of coalition forces throughout Baghdad (facilitated by the troop surge in 2007), and operations against IED "event chains" and IED networks.[10] Technological countermeasures and tactics, techniques and procedures against devices is noticeably absent from the list. Based on JIEDDO's report, it is clear that in Iraq, attacking the network has been more effective than chasing devices. However, IEDs remain a potent threat to coalition forces, as evidenced by the continuing -- albeit reduced -- casualties from IED attacks, and the US military's continuing emphasis on deploying heavily armored vehicles to Iraq. Thus, coalition forces require an even more effective means of attacking the network.

Research Question

This study seeks to employ a specific type of analytic method and disrupt mechanism to significantly enhance the disruption of the IED network in Iraq. How can Coalition forces most effectively disrupt this network?

This thesis presents center of gravity (COG) analysis and social network viral targeting as the means to most effectively disrupt the IED network in Iraq. A COG is a physical or moral entity that is the primary component of physical and moral strength, power and resistance that allows victory in battles, operations, and wars. COG analysis identifies these COGs and their critical vulnerabilities that are vulnerable to neutralization, degradation, or defeat. COG analysis can help to identify critical vulnerabilities associated with the IED network's key people, facilities, and aspects of its support network.

Social network viral targeting disrupts the human elements of networks by sowing social "viruses" such as animosity, disinformation, distrust, and humiliation.[11] Using "carriers" and "vectors" to spread viral information, this targeting can disrupt the IED network by disrupting the human element around critical vulnerabilities identified during COG analysis. Viral targeting can include planting derogatory information about specific bomb makers and their affiliations, and allowing vectors to spread the information. The ensuing social disruption and resources expended on protecting IED cell members' reputations and reacting to interpersonal, tribe, and clan-based tensions reduces the effectiveness of their IED cell.

Assumptions and Limitations

A few assumptions and limitations are associated with this thesis. First, this paper assumes that most IED-related people, facilities, and support entities in Iraq are interconnected in some manner, resulting in the existence of an IED network. This assumption seems reasonable given the evidence of cooperation among many IED cells,[12] the sharing and selling of bomb making expertise among IED cell members, and the vibrant black market trade of bomb making material among IED cells. Lack of such connectivity would mean that instead of *one* IED network, numerous such networks exist, complicating the spread of social network viral

information aimed at most effectively disrupting the IED threat. Furthermore, the absence of interconnectivity could also indicate the absence of *any* IED network, severely complicating or even rendering impossible coalition forces' ability to sufficiently reduce IED attacks. This paper also assumes that this interconnectivity yields centers of gravity that serve to hold the IED network together and also provide the network with strength, power, and resistance.

Classification of material from the Joint IED Defeat Office (JIEDDO) and other government entities is the most significant limitation with this framework; here the research relies on only unclassified information to facilitate the widest distribution and to prevent the disclosure of sensitive information. However, the availability of unclassified, non-sensitive government reports, in addition to other open source data, analysis and news reports, allows the required research and analysis to be accomplished without classified material.

Overview

This research paper uses a problem/solution framework to answer the question: how can the United States most effectively disrupt the IED network in Iraq? Section 1 defines IEDs, provides an overview of the problems associated with IEDs in Iraq, and summarizes efforts to defeat this IED network. Section 2 selects and describes the criteria that directly relates to the IED problem. Section 3 describes two tools -- COG analysis and viral targeting -- that can be used to disrupt the IED network. Section 4 applies these tools to the criteria to examine if and how they can be used to solve the IED network problem. Finally, the Conclusion examines the implications of section 4's findings and provides recommendations, on the employment of social network viral targeting.

Description of Problem

IED Characteristics

According to the DOD and the North Atlantic Treaty Organization (NATO), an improvised explosive device is "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components."[13] Thus, an IED is basically a homemade, relatively inexpensive bomb that insurgents and terrorists use to wage unconventional or asymmetric warfare against their adversaries. It is a cheap, stand-off, precision targeting system that provides attackers with complete anonymity.[14] IEDs can be categorized into static (i.e., non-moving) IEDs, vehicle-borne IEDs (VBIED), suicide VBIEDs (SVBIED), and personal-borne IEDs (PBIED).

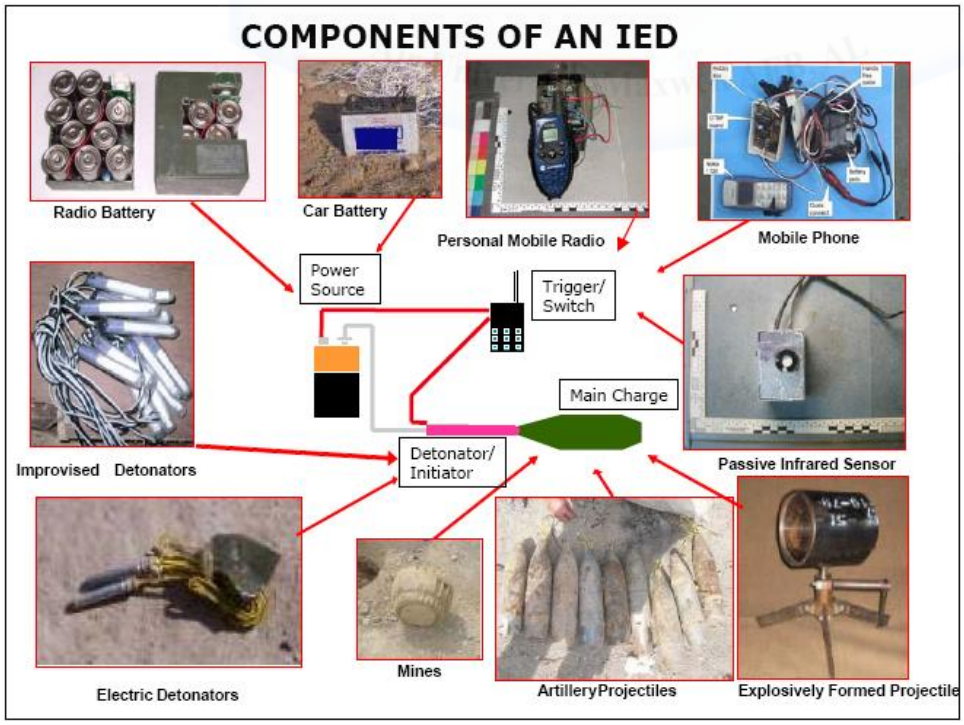

Figure 1. IED Components. (Reprinted from Australian Army, *Improvised Explosive Device (IED) Fact Sheet*, 1.)

IEDs are composed of four main parts: the power source, the trigger or switch, the detonator, and the main explosive charge.[15] The power source is usually a battery that supplies enough energy to the detonator to enable it to set off the main charge.[16] The trigger or switch, which provides another method of categorizing IEDs, is the mechanism by which the IED is detonated. It can be a radio control device (such as a mobile phone, pager, personal mobile radio, or a door bell system), a command wire (triggered by the terrorist or insurgent), a timer, or a victim-operated switch – such as a pressure plate,[17] tripwire, or infrared sensor. The detonator is a small explosive charge used to initiate the larger, main explosive charge.[18] The main charge can be conventional military explosives such as anti-tank mines, air-to-ground aircraft bombs,[19] artillery rounds, and plasticized explosives; or homemade explosives composed of nitrogen-based fertilizer.

IEDs have destroyed Bradley fighting vehicles, 70-ton Abrams tanks, and up-armored military Humvees,[20] and have also damaged the more extensively armored, $600,000 to $1 million Mine Resistant Ambush Protected (MRAP). Deep-buried IEDs and explosively formed penetrators (sometimes called explosively formed projectiles) (EFP) are the most lethal IEDs. Although they account for only 5 to 15 percent of all IEDs in Iraq, they cause approximately 40 percent of IED casualties.[21] Deep-buried IEDs often contain a couple hundred pounds of explosives and have flung heavily armored vehicles like MRAPs a hundred feet, in one case killing all on board.[22] Deep-buried IEDs became prominent in August 2005,[23] and were responsible for half of all coalition forces killed in the summer of 2007.[24] EFPs consist of a concave copper disk, behind which lies plasticized military explosives. Detonation releases an extremely fast-moving shock wave, which turns the copper disk into a hot, explosively formed

shaped charge moving at over one mile per second—faster than a rifle round. This shaped charge penetrates most kinds of armor, including that of the MRAP. EFPs first appeared in Iraq in May 2004, and the US Government has linked them to Iran.[25]

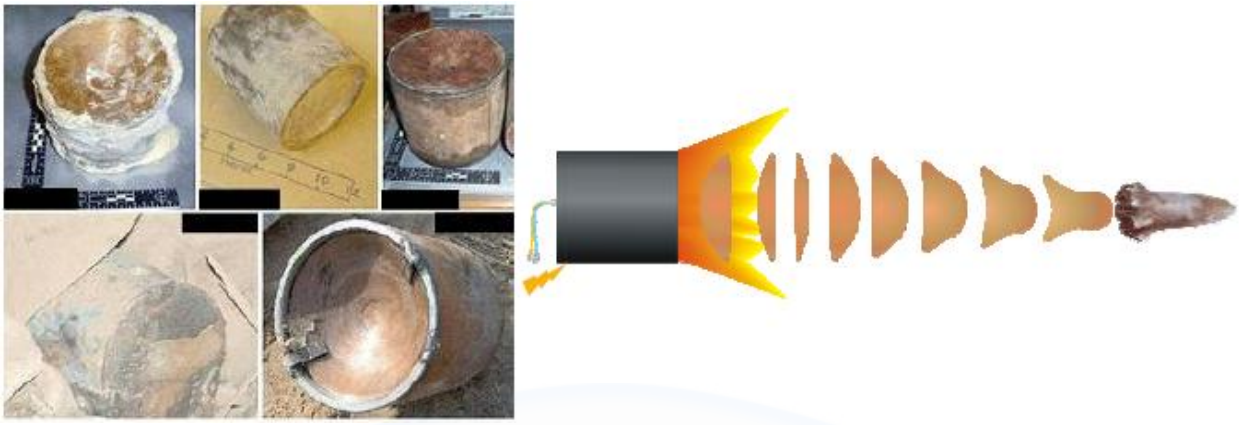

Figure 2. Explosively Formed Projectile (EFP). (Reprinted from Australian Army, *Improvised Explosive Device (IED) Fact Sheet*, 1.)

IEDs are responsible for 70 percent of coalition casualties in OIF.[26] And as of December 2008, the devices have wounded over 20,000 coalition forces, causing over 600 amputations.[27] IED attacks also negatively affect morale, especially since even some MRAPs are not impervious to the most lethal IEDs. Random, unassociated individuals are not the makers and users of these lethal devices. Rather, a network of insurgents and people who support insurgents are responsible for the use of these devices against coalition forces and Iraqi civilians.

Description of the IED Network

Merriam-Webster's Collegiate Dictionary defines a network as "an interconnected or interrelated chain, group, or system" and "a usually informally interconnected group or association of persons (as friends or professional colleagues)." Both definitions apply to an IED network. An IED network is an interconnected system of people, facilities, supplies, finances, and information that insurgents use to produce and transport IEDs, plan and execute IED attacks,

and train others to do so. Furthermore, an IED network consists of lose overlapping social partnerships that "facilitate IED core and supporting tasks."[28]

In Iraq, IED cells are typically comprised of 5-10 insurgents with specialized skills, although there are some less effective cells consisting of three to four people.[29] Up to at least 2007, there were more than 100 IED cells with specialized skills.[30] The IED network includes financiers, recruiters, acquisition personnel, bomb makers, IED emplacers and concealers, scouts (who watch for American convoys and patrols), and triggermen/bombers.

Financiers are particularly important in Iraq's IED network, as evidenced by the large sums of money being sent from outside of Iraq to fuel the insurgency.[31] Although some IED cell members are ideologically motivated, the IED network uses this money to pay some financially motivated young men to be IED bomb makers, emplacers, scouts, and triggermen.[32] Some other costs include the purchase of bomb making material. For example, supply and demand dynamics drive the price of military explosives sold on the black market to be used in IEDs.

The number of highly skilled bomb makers who use these explosives to make the most complex IEDs (e.g., difficult to detect, or made with high-tech detonation) is relatively small due to the training, military experience, or engineering skills required.[33] An indicator of the exclusivity and rare, highly technical skills of this bomb making group is the fact that most of the insurgency's expert bomb makers are former members of the Saddam Hussein-era Iraqi Intelligence Service (IIS).[34] An IIS unit called M-21 (also known as the Al Ghafiqi Project) designed IEDs.[35] And the increasing sophistication of some IED manufacturing and emplacement from September 2003 onward indicates that their design and construction has become a specialized function of a relatively few expert bomb makers."[36]

Efforts to Attack the IED Network

Although military strategists have long acknowledged that eliminating IEDs depends on neutralizing the networks that buy, build and disseminate those IEDs, only in 2006 did going after the networks become a part of counter-IED strategy.[37] In the interim, IED attacks steadily increased a few months after the war started in March 2003, reaching 100 attacks per month by the early fall of that year.[38] In October, the US Army responded by establishing a 12-person Army IED Task Force.[39] As the US Army admits, "During the early stages of the IED problem, Task Force officials believed that technology was the best way to defeat the threat."[40] Focused on training troops to recognize and counter IEDs, the task force never moved "left of boom" by attacking bomber networks before devices could be placed and detonated.[41] Even the efforts in early 2004 by a little-known Pentagon office called the Technical Support Working Group (TSWG) to target bomb makers did not push the military's counter IED efforts "left of boom."[42] Most of the task force's efforts focused on counter-IED electronic jammers, while a few members of the US Congress pushed the military and industry to rush armored vehicles to Iraq. Adm Dennis C. Blair, US Navy, retired, complained to the Joint Staff about the lack of systematic, rigorous analysis of IED trends. The former commander of US Pacific Command also considered the focus on defeating devices as analogous to focusing on a goalie's gloves -- the last line of defense -- during a soccer game.[43]

JIEDDO points to the "early success of the Army IED Task Force, which saw a reduction in casualty rates per IED attack despite an increased in-theater use of the devices over its period of operation," as the reason that then Deputy Secretary of Defense Paul Wolfowitz "transformed the entity into a Joint IED Task Force" on 12 July 2004.[44] However, the more accurate explanation is that in the eight months between the establishment of the Army IED Task Force in

October 2003 and June 2004, IEDs caused 160 Coalition fatalities, with an increase in the monthly fatality rate occurring after the creation of the Army IED Task force.[45] And in March 2004 the commander of US Central Command, Gen John Abizaid, told the House Armed Services Committee that IEDs were "the greatest casualty producer among our troops in the field."[46]

In June 2004, Gen Abizaid wrote a memorandum to Secretary of Defense Donald Rumsfeld and Chairman of the Joint Chiefs of Staff, General Richard Myers, asking for a "Manhattan Project-like effort" to help counter the IED threat.[47] This memorandum, the aforementioned IED attack and casualty trends, and the Pentagon's perceived inability to quickly deploy counter-IED technology to Iraq, prompted Wolfowitz to sign the July 2004 one-paragraph order transforming the Army IED Task Force into the Joint IED Task Force.[48]

Despite the creation of the Joint IED Task Force, US efforts still focused on only the device, resulting in no significant reduction in IED attacks or casualties. Epitomizing this futility was IED Blitz, a counter-device operation using persistent surveillance of a 12-mile section of Route Tampa, south of Balad city. Between August and November 2004, spy satellites and various manned and unmanned intelligence aircraft focused on this stretch of Route Tampa. Of the 44 IEDs detonated or were discovered by ground troops, the multimillion dollar surveillance operation did not detect any of these devices.

Meanwhile, IED attacks increased dramatically, from 5,607 in 2004 to 10,953 in 2005.[49] However, a slight shift in strategy occurred between 2005 and 2006, with more emphasis on law enforcement techniques, albeit initially with very low conviction rates.[50] The strategy shift also included the deployment of US Air Force weapons intelligence teams WITs and also a $35 million pilot program involving 90 Federal Bureau of Investigation and Drug Enforcement

Agency agents.[51] These forensics teams, in addition to operations to kill insurgents planting IEDs, were the first true attempts to attack the IED network, albeit with limited results. For example, Task Force Odin, an Army aviation unit established in July 2006, focused on insurgents planting IEDs instead of more lucrative insurgents further "left of boom" in the IED network.[52]

Criteria

Before a new method of attacking the IED network can be developed, the criteria, or desired effect must be determined (e.g, Is the goal to degrade, delay, destroy, or disrupt the IED network?). To establish this criteria, the relevant objectives at the operational level (where the tactical employment of forces is linked to national and military strategic objectives)[53] or theater strategic level of war (where military forces are employed to secure the objectives of national and multinational policies and strategies)[54] must be determined; it is at these levels that operations against IED networks occur. It is also preferable -- but not absolutely required -- to know the objectives at the national strategic level (where the nation determines national or multinational strategic objectives and guidance).[55]

Since the White House published the latest national strategy for Iraq, *The New Way Forward*, in January 2007, the situation in Iraq has changed considerably. Also, that document articulates US goals and objectives up to only July 2008.[56] So, unfortunately, *up-to-date* national security objectives for US efforts in Iraq are not available to develop criteria to counter the IED threat. Regardless, objectives at the theater strategic or operational level of war must be known in order to develop necessary criteria. Here too, there are obstacles; the April 2006 Multi-National Force - Iraq/US Embassy Baghdad Joint Campaign Plan is classified.[57]

Since Iraq-related goals and objectives are not available to guide selection of criteria vis-à-vis IEDs, any available "guidance" related to IEDs might be useful. DOD Directive 2000.19E, *Joint Improvised Explosive Device Defeat Organization (JIEDDO),* offers some guidance. The directive states that "the JIEDDO shall focus (lead, advocate, coordinate) all Department of Defense actions in support of the Combatant Commanders' and their respective Joint Task Forces' efforts to *defeat* Improvised Explosive Devices as weapons of strategic influence (emphasis added)".[58] JIEDDO's description of its lines of operations (LOO, "A logical line that connects actions on nodes and/or decisive points")[59] also provides guidance than can be used to establish desired effects of operations against the IED network. Of its three LOOs, the most pertinent is "Attack the Network." This LOO "includes actions and activities against networks designed to *reduce* their effects and to interrupt the enemy's chain of IED activities. … The offense *disrupts* the enemy's innovation cycle…"[60]

The next step is to translate the aforementioned "guidance" into desired effects using joint terminology. Joint Publication (JP) 3-03, *Joint Interdiction,* is arguably the most appropriate joint doctrinal document for this purpose, due to the fact that we seek to *interdict* -- in some form -- aspects of the IED network (the only relevant definition related to desired effects in JP 3-60, *Joint Targeting,* is actually the definition of "interdiction" from JP 3-03). JP 3-03 defines interdiction operations as "actions to **divert, disrupt, delay, or destroy an enemy's surface capabilities before they can be used effectively against friendly forces, or to otherwise achieve objectives**" (emphasis in original).[61] While the definition's use of the term "surface capabilities" is unfortunate due to potential desire and capability to disrupt or delay enemy capabilities in space or cyberspace (e.g., computer network attack), JP 3-03 redeems itself with its definition of "disrupt" -- "…*interrupt or impede* enemy or enemy capabilities or

systems, *upsetting* the flow of information, operational tempo, effective interaction, or cohesion of the enemy force or those systems. Interdiction can *disrupt* the enemy's command and control (C2) systems, intelligence collection capability, transportation systems, supply lines, industrial base, and *psychological will*" (emphasis added).[62]

Thus, "disrupt" appears to be the most appropriate and applicable desire effect against the IED network for the following reasons:

1. JIEDDO's aforementioned description of the desired effect -- *disruption* -- of offensive operations on the enemy's innovation cycle
2. JIEDDO's aforementioned description of the desired effect -- *interruption* -- of actions and activities against the enemy's chain of IED activities
3. JP 3-03 states that "*disruption will interrupt* or impede enemy or enemy capabilities or systems"

Thus, it can be logically concluded that the analytic and targeting tools to be used against the IED network in Iraq must be able to *disrupt* the network. Specifically, the tools must allow coalition forces to interrupt or impede the IED network's capabilities, upsetting the flow of information, operational tempo, effective interaction, or cohesion of the IED network. They should also be able to disrupt the IED cells' command and control (C2) systems, intelligence collection capability, transportation systems, supply lines, bomb making and procurement ability, and psychological will. The next step is to examine the tools that can potentially enable or cause this disruption.

Enabling Tools

Social Network Viral Targeting

Coalition forces in Iraq (and Afghanistan) use direct action operations such as raids and assassinations in attempts to degrade or destroy insurgent networks. However, the regenerative abilities of insurgent cell leadership often minimize the effects of these direct action operations. For example, IED cell leaders -- including sometimes even those with rare skills -- are usually easily replaced by other leaders when coalition forces capture or kill them. Furthermore, raids and assassinations fail to exploit any competitiveness among IED cell members who are aspiring to step into cell leadership roles, and also fail to exploit tensions between a new IED cell leader and other cells. While capturing and killing insurgent personalities with rare skills will remain important, coalition forces should complement these operations with other activities to further disrupt the IED network with longer lasting effects. Social network viral targeting is a mechanism that has the potential to achieve this longer lasting disruption.

Social network viral targeting disrupts the human element around rare and valuable skills of insurgent networks by sowing social "viruses" such as animosity, disinformation, distrust, and humiliation while minimizing the negative effects on innocent civilians.[63] Analogous to exposure to and the spread of biological and computer viruses, viral information is first planted into "carriers", or people associated in some way with targeted individuals. These carriers then spread the viral information via various "vectors" (e.g., phone texting), resulting in the dissemination of disruptive information throughout the targeted persons' social network. Viral information can also be placed in "reservoirs" such as Web sites, where the information sits until carriers "contract" the disruptive information.

Sowing humiliation is one particularly useful means of social network viral targeting. In fact, planners can multiply their targeting effects by impersonating one enemy leader humiliating another leader. Because everyone needs recognition and respect,[64] humans have a universally

negative reaction to shame and humiliation, varying in degree among individuals and specific cultures. In fact, research shows that shame and humiliation cause the most bitter divisions.[65] However, as shame occurs only when a person accepts, or internalizes it, it is less useful for social network viral targeting.[66] On the other hand, humiliation results in a more outward reaction that involves feeling enraged.[67] "Humiliation could be the strongest force that creates rifts between people and breaks down positive relationships."[68] This humiliation and other derogatory information causes individuals to expend energy and resources to counter the viral attack on their reputation and credibility, possibly taking time away from their primary duties.[69]

Impersonation can be accomplished by voice "morphing" technology, first developed at the Los Alamos National Laboratory in New Mexico in the late 1990s.[70] The technology allows users to take a few minutes digital recording of a voice and clone speech patterns in near real time.[71] Thus, voices of enemy leaders can be cloned to pass disruptive, fake orders to their subordinates; to respond insubordinately to their superiors; or to in speak derisively of their peers in order to create tensions within that peer group.

Using impersonation, humiliation, and various other techniques, social network viral targeting can create, exacerbate, or re-ignite tensions among groups. Law enforcement again provides examples of practices applicable to viral targeting. Prison guards sometimes create rifts and tensions among gang members. The ensuing distrust and rivalries result in the gangs' unwillingness to coordinate and collaborate among themselves.

These social network viral targeting operations can be conducted in the form of computer network attack, civil affairs, psychological operations (PSYOPS), covert or overt special operations, and information operations (IO).[72]

To successfully insert believable, compelling viral information into the social network, and to facilitate propagation of this information among "carriers", a detailed knowledge of the targets, social network, and culture is required. Planners must know the demographics of the specific group they are targeting, as these traits should influence the medium used to insert and propagate the social virus. For example, if the intent is to exacerbate tensions *among* octogenarian leaders in an autocracy (vice simply spreading propaganda about them throughout the population), it might be of pointless to use Internet chat rooms to spread social viruses. These elder leaders (or any country's leaders for that matter) are unlikely to use Internet chat rooms. Planners must also know the primary and secondary means of information transmission in a society. Is it accomplished by mostly electronic media such as radio or television, or is information usually spread by rumor? If by rumor, what are the means of doing so? Is it by some form of phone, or primarily by face-to-face communication?

In essence, social network viral targeting seemingly provides the "disrupt mechanism", or the means of achieving our aforementioned objective of *disrupting* the IED network. A subsequent section will apply this disrupt mechanism to the IED network in Iraq. However, there must be a method of identifying the relevant, key entities in a social network in order to facilitate viral targeting. Without this identification, limited computer network attack, civil affairs, PSYOPS, SOF, and IO resources might be expended on entities of the social network that are of limited importance and thus do not effectively facilitate disruption of the IED network. Center of gravity (COG) analysis potentially aids in identifying these key entities.

Center of Gravity Analysis

Center of gravity, first articulated by Prussian military theorist Carl von Clausewitz in 1832, can be a somewhat confusing concept as evidenced by the differing definitions and

explanations in NATO and US joint doctrine. The differences in COG definition among Allied Administrative Publication-6 (AAP-6), *NATO Glossary of Terms and Definitions*; JP 1-02, *DOD Dictionary of Military and Associated Terms;* JP 3-0, *Joint Operations*; and JP 5-0, *Joint Operation Planning* are minor yet significant.[73] Also indicative of the struggle the US military has had with the concept is the frequency of changes to the definition and explanation of COG; since the end of Operation Desert Storm in 1991, JP 3-0 updated the definition four times (1993, 1995, 2001, and 2006). These contradictory definitions in joint doctrine are partly a result of imperfect translations of Clausewitz's seminal book, *On War*[74] in addition to parochial military service attitudes towards the concept.[75] The result has been enduring confusion with the COG concept.

However, it is necessary to decide on a definition of COG that is close as possible to Clausewitz's original meaning, while also facilitating this research. Unfortunately, none of the aforementioned joint or allied doctrinal publications provide an accurate or suitable definition of or explanation for COG. Even the most consistent definition among the aforementioned doctrine documents -- that a COG is *the source* of moral or physical strength, power, and resistance -- is problematic, as will be explained. Three prominent experts on the COG concept, despite differences in their definitions of COG, have concluded that the aforementioned issues with imperfect translations and military service parochialism plague the definitions in joint and allied doctrine, rendering them inaccurate and useless.

Lt Col Antulio J. Echevarria II has concluded that to align the definition of COG with Clausewitz's original concept, joint doctrine should redefine center of gravity. It is not a source of strength, but rather relates to balance.[76] It is the "focal point -- the element with centripetal force to hold everything together and provide raw power, purpose, and direction."[77] Echevarria

also assesses that COGs are relevant only if a total collapse of the enemy is desired; COGs are of little to no value in wars with limited objectives[78] (e.g., the Gulf War of 1991, in which the United Nations, United States, and coalition objectives did not include destabilization and overthrow of Saddam Hussein's regime).[79] Furthermore, Echevarria concludes that joint doctrine incorrectly states that a COG exists at each of the three levels of war (strategic, operational, and tactical); based on Clausewitz's COG concept, he believes that one COG exists for an enemy's entire system.[80] Echevarria's very literal interpretation and arguably dogmatic application of Clausewitz's concepts prevents the use of the COG concept for the purpose analyzing an IED network. For example, IEDs are only a tool that insurgents use, and thus the IED network is a subset of the insurgency. Hence, IEDs and the IED network exist at the tactical and operational level of war, respectively (despite the fact that the DOD considers them weapons of strategic influence).[81]

Dr. Joseph Strange and Mr. Richard Iron also conclude that the NATO and joint definitions of COG are flawed. Like Echevarria, Strange and Iron conclude that COGs are not *the sources* of physical strength. However, unlike Echevarria, Strange and Iron claim that COGs are *the* strengths -- that COGs are simply "physical or moral entities that are the primary components of moral strength, power and resistance."[82] Using this simpler definition, Strange and Iron claim that COGs can exist at each level of war.[83]

Strange and Iron's definition of COG thus seems to be the most appropriate of the definitions examined. The definitions in NATO and joint doctrine is based on imperfect translations of Clausewitz. And Echevarria's definition is based on the dogmatic application of analogies from mechanical science. Additionally, in his view, an enemy has only one COG.

Thus, more detailed examination of the Strange and Iron model is required to ensure it will be able to identify key, vulnerable IED-related entities.

The ultimate goal of the Strange and Iron model is to identify critical vulnerabilities that are vulnerable to neutralization or defeat that will contribute to the COG failing.[84] But Strange's and Iron's full COG model contains interim steps, based on four related concepts:

1. Centers of gravity
2. Critical capabilities
3. Critical requirements
4. Critical vulnerabilities

First, planners must identify a COG. Sometimes difficult to identify, planners can identify a COG based on seven descriptors, or characteristics:

1. It is essential
2. It is a dominant characteristic
3. Everything depends on it
4. It is a hub of all power and movement
5. It is an effective target for a blow
6. It offers resistance
7. It strikes effective or heavy blows

According to Strange and Iron, a candidate COG must possess all seven characteristics.[85]

Strange and Iron effectively use the example of the Battle of the Atlantic (early to mid-1940s) during World War II. In this battle, the German U-boats, or submarines, were a COG for the Germans. The U-boats were highly effective and struck effective and heavy blows against

Allied sea routes, sinking almost 2,800 Allied merchant ships -- 68 percent of all tonnage the Germans sunk during the war.[86] The U-boats were a COG because of their critical capabilities.

Every COG has a primary ability (or abilities) that makes it a COG in a specific scenario or situation. Planners can identify a critical capability by the verb; "it can *destroy* something, or *seize* an objective, or *prevent* you from achieving a mission."[87] One of the critical capabilities of the German U-boats was their ability to overwhelm Allied warships during prolonged battles. Critical capabilities, in turn, have critical requirements that are "essential for a COG to achieve its critical capability."[88] In order to overwhelm Allied warships during prolonged battles, the Germans had to have at least 250 operational U-boats. This is a critical requirement. Once planners determine critical requirements, they can then determine the critical vulnerabilities.

"Critical vulnerabilities are those critical requirements that are deficient or vulnerable to neutralization or defeat in a way that will contribute to a center of gravity failing to achieve its critical capability."[89] In the U-boat example, the critical vulnerability is U-boat attrition (e.g., by mechanical failure or Allied attack) exceeding U-boat production.[90] Table 1 summarizes the Center of Gravity-Critical Requirement-Critical Capability-Critical Vulnerability model as it relates to the U-boats. Of note, Strange and Iron highlight two other critical capabilities, nine additional critical requirements, and over a dozen corresponding critical vulnerabilities.

German COG	**Critical Capability**
• German U-boat fleet	• Ability to overwhelm Allied warships during prolonged battles
Critical Requirement	**Critical Vulnerability**
• Achieve an operational strength of least 250 U-boats	• If U-boat attrition exceeds U-boat production

Table 1. Center of Gravity Analysis of Battle of the Atlantic (Reprinted from Dr. Joe Strange and Col Richard Iron, "Understanding Centers of Gravity and Critical Vulnerabilities," 2003, 8.)

Once planners identify COGs they must decide, in broad terms, how they will defeat them. Strange and Iron identify three principle ways to defeat or neutralize a COG. The first method is to make the COG irrelevant.[91] In the U-boat example this could have meant creating a deception plan that caused the Germans to focus their U-boat operations on targets other than merchant shipping.

Strange and Iron's second method of defeating or neutralizing a COG is to strip the COG of the support it needs to be successful.[92] In the U-boat example, Allies could have defeated or neutralized the German Fw 200 Condor aircraft that performed reconnaissance for the U-boats, finding targets for the U-boats to attack.

The final method for defeating a COG is to exploit its weaknesses.[93] For example, the U-boats are submarines, and are thus vulnerable to anti-submarine warfare technologies and techniques. In countering the IED threat, this method of exploiting systematic weaknesses is the most intuitive to consider, but all three methods can be applied.

Analysis

Viral Targeting of the IED Network in Iraq

Having examined the social network viral targeting and COG analysis concepts, it is now necessary to apply these concepts to the IED network in Iraq. As previously explained, the goal of viral targeting is to sow social "viruses" such as animosity, disinformation, distrust, and humiliation throughout a social network. Viral targeting of the IED network in Iraq is potentially a very promising disrupt mechanism due to Arab culture in addition to Iraqi tribal and family structure.

These cultural, tribal, and familial characteristics in Iraq compound the aforementioned natural human reaction to humiliation, giving planners the ideal environment in which to employ

social viral network targeting. For example, while dignity and stature are important in all cultures around the world, these traits have increased importance in the Arab world. As a previously classified Central Intelligence Agency paper indicates, dignity and stature in the Arab world are granted to only those who appear to be flawless; there is no respect for those whose faults or errors become public knowledge.[94] Thus, an Arab will expend considerable energy to keep his public persona flawless.[95] Honor is equally important, arguably the most important value in among Arabs.[96] Thus, social network viral targeting that successfully spreads believable, derogatory disinformation (or truthful information) about IED cell leaders or other key personalities in the Iraq IED network can be very effective, prompting these targeted individuals to expend considerable time and resources to recover their reputations. Furthermore, other IED cell leaders might be reluctant to interact with other IED cell leaders with sullied reputations.

Tribal culture in Iraq also offers the perfect conduit for social network viral targeting. At least three quarters of Iraq's 24 million-person population belong to one of Iraq's 100 to 150 tribes,[97] with an estimated 40 percent of Iraqis feeling "a close affinity to their tribes."[98] And although tribal power is stronger in rural areas and limited in cities, most Iraqis have a tribal affinity.[99] The downside of the tribal ethos is the occasional inter-tribal feud, occasionally leading to tit-for-tat vendetta killings and retaliations between tribes.[100] Social network viral targeting can thus attempt to create, exacerbate, or re-ignite inter-tribal conflict in order to disrupt the IED network. For example, if coalition forces successfully kill an IED cell leader from tribe A, rumors can be inserted into tribe A that informants from an IED cell comprised predominantly of tribe B was indirectly responsible for the death. The potential for a tribal feud is then born. Of course, such planning and operations would require extensive finesse. As some tribes in Iraq number more than 100,000 people, the risk exists of inter-tribal vendettas targeting

innocent members of each tribe. Coalition planners may have to target one "level" below the tribe, which in Iraq is the *clan*.

The aforementioned example that uses the spread of rumor is particularly suited for Iraq. Americans tend to view communication primarily as a means to pass information, resulting in an American preference for efficient communication.[101] Arabs tend to treat communication as relationship-centered, resulting in an Arab preference for interpersonal, or face-to-face information transfer.[102] The credibility of this interpersonal takes an extreme form in Iraq ,resulting in the prevalence of rumors in that country.[103] In fact, Iraqis pass information predominantly through rumor[104], be it by face-to-face communication, or through cellular telephone texting.

Unfortunately, social network viral targeting is only the *means* to accomplish the objective of disrupting the IED network in Iraq. The targeting by itself does not provide the necessary focus to Coalition forces. Based on the previously mentioned IED network size in Iraq of 100 IED cells, the network could have 100 cell chiefs, 50 deputies (assuming not all the cells have deputy chiefs), 60 financiers, 25 financial donors, 40 recruiters, 30 bomb makers, 15 *expert* bomb makers, and 200 emplacers (in addition to hundreds more *potential* emplacers), 10 suicide bomber smugglers, 80 bomb making facilities, and 75 weapons caches (non-descript buildings or concealed areas in which IED cells store IED explosives, other IED components, and other weapons), and 10 front companies. And as Figure 3 shows, there are numerous other physical and moral entities that would have to be considered for social network viral targeting. Social network viral targeting by itself does not offer a method to determine which of the more than 500 IED network personalities and over 100 facilities should be the focus of our viral targeting efforts, and thus the *specific* methods to use.

Naturally, our notional problem set offers some obvious targets, such as the 15 expert bomb makers. The rare skills these 15 insurgents possess should presumably be included in the viral targeting list. However, they could (and should) be prioritized on the targeting list. And for the other personalities and entities, Coalition planners need to apply some level of intellectual rigor to determine where to focus viral targeting resources. For example, which of those 100 IED cell leaders are the most relevant to the IED problem (as COG analysis will show, this relevancy can vary) *and* which are most vulnerable to social network viral targeting? To what tribes and clans do they belong? Are there existing inter-tribal or inter-clan tensions or rivalries that Coalition forces can exploit? And do *intra*-tribal or *intra*-clan rivalries exist among the IED cells? In other words, analysis is required to determine the *key* IED-related personalities and nodes that are vulnerable to our viral targeting efforts. With this determination, Coalition forces can determine the specific viral targeting methods. Center of gravity analysis potentially provides the tool to assist in these determinations.

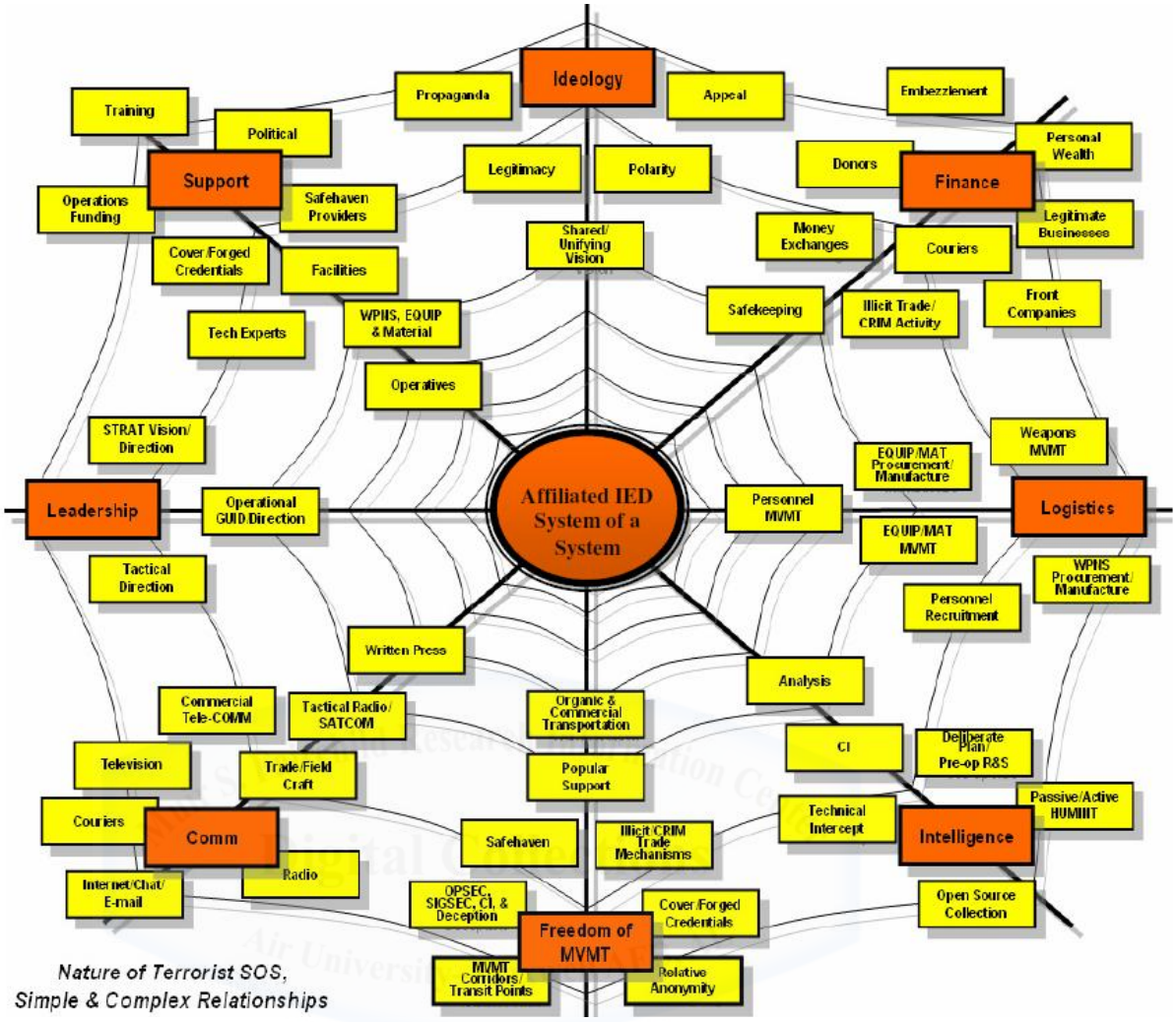

Figure 3. Nature of Terrorist Systems of Systems (Reprinted from Scott Swanson, "Viral Targeting of the IED Social Network System," *Small Wars Journal* 8, (May 2007): 64)

Center of Gravity Analysis of the IED Network in Iraq

To determine vulnerabilities in the IED network in Iraq, the COG analysis construct must be applied. The first step is to lay out what is known about the IED network. As stated previously, the IED network includes financiers, recruiters, acquisition personnel, bomb makers, IED emplacers, scouts (who watch for American convoys and patrols), and triggermen/bombers. Additionally, there are various physical and moral supporting elements of the IED network requires in order to function (see Figure 3).

COGs

The Strange and Iron definition of COG definition, "physical or moral entities that are the primary components of moral strength, power and resistance,"[105] assist in determining the COGs of Iraq's IED network. Additionally, the aforementioned seven descriptors can assist in determining if an entity is truly a COG. The most obvious potential COG of the IED network is perhaps the IEDs themselves.

Are IEDs a COG?

1. It is essential. Yes. The IED is the main output, or product of the IED network.

2. It is a dominant characteristic. Yes. As the primary cause of casualties among US and Coalition forces, IEDs have been a dominant characteristic of the insurgency in Iraq.

3. Everything depends on it. Yes. Without IEDs, the IED network loses its reason for existence.

4. It is a hub of all power and movement. Yes. IEDs serve as the hub of all power and movement for the IED network, providing IED cells a means of income, stature, and both offensive and defensive capabilities against Coalition ground movements.

5. It is an effective target for a blow. Yes. While *individual* IEDs that IED cells hav already planted are not effective "targets for a blow", Coalition forces can effectively target IEDs "left of boom" (e.g., targeting IEDs that bomb makers are manufacturing could result in the destruction of dozens of complete IEDs, in addition to numerous IED components for hundreds of other IEDs).

6. It offers resistance. Yes. IEDs have been the primary means of resistance for the IED network and insurgency at large. Indicative of the effectiveness of this mostly asymmetric resistance is the decrease in popular support for the Iraq War, partly because of the number of

Coalition casualties that IEDs continue to inflict. The percentage of Americans who consider the Iraq war a mistake has increased every year since the war began, surpassing the unpopularity of the Vietnam war.[106]

7. It strikes effective or heavy blows. Yes. IEDs in Iraq have killed almost 2,000 Coalition personnel and caused almost 600 amputations.

These findings confirm IEDs are a COG for the IED network in Iraq. The next steps are to determine the critical capabilities, critical requirements, and critical vulnerabilities. These vulnerabilities will be what coalition forces can destroy, disrupt, or neutralize.

An entity is a COG because of some primary ability or abilities. For IEDs, this critical capability is the ability to kill and injure Coalition forces. To achieve this critical capability, IEDs require designs that defeat the Coalition's armored vehicles (e.g., the deadly explosively formed projectiles or deep-buried IEDs); adaptive, innovative tactics of deploying and using IEDs (e.g., switching from RCIEDs to command wire or victim operated IEDs in response to Coalition counter-IED efforts); intelligence on Coalition convoy movements (eerily similar to U-boat fleet's critical requirements); good concealment (to prevent coalition forces from detecting the IEDs and subsequently taking evasive action or using explosive ordnance disposal personnel to disabling them); and limit IED attrition to less than what Coalition forces can destroy.

In turn, each of these critical requirements has *potential* vulnerabilities, which are those critical requirements (or components of them) that are deficient or vulnerable to neutralization or defeat in a way that will contribute to IEDs failing to kill or injure Coalition forces (see Table 2). Some critical requirements do not have associated critical vulnerabilities. Take for example, the critical requirement of the IED network to conceal IEDs to prevent Coalition forces from detecting them. As evidenced by the aforementioned IED Blitz between August and November

2004, in addition to continuing IED-related casualties in Iraq (and Afghanistan), no "reliable" vulnerabilities exists for most concealed IEDs. Advanced technology has so far failed to reliably detect these emplaced devices.

In some cases, a critical requirement may have vulnerabilities of varying degrees, with only a couple or few that can be characterized as critical. The critical requirement of IED designs that defeat the coalition's armored vehicles fails to provide a critical vulnerability associated specifically with all armored vehicles. Even the extensively armored, $600,000 to $1 million MRAP is susceptible to damage or destruction from EFPs and deep-buried IEDs. However, critical vulnerabilities exist with the bomb makers and the suppliers of EFPs and their components. Killing, capturing, and social network viral targeting of critical vulnerabilities can -- in theory -- lead to the disruption of the IED network.

One benefit COG analysis provides is the focus for social network viral targeting efforts. Based on the analysis of the IED COG, Coalition forces can consider a higher priority IED cells that produce and employ primarily EFPs. Intelligence must first identify the specific IED cells producing and employing EFPs. Next, intelligence must determine if any tribal, clan, or other tensions or rivalries exist among these IED cells, their leaders or their members. For example, Coalition forces can foment tensions between IED cell leaders in the same Iraq province by not only spreading derogatory information about one of the cell leaders, but also by impersonating the other cell leader spreading the derogatory information. If Coalition forces decide to kill or capture the cell leader and there is competition within the cell to replace him, the same sowing of humiliation and distrust can be spread. While it is unrealistic to expect social network viral targeting *by itself* to bring a specific IED cell or even a portion of the IED network to its knees,

this viral targeting of identified critical vulnerabilities can effectively complement direct action and air-to-ground bombing to disrupt the IED network.

The analysis also highlights that a priority should be the source of these EFPs and their components. In this example, one critical vulnerability is the reliance on Iran for EFP and EFP components. Further analysis can then identify the specific supply chain and key nodes for those EFPs. For example, it might be possible to conduct COG analysis of the EFP supply chain to identify its critical vulnerabilities. Considering the links between EFPs and Iran, some of these critical vulnerabilities will inevitably be Iranians or Iranian facilities in both Iraq and Iran. Here, social network viral targeting may be value, as it is unlikely the US Government will risk war with Iran over the latter's support for the insurgency as a whole or the IED network.[107] So more palatable options other than starting another war over EFPs and other IEDs may include the social viral targeting of IED cell leaders who receive aid and training from Iran, in addition to the social viral targeting of those Iranian officials.

In addition to IEDs, other COGs in the IED network may include ideology and IED cell leadership. As with the IED COG, analysis of these other COGs will identify the critical vulnerabilities that are susceptible to social network viral targeting.

IED Network COG	**Critical Capability**
• IED	• Kill and injure Coalition forces
Critical Requirement	**Critical Vulnerability**
• IED designs that defeat the Coalition's armored vehicles - EFP - Deep-buried IEDs	• If all Coalition armored vehicles are impervious to all IEDs and IED tactics [not possible] • If IED cell bomb makers can't design and manufacture IEDs that defeat Coalition's armored vehicles **[possible]** • If Iran no longer supplies EFPs and EFP

	components to insurgent groups **[possible]**
• Adaptive, innovative tactics of deploying and using IEDs - Alternate between or combine RCIEDs, command wire IEDs, and victim operated IEDs - Hidden IEDs used effectively against first responders	• If Coalition tactics, techniques, and procedures reduce or eliminate effectiveness of attacks [not possible] • If IED cell leaders or subordinates are not sufficiently experienced to employ adaptive, innovative techniques **[possible]** • If Iran no longer trains IED cell members in IED tactics **[possible]**
• Intelligence on Coalition convoy movements - IED cell discovery of predictable Coalition behavior ("Operational" warning) - IED cell knowledge of specific convoy movements ("tactical" warning)	• If Coalition movements aren't predictable **[possible]** • If Coalition operational security prevents IED cell from tactical warning [***sometimes*** **possible]**
• Good concealment	• If Coalition has technology to discover most or all concealed IEDs **[not possible]**
• Limit IED attrition to less than what Coalition forces can destroy or neutralize	• If Coalition can destroy or neutralize more IEDs than the IED network can produce **[not possible]**
• No "all-out" Coalition focus on the IED network	• Timely Coalition decision to focus on disrupting the IED network **[did not happen]**

Figure 4. IED Center of Gravity Analysis

The analysis has shown that social network viral targeting is an extremely useful tool, or method to Coalition forces can use to disrupt the IED network in Iraq. However, this targeting by itself lacks a methodology to focus the limited resources that Coalition forces have at their disposal. An analytic method that identifies the most relevant and important entities in the IED network is required to provide this focus. COG analysis provides this methodology, yielding critical vulnerabilities against which social network viral targeting can be used.

Conclusion

Although 2008 was the first year IED attacks and IED casualties in Iraq have decreased from the previous year, IEDs still killed over 130 coalition forces in 2008. Many Coalition lives and limbs could have been saved with an early, consistent emphasis on defeating or disrupting the IED network in Iraq. This paper sought a specific type of analytic method and disrupt mechanism to most effectively disrupt the IED network in Iraq. It finds that the United States can still accelerate the downward trend in IED-related casualties among coalition forces in Iraq by combining the proven analytic technique of center of gravity analysis with a new and creative disrupt mechanism -- social network viral targeting.

Center of gravity analysis identifies the primary components of moral strength, power and resistance of the IED network, thus allowing Coalition forces to focus resources on the IED network's critical vulnerabilities. Social network viral targeting subsequently offers a creative disrupt mechanism to disrupt IED network, either by itself or in conjunction with other disrupt mechanisms such as bombing or direct action by ground forces. However, coalition forces must modify some paradigms and procedures in order to accomplish this task. The following are some recommendations for using social network viral targeting.

First, coalition forces must constantly conduct center of gravity analysis on the IED network. Centers of gravity change throughout battles, operations, and wars. What might be critical requirements or critical vulnerabilities for a certain period of time may change due to coalition victories against the IED network, or clever adaptability of IED cell members.

Second, coalition forces must constantly gather cultural and biographical intelligence to facilitate social network viral targeting. This intelligence must include information on tribal, clan, and interpersonal rivalries and tensions among and within IED cells. Planners must also

collect detailed biographical intelligence on specific IED cell leaders. Not only might this intelligence reveal compromising information on specific cell leaders, it may provide enough factual information to make fabricated derogatory information more believable to intended audiences, or "carriers". Human intelligence is vital to produce this type of information.

Third, coalition forces must develop a strategic concept that *always* compliments US Air Force and Navy air-to-ground bombing with social network viral targeting. The same recommendation applies to direct action (e.g., raids, captures, assassinations) by Army, Marine and special operations forces units. In counterinsurgency operations, every bomb that an aircraft drops and every direct action by ground forces carries the risk of collateral damage, which plays into the hands of insurgents. It is important to maximize the benefits of aerial bombing and direct action by ensuring that desired effects go beyond killing the targeted individuals. Virally targeting certain IED cell members prior to and after the capture or deaths of their colleagues (without compromising operational security) would go a long way in deterring further nefarious activity by some IED cell members. At minimum, these IED cell members would be probably become paranoid about their operational security and safety, thus reducing their effectiveness. The goal would be to counter the proven regenerative ability of IED cell membership.

Fourth, Coalition forces should leverage existing service cyberspace, information operations, and psychological operations and capabilities to in order to conduct social network viral targeting. For example, US Air Force computer network attack capability, or what the Air Force calls network attack (NetA), can be used for social network viral targeting by itself, or in conjunction with air-to-ground bombing or ground force direction action.

Fifth, based on lessons learned from doing center of gravity analysis and social network viral targeting in Iraq, Coalition forces should apply these techniques to Afghanistan, where casualties from IED attacks in that conflict more than doubled in 2008.

The use of center of gravity analysis with social network viral targeting has tremendous potential to save numerous lives and limbs in Iraq and in other conflict areas.

Notes

1. Iraq Coalition Casualty Count, "Deaths Caused by IED," http://icasualties.org/Iraq/IED.aspx.

2. Ibid.

3. DOD Directive (DODD) 2000.19E, *Joint IED Defeat Organization*, 14 February 2006, 2.

4. Congressional Research Service, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*, Report RL33110 (Washington, DC: Congressional Research Service, 15 October 2008), 39.

5. Naval Postgraduate School, Office of the Dean of Research, *Improvised Explosive Devices (IEDs): An NPS Research Update*, 1 November 2005, 2.

6. White House, *National Drug Control Strategy: 2008 Annual Report* (Washington, DC: The White House, n.d.), 48.

7. Kai Stinchcombe, "How Can Governments Disrupt Terrorist Social Networks?" draft, 16 October 2004.

8. Montgomery McFate, J.D., Ph.D., "Iraq: Social Context of IEDs," *Military Review*, May-June 2005, 37.

9. DODD 2000.19E, *Joint IED Defeat Organization*, 2.

10. Joint Improvised Explosive Device Defeat Organization, *Annual Report Fiscal Year 2007* (Washington, DC: Joint Improvised Explosive Device Defeat Organization, 30 January 2008), 4.

11. Scott Swanson, "Viral Targeting of the IED Social Network System," *Small Wars Journal* 8, (May 2007): 73, www.smallwarsjournal.com.

12. Ibid, 65-66.

13. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 12 April 2001 (As Amended Through 30 September 2008), 256.

14. JIEDDO, *Annual Report Fiscal Year 2007*, 5.

15. Australian Army, *Improvised Explosive Device (IED) Fact Sheet*, 1.

16. Glenn Zorpette, "Countering IEDs," *IEEE Spectrum Online*, 1 September 2008, http://spectrum.ieee.org/sep08/6627.

17. Australian Army, *IED Fact Sheet*, 1.

18. Ibid.

19. Greg Grant, "Behind the Bomb Makers," *Defense Technology International*, January/February 2006, 30, http://www.nxtbook.com/nxtbooks/mh/dti0206/index.php?startpage=30.

20. Ibid, 32.

21. Zorpette, "Countering IEDs."

22. Ibid.

23. Rick Atkinson, "'The single most effective weapon against our deployed forces,'" *Washington Post*, 30 September 2007.

24. Rick Atkinson, "'If you don't go after the network, you're never going to stop these guys. Never,'" *Washington Post*, 3 October 2007.

25. Jim Garamone, "Precision Important to Intelligence Analysis, Pace Says," *American Forces Press Service*, 14 February 2007; Tim Kilbride, "Iranian Interference a Force-Protection Issue, General Says," *American Forces Press Service*, 14 February 2007; Atkinson, "'Single most effective weapon,'" *Washington Post*, 30 September 2007; Atkinson, "'There was a two-year learning curve . . . and a lot of people died in those two years,'" *Washington Post*, 1 October 2007**;** and Maj Gen Richard Sherlock, director for operational planning, Joint Chiefs of Staff (DOD news briefing, Pentagon, Arlington, VA, 7 February 2008).

26. Statement of Robert Gates, secretary of defense, in Senate, *Hearings before the Committee on Appropriations*, 110 Cong., 1st sess, 2007.

27. Defense Manpower Data Center, Data, Analysis and Programs Division, *Global War on Terrorism by Reason*, December 2008; and Amputee data, Charles R. Scoville, Walter Reed Army Medical Center, in Michael J. Carino, "CRS January 2009," (Fall Church, VA: US Army Office of the Surgeon General, January 2009), slide 11.

28. Swanson, "Viral Targeting," 63.

29. Ibid, 64, 66; and Grant, "Behind the Bomb Makers," 30.

30. Swanson, "Viral Targeting," 65; and Grant, "Behind the Bomb Makers," 30.

31. Grant, "Behind the Bomb Makers," 31.

32. Ibid; and Swanson, "Viral Targeting," 71.

33. Swanson, “Viral Targeting,” 65.

34. Rowan Scarborough, “Saddam’s spies had grip on Iraq,” *Washington Times,* 8 October 2004, in McFate, “The Social Context of IEDs,” 37.

35. Charles Duelfer, “Comprehensive Report of the Special Advisor to the DCI [Director of Central Intelligence] on Iraq’s WMD [weapons of mass destruction],” 30 September 2004, https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/index.html, in McFate, “The Social Context of IEDs,” 37.

36. McFate, “The Social Context of IEDs,” 37.

37. Rick Atkinson, “'The IED problem is getting out of control. We've got to stop the bleeding,'” *Washington Post,* 30 September 2007.

38. Ibid.

39. Joint Improvised Explosive Device Defeat Organization, “History,” https://www.jieddo.dod.mil/ABOUTJIEDDO/AJHOME.ASPX.

40. Rey Guzman, “Joint IED Task Force helping defuse insurgency’s threat,” *Army News Service,* 18 July 2005.

41. Atkinson, “'The IED problem is getting out of control.'”

42. House, *Testimony Of Lieutenant General Edward Hanlon Jr., Deputy Commandant For Combat Development, United States Marine Corps, Regarding Future Combat System And Force Protection Initiatives: Hearings Before The Subcommittee On Tactical Air And Land Forces of the Committee on Armed Services*, 108th Cong., 2nd sess., 2004; and US Army Sergeants Major Academy, *Long Hard Road: NCO Experiences In Afghanistan And Iraq* (Fort Bliss, TX: US Army Sergeants Major Academy, 2007), 168-169.

43. Atkinson, “'The IED problem.'”

44. JIEDDO, “History”.

45. Iraq Coalition Casualty Count, “Deaths Caused by IED.”

46. House, *Fiscal Year 2005, National Defense Authorization Act—Regional Combatant Commander, US Central Command; Assistant Secretary of Defense For International Security: Hearings before the Committee on Armed Services,* 108th Cong., 2nd sess., 2004.

47. John Barry, Michael Hastings, and Evan Thomas, “Iraq’s Real WMD,” *Newsweek,* 27 March 2006; and Atkinson, “'The IED problem is getting out of control.'”

48. Atkinson, "'The IED problem.'"

49. Barry, Hastings, and Thomas, "Iraq's Real WMD."

50. Rick Atkinson, "'If you don't go after the network.'"

51. Ibid.

52. Ibid; and Thom Shanker, "At Odds With Air Force, Army Adds Its Own Aviation Unit," *New York Times*, 22 June 2008.

53. Joint Publication 3-0, *Joint Operations*, 13 February 2008, xiii.

54. Ibid, xi.

55. Ibid, xiii.

56. House, *Securing, Stabilizing, And Rebuilding Iraq—Progress Report: Some Gains Made, Updated Strategy Needed: Hearings before the Committee on Armed Services*, 110th., 2nd sess., 2008.

57. Ibid.

58. DODD 2000.19E, *Joint IED Defeat Organization*, 2.

59. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 314.

60. JIEDDO, *Annual Report Fiscal Year 2007*, 6 (emphasis added).

61. Joint Publication 3-03, *Joint Interdiction*, 3 May 2007, vii.

62. Ibid, vii.

63. Swanson, "Viral Targeting," 63, 73.

64. Evelin Gerda Lindner, "In Times of In Times of Globalization and Human Rights: Does Humiliation Become the Most Disruptive Force?" *Journal of Human Dignity and Humiliation Studies*, 1, no. 1 (March 2007): 3.

65. Ibid, 7.

66. Ibid, 6.

67. Ibid, 6.

68. Ibid, 3.

69. Swanson, "Viral Targeting," 73.

70. William M. Arkin, "When Seeing and Hearing Isn't Believing," *Washington Post.com*, 1 February 1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin020199.htm.

71. Arkin, "When Seeing and Hearing."

72. Swanson, "Viral Targeting," 73.

73. Allied Administrative Publication-6 (AAP-6), *NATO Glossary of Terms and Definitions*, 1 April 2008, 2-C-3; JP 1-02, *DOD Dictionary*, 81; JP 3-0, *Joint Operations*, IV-10; and Joint Publication 5-0, *Joint Operation Planning*, 26 December 2006, IV-10.

74. LTC Antulio J. Echevarria II, "Center of Gravity: Recommendations for Joint Doctrine," *Joint Force Quarterly* 35 (2004): 13, http://www.ndu.edu/inss/Press/jfq_pages/0535.pdf; and Joseph L. Strange and Col Richard Iron, "Center of Gravity: What Clausewitz Really Meant," *Joint Force Quarterly* 35 (2004): 22-25, http://www.ndu.edu/inss/Press/jfq_pages/0735.pdf.

75. LTC Christopher W. Fowler, "Center of Gravity - Still Relevant After All These Years," 9 April 2001, 1.

76. Echevarria II, "Center of Gravity: Recommendations," 13.

77. Ibid, 12.

78. Ibid, 12, 15-16.

79. National Security Directive 54, Responding to Iraqi Aggression in the Gulf, 15 January 1991. Document is now declassified.

80. Echevarria II, "Center of Gravity: Recommendations," 12, 16.

81. DODD 2000.19E, JIEDDO, 14 February 2006, 2.

82. Dr. Joe Strange and Col Richard Iron, "Understanding Centers of Gravity and Critical Vulnerabilities," 2003, 1.

83. Strange and Iron, "Center of Gravity, " 25-26.

84. Strange and Iron, "Understanding Centers of Gravity," 8.

85. Ibid, 10.

86. Naval Doctrine Publication 1, *Naval Warfare*, 24 Mar 1994, 32.

87. Strange and Iron, "Understanding Centers of Gravity," 8.

88. Ibid, 7.

89. Ibid, 8.

90. Ibid, 8.

91. Ibid, 6.

92. Ibid, 6.

93. Ibid, 6.

94. Central Intelligence Agency. *"Face" Among the Arabs*. (Washington, DC: Central Intelligence Agency, 1 June 1964), 44. Document is now declassified.

95. Ibid, 49.

96. SGT Christopher Alexander, CPT Charles Kyle, and MAJ William S. McCallister, "The Iraqi Insurgent Movement," 14 November 2003, 8-9.

97. Ibid, 8; Susan Sachs, "The Sheik Takes Over; In Iraq's Next Act, Tribes May Play the Lead Role," *New York Times,* 6 June 2004; and Theodore Karasik and Ghassan Schbley, "A House of Tribes for Iraq," *Washington Post*, 25 April 2008.

98. Sachs, "The Sheik Takes Over."

99. Karasik and Schbley, "A House of Tribes"; and Valentinas Mite, "Iraq: Tribal Influence Still Strong, But Some Say Its Power Is Waning," *Radio Free Europe/Radio Liberty*, 16 July 2004, http://www.rferl.org/content/article/1053898.html.

100. William S. McCallister, "The Iraq Insurgency: Anatomy of a Tribal Rebellion," *First Monday* 10, no. 3 (7 March 2005), http://outreach.lib.uic.edu/www/issues/issue10_3/index.html.

101. Capt Stephanie R. Kelley, "Rumors in Iraq: A Guide to Winning Hearts and Minds" (master's thesis, Naval Postgraduate School, September 2004), 42.

102. Ibid, 42.

103. Ibid, 43.

104. Montgomery McFate, "The Military Utility of Understanding Adversary Culture," Joint Force Quarterly 38 (2005): 44, under "JFQ Forum," http://www.ndu.edu/inss/Press/jfq_pages/i38.htm; and Stephen Farrell, "From Iraq's Rumor Mill, a Conspiracy of Badgers," *New York Times,* 31 July 2007.

105. Strange and Iron, "Understanding Centers of Gravity," 1.

106. Jeffrey M. Jones, "Opposition to Iraq War Reaches New High," *Gallup.com*, 24 April 2008, http://www.gallup.com/poll/106783/Opposition-Iraq-War-Reaches-New-High.aspx.

107. Fred W. Baker III, "Bush Says He Will Protect US Troops, But Not Provoke War With Iran," *American Forces Press Service*, 14 Feb 2007.

Bibliography

Alexander, SGT Christopher , CPT Charles Kyle, and MAJ William S. McCallister. “The Iraqi Insurgent Movement.” 14 November 2003.

Allied Administrative Publication-6 (AAP-6), *NATO Glossary of Terms and Definitions*, 1 April 2008.

Arkin, William M. “When Seeing and Hearing Isn’t Believing.” *Washington Post.com*, 1 February 1999. http://www.washingtonpost.com/wp-srv/national/dotmil/arkin020199.htm.

Atkinson, Rick. “'The single most effective weapon against our deployed forces.'” *Washington Post*, 30 September 2007.

------. “'The IED problem is getting out of control. We've got to stop the bleeding.'” *Washington Post*, 30 September 2007.

------. “‘If you don’t go after the network, you’re never going to stop these guys. Never.’” *Washington Post,* 3 October 2007.

------. “'There was a two-year learning curve . . . and a lot of people died in those two years.’” *Washington Post,* 1 October 2007**.**

Australian Army. *Improvised Explosive Device (IED) Fact Sheet*, n.d.

Baker III, Fred W. “Bush Says He Will Protect US Troops, But Not Provoke War With Iran.” *American Forces Press Service,* 14 Feb 2007.

Barry, John, Michael Hastings, and Evan Thomas. “Iraq’s Real WMD.” *Newsweek,* 27 March 2006.

Carino, Michael J. “CRS January 2009.” Fall Church, VA: US Army Office of the Surgeon General, January 2009.

Central Intelligence Agency. “*Face” Among the Arabs*. Washington, DC: Central Intelligence Agency, 1 June 1964. Document is now declassified.

Congressional Research Service. *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*. Report RL33110. Washington, DC: Congressional Research Service, 15 October 2008.

Department of Defense (DOD) Directive 2000.19E. *Joint IED Defeat Organization*, 14 February 2006.

Defense Manpower Data Center, Data, Analysis and Programs Division. *Global War on Terrorism by Reason*, December 2008.

Duelfer, Charles. "Comprehensive Report of the Special Advisor to the DCI [Director of Central Intelligence] on Iraq's WMD [weapons of mass destruction]." VA: Central Intelligence Agency, 30 September 2004. https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/index.html.

Gates, Robert, secretary of defense. Statement in Senate, *Hearings before the Committee on Appropriations.* 110 Cong., 1st sess, 2007.

Garamone, Jim. "Precision Important to Intelligence Analysis, Pace Says." *American Forces Press Service*, 14 February 2007.

Grant, Greg. "Behind the Bomb Makers." *Defense Technology International*, January/February 2006, 30-32. http://www.nxtbook.com/nxtbooks/mh/dti0206/index.php?startpage=30.

Guzman, Rey. "Joint IED Task Force helping defuse insurgency's threat." *Army News Service*, 18 July 2005.

Echevarria, LTC Antulio J. II. "Center of Gravity: Recommendations for Joint Doctrine." *Joint Force Quarterly* 35 (2004): 10-17. http://www.ndu.edu/inss/Press/jfq_pages/0535.pdf.

Farrell, Stephen. "From Iraq's Rumor Mill, a Conspiracy of Badgers." *New York Times,* 31 July 2007.

Fowler, LTC Christopher W. "Center of Gravity - Still Relevant After All These Years." 9 April 2001.

Iraq Coalition Casualty Count. "Deaths Caused by IED." http://icasualties.org/oif/IED.aspx.

Joint Improvised Explosive Device Defeat Organization. *Annual Report Fiscal Year 2007*. Washington, DC: Joint Improvised Explosive Device Defeat Organization, 30 January 2008.

------. "History." https://www.jieddo.dod.mil/ABOUTJIEDDO/AJHOME.ASPX.

Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (As Amended Through 30 September 2008).

Joint Publication 3-0, *Joint Operations*, 13 February 2008.

Joint Publication 3-03, *Joint Interdiction*, 3 May 2007.

Joint Publication 5-0, *Joint Operation Planning*, 26 December 2006.

Jones, Jeffrey M. “Opposition to Iraq War Reaches New High.” *Gallup.com*, 24 April 2008. http://www.gallup.com/poll/106783/Opposition-Iraq-War-Reaches-New-High.aspx.
Karasik, Theodore, and Ghassan Schbley. “A House of Tribes for Iraq.” *Washington Post*, 25 April 2008.

Kelley, Capt Stephanie R., “Rumors in Iraq: A Guide to Winning Hearts and Minds.” Master’s thesis, Naval Postgraduate School, September 2004.

Kilbride, Tim, “Iranian Interference a Force-Protection Issue, General Says.” *American Forces Press Service*, 14 February 2007.

Lindner, Evelin Gerda. “In Times of In Times of Globalization and Human Rights: Does Humiliation Become the Most Disruptive Force?” *Journal of Human Dignity and Humiliation Studies*, 1, no. 1 (March 2007).

McCallister, William S. “The Iraq Insurgency: Anatomy of a Tribal Rebellion.” *First Monday* 10, no. 3 (7 March 2005). http://outreach.lib.uic.edu/www/issues/issue10_3/index.html.

McFate, Montgomery, J.D., Ph.D. “Iraq: Social Context of IEDs.” *Military Review*, May-June 2005, 37-40.

------. “The Military Utility of Understanding Adversary Culture.” Joint Force Quarterly 38 (2005): 42-48. Under “JFQ Forum.” http://www.ndu.edu/inss/Press/jfq_pages/i38.htm.

Mite, Valentinas. “Iraq: Tribal Influence Still Strong, But Some Say Its Power Is Waning.” *Radio Free Europe/Radio Liberty*, 16 July 2004. http://www.rferl.org/content/article/1053898.html.

Naval Postgraduate School. Office of the Dean of Research. *Improvised Explosive Devices (IEDs): An NPS Research Update*, 1 November 2005.

National Security Directive 54, Responding to Iraqi Aggression in the Gulf, 15 January 1991. Document is now declassified.

Sachs, Susan. “The Sheik Takes Over; In Iraq’s Next Act, Tribes May Play the Lead Role.” *New York Times*, 6 June 2004.

Scarborough, Rowan. “Saddam’s spies had grip on Iraq.” *Washington Times*, 8 October 2004.

Shanker, Thom. “At Odds With Air Force, Army Adds Its Own Aviation Unit.” *New York Times*, 22 June 2008.

Sherlock, Maj Gen Richard, director for operational planning, Joint Chiefs of Staff. DOD news briefing, Pentagon, Arlington, VA, 7 February 2008.

Stinchcombe, Kai. "How Can Governments Disrupt Terrorist Social Networks?" draft, 16 October 2004.

Strange, Joseph L., and Col Richard Iron. "Center of Gravity: What Clausewitz Really Meant." *Joint Force Quarterly* 35 (2004): 20-27. http://www.ndu.edu/inss/Press/jfq_pages/0735.pdf.

Strange, Dr. Joseph L., and Col Richard Iron. "Understanding Centers of Gravity and Critical Vulnerabilities." 2003.

Swanson, Scott. "Viral Targeting of the IED Social Network System." *Small Wars Journal* 8, (May 2007): 62-77. www.smallwarsjournal.com.

US House. *Fiscal Year 2005, National Defense Authorization Act—Regional Combatant Commander, US Central Command; Assistant Secretary of Defense For International Security: Hearings before the Committee on Armed Services.* 108th Cong., 2nd sess., 2004.

------. *Testimony Of Lieutenant General Edward Hanlon Jr., Deputy Commandant For Combat Development, United States Marine Corps, Regarding Future Combat System And Force Protection Initiatives: Hearings Before The Subcommittee On Tactical Air And Land Forces of the Committee on Armed Services.* 108th Cong., 2nd sess., 2004.

------. *Securing, Stabilizing, And Rebuilding Iraq—Progress Report: Some Gains Made, Updated Strategy Needed: Hearings before the Committee on Armed Services*. 110th., 2nd sess., 2008.

US Army Sergeants Major Academy. *Long Hard Road: NCO Experiences In Afghanistan And Iraq*, Fort Bliss, TX: US Army Sergeants Major Academy, 2007.

White House. *National Drug Control Strategy: 2008 Annual Report.* Washington, DC: The White House, n.d.

Zorpette, Glenn. "Countering IEDs." *IEEE Spectrum Online*, 1 September 2008. http://spectrum.ieee.org/sep08/6627.