# In Support of the Common Defense: Homeland Defense & Security Journal

## Volume 1

Edited by: Professor Bert B. Tussing, Colonel Kurt S. Crytzer, Colonel Steven P. Carney, Colonel Janice E. King

United States Army War College
Center for Strategic Leadership
Homeland Defense and Security Issues Group

# In Support of the Common Defense

## A Homeland Defense and Security Journal


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# IN SUPPORT OF THE COMMON DEFENSE

## A Homeland Defense and Security Journal

*A Selection of United States Army War College Student Papers Relevant to Issues Surrounding Homeland Security*

**Volume One**

**Editors:**

**Bert B. Tussing, Kurt Crytzer and Steve Carney**

**In Support of the Common Defense**

***A Homeland Defense and Security Journal***

**A Selection of United States Army War College Student Papers Relevant to Issues Surrounding Homeland Security**

***Volume One***

**April 2012**

**Executive Agent for this publication:**
**United States Army War College**



**This publication is available on line at:**

**http://www.csl.army.mil/AllPublications.aspx**

**Cover design by Helen Musser and Janice King.**

**U.S. ARMY WAR COLLEGE**
**CARLISLE BARRACKS, PENNSYLVANIA 17013**

# Contents

**Preface** vii

**Section 1: Threats Facing Our Nation: Challenges and Responses**

**Introduction** 3
*Colonel Kurt S. Crytzer*

**A New Mindset for Countering Terrorism** 7
*Colonel David P. Goldthorpe*

**Systems Analysis, Centers of Gravity and Homeland Security** 27
*Lieutenant Colonel David Rodriguez*

**Electromagnetic Pulse: A Catastrophic Threat to the Homeland** 45
*Colonel Robert Oreskovic*

**DIME Elements of Jihad** 61
*Colonel Shirley J. Lancaster*

**Cyber Attack! Crime or Act of War?** 81
*Lieutenant Colonel David M. Keely*

**Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy** 103
*Lieutenant Colonel Douglas S. Smith*

**History and Evolution of MalWare** 123
*Colonel Jason M. Spade*

**Section 2: Strengthening Defense Support of Civil Authorities**

**Introduction** 131
*Professor Bert B. Tussing*

**Reforming Disaster and Emergency Response** 133
*Colonel Mark D. Johnson*

**Homeland Security Regional Unity of Effort** 149
*Lieutenant Colonel Valery C. Keaveny, Jr.*

**Miltary Police Mutual Aid and the Posse Comitatus Act** 171
*Lieutenant Colonel Dennis M. Zink*

**Contingency Dual Status Commander: Balancing Title 10 and 32 Responsibilities** 187
*Lieutenant Colonel William J. Pendergast IV*

## Section 3: Securing our Borders

**Introduction** 207
*Colonel Steven P. Carney*

**The Mexican Cartels and Jihadist Terrorism** 209
*Lieutenant Colonel John P. Maier*

**Securing the U.S. Southern Land Border: Enhancing the Interagency Effort** 215
*Special Agent Michael D. Kennedy*

**U.S.-Mexico Security Cooperation: The Time to Act is Now** 237
*Colonel Vance F. Stewart III*

**Endnotes** 255

# Preface

AN UNSPOKEN STANDARD of the Armed Forces has always been, "When the nation is least ready, we must be most ready." While that rings clear as far as warfare is concerned, it is not nearly so when it comes to the realm of domestic security. In spite of strategies that continue to espouse homeland security and homeland defense as "job one," woefully few in the Department of Defense have studied the issues, the intricacies, and the nuances that necessarily surround the use of the military in the domestic environment. Our military's leadership understands intuitively that there are differences in the way that we can respond "over here" as opposed to "over there." But the majority of our forces have not devoted the type of thinking to those vital distinctions as is most often associated with other aspects of our military's employment. As 9/11 drifts from the personal to the historic, the need to focus on these issues seems to have faded.

To contribute to a renewed focus on these vital issues, the Homeland Defense and Security Issues Group of the United States Army War College's Center for Strategic Leadership is pleased to present this journal of selected student works. Taken from the classes of 2010 and 2011, the papers represent the cross section of the War College community – drawing from our resident classes, distance education classes and the War College fellows. The authors of our selections are from both inside and out of the Department of Defense, and include representatives of the Active Military Component, the Services' Reserve, and the National Guard.

Not surprisingly, the themes of several of the papers have followed the headlines of America's security concerns. The southwest border of the United States captured the attention and commitment of several of our authors. Safeguarding "cyberspace," as a function of domestic law, and as a function of national security, garnered a predictable focus. A dedicated assessment of the terrorist threat and its immediacy to our people also finds its appropriate place in the collection.

But beyond these are things the average reader may find less intuitive, but nevertheless essential to the civil-military partnerships required in

meeting our domestic security requirements. Several of our authors delve into the appropriate relationship between military and civil agencies in preparing for and responding to disasters – whether those disasters are natural calamities, large-scale accidents, or deliberate attacks against our people and our infrastructure. The range of considerations contained in these papers includes discussions over the interactions that must take place among various federal interagency components, parallel activities within the states, and the largely unchartered territory between the two. Of equal importance, the interaction between military components within the envisioned civil-military response is also examined. In each case, the authors' intent is to help define solutions to questions in theory, rather than risk their becoming obstacles in practice.

In some cases, our contributors have reached beyond singular military application (albeit with an understandably military viewpoint) to examine existing strategies and evolving conditions surrounding emergency management and other aspects of homeland security. One submission balances perspectives of "center of gravity" against institutional risk assessment; another calls us to view jihad through the prism of "instruments of power." In both cases, we are reminded that existing institutional mindsets and models – that have been developed, evaluated and amended over time – may find application against these new challenges. In both cases, we are left to understand that continued evaluation and amendments will always be required.

In bringing together this publication, particular thanks go out to several behind-the-scenes contributors without whom it would have never found its way to print. We are grateful to Dr. Larry Miller and Ms. Karen Slusser of the United States Army War College's Communicative Arts Division for assisting us in identifying potential papers for this compendium. Likewise, we wish to thank Ms. Helen Musser of Metro Productions and Colonel Janice King for our cover design. In particular, however, we would like to gratefully acknowledge the work of Mr. Ritchie Dion, whose meticulous editing played a vital part in fielding not only this publication, but so many others for the U.S. Army War College's Center for Strategic Leadership.

Finally, we are both gratified and grateful to the students of the United States Army War College who have devoted time and effort in these

studies. In doing so, they have fulfilled a vital part of the U.S. Army War College's mission: bringing a disciplined brand of strategic thinking to the examination of issues of importance to the defense and security of the homeland.

Professor Bert B. Tussing,
Director, Homeland Defense and Security Issues Group
United States Army War College
Center for Strategic Leadership


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Section One

## Threats Facing Our Nation


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Introduction

**Colonel Kurt Steele Crytzer**

Homeland Defense and Security Issues Group
Center for Strategic Leadership
U.S. Army War College

AS I STOOD AT THE FLIGHT 93 MEMORIAL WALL watching, the President and First Lady laid a wreath in remembrance of the victims lost on that terrible day. Not a word was spoken, no speeches given, just the somber ceremony of remembrance dedicated to victims of a once unfathomable act of terror. At that moment the thought occurred to me that 10 years had passed by so quickly. It had actually been a decade since we witnessed the horrors attributed to the worst attacks our country had ever known on its soil. The emotion and mourning of millions, along with the unification and anger that followed still seemed new rather than a decade old. I also reflected on other actions that had followed the events of that day, such as military deployments, the eventual fighting, and the additional losses our nation experienced in terms of blood and treasure. We had become a generation defined by the horrendous events of September 11th and the actions which followed.

In thar somber moment, there seemed to be another dynamic stirring. As we remembered all of the sacrifice and loss, there appeared to be a sense of closure. After all, the leader of the organization that had started all this had recently been killed, we were beginning to pull out of Iraq, and a tentative timeline had been set for Afghanistan. There seemed to be an attitude that the time had come to move on, as if a decade was enough time to mourn. It was time to focus on life as it is now and look towards other pressing issues such as the economy or new adversaries rising in power on the world's stage. It was time to focus on today's problems.

As I observed this dynamic, the thought occurred to me that this was both a positive and a negative phenomenon. The positive part follows the logic that we cannot live our lives in fear anymore. We must be

resilient, knowing that there are many threats still out there, perhaps even more so than before. And while these threats could attempt to strike at the heart of this nation sometime in the future, we will not allow our society to be crippled by angst. There is a delicate balance between remaining vigilant and not becoming a slave to fear. We can acknowledge that there are risks, but must remain determined that the knowledge of risk will not disrupt our way of life. We may be prudent in the face of all we have learned, but must not allow ourselves to become overly anxious.

These thoughts led me to a negative side of the dynamic. There is a distinct possibility that our society could stop thinking about all that we have learned, which in itself would be tragic. We simply cannot forget the lessons and we must continue to prepare for dealing with future occurrences of terror and disaster. We cannot allow the horror of our recollections to become a distant nightmare, one that is sometimes mentioned but not really considered. We cannot forget and we cannot become complacent, as such attitudes have cost our country too much already.

It is not easy to remain vigilant. In a time of shrinking budgets, rising deficits and hurried deadlines, it is extremely easy to look away. The reality of these factors will at least alter the risk we are willing to accept and the methodologies we use in an effort to protect our citizens, but we cannot forget the lessons. The costs have been too high to now be forgotten. Other events which have subsequently followed and severely cost this nation are just as important to remember, such as Hurricane Katrina. We must be prudent, and even under greater constraints, we must be prepared. Otherwise, we have suffered in vain.

So in this time, a decade on, let us live the American Dream while keeping an eye to the threat. Let us work on internal issues while remaining alert to new storm clouds approaching. Let us be fiscally responsible, without decimating the systems that will protect America. The balance is our challenge, and our success in attaining that balance may well be determined in the not too distant future.

This section of the Journal reflects the works of multiple students and covers a myriad of "threat" related topics. Within this section, the

reader will find differing opinions from the authors on some of the most complex issues facing our country today. These opinions are those of the authors, and not necessarily the opinions of the U.S. Army War College or the publishers of this journal. Some of the topics addressed are controversial, but none are without merit or fully resolved. We dedicate this section of the Journal to the unsung heroes, both on the battlefields abroad and on the streets of our nation, who have dedicated their lives to the protection of their fellow countrymen. We also dedicate this to the fallen and to the families who have suffered great loss in this decade of challenge. Our charge remains to ensure their sacrifices are never forgotten, nor their losses paid in vain.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# A New Mindset for Countering Terrorism

**Colonel Daniel P. Goldthorpe**
United States Army

NOTHING HAS SHAPED THE SECURITY environment of the 21st century more than the specter of global terrorism. As the sole remaining superpower, how the United States responds to, and can affect terrorism will have a profound impact on world security for decades to come. This paper examines U.S. counterterrorism policy, national security interests and foreign relations to establish options for a more effective policy that provides a national direction and synchronizes all instruments of national power in the struggle against terrorism. For the purpose of this paper, I will analyze terrorism in the context of transnational movements rather than individual acts or organizations. A new mindset is necessary to accurately analyze the threat and craft a successful vision that leads to a more effective policy, not only to combat terrorism in the near term, but to ultimately protect U.S. interests domestically and abroad in the long-term.

## The Road to Current Policy

American policy and actions in the past several decades are a legacy that the rest of the world is keenly observing and devising strategies against. In the post-World War II era, terrorism was a tactic commonly used by militant groups as a violent means to bring about political change within their ruling governments. As a stable democracy, the United States was largely immune to the influence of terrorism, particularly to the homeland during this period. Moreover, the United States was engaged in a monolithic struggle against communism in the Cold War; counterterrorism received little attention in the realm of National Security Strategy. Although President Reagan first established a Combating Terrorism Task Force with National Security Decision Directive 179 (NSDD-179),[1] it focused primarily on travel of U.S. citizens abroad and the security of service members. It was not until the Clinton administration when international terrorism became considered a significant national security threat.

**Clinton Administration, 1992-2000**

The most significant occurrences of international terrorism against U.S. interests prior to the Clinton administration were the Beirut bombing in 1983, the Achille Lauro hijacking in 1985, and the Pan Am flight 103 bombing in Lockerbie, Scotland.[2] These attacks characterized international terrorism at the time, which was motivated by a desire to influence policy, exploit Palestinian unrest, anti-Zionism and increase the influence of groups such as Hezbollah and the Palestinian Liberation Organization (PLO). Additionally, state sponsors of terrorism like Libya fomented anti-Western sentiment in the Middle East, yet lacked the audacity or the means to attack the U.S. homeland. Thus, the rise of international terrorism in the 1970s and 1980s caused a sense of vulnerability for Americans abroad, but also reinforced a sense of security that the U.S. homeland was insulated from terrorist attacks.

In 1993, the al Qaeda bombing of the World Trade Center exposed a vulnerability to terrorist attacks on U.S. soil, in addition to revealing an increased audacity and determination of international terrorist networks. In 1995, the Clinton Administration issued a Presidential Decision Directive outlining *U.S. Policy on Counterterrorism*, entitled PDD-39. The directive outlined four basic elements for combating terrorism: reduce vulnerabilities; deter; respond; and weapons of mass destruction. It also stated the intent to deter, defeat and respond vigorously to preempt, apprehend and prosecute governments or individuals that perpetrate or plan such attacks. The directive further reiterated that U.S. policy will not be affected by terrorist acts.[3] The counterterrorism policy announced in PDD-39 was largely focused on defense and deterrence, relying heavily on diplomacy, sanctions and increased vigilance. A fairly comprehensive policy, it emphasized passive and reactive measures with the offensive focus tied primarily to preventing the acquisition and use of weapons of mass destruction.

**Bush Administration, 2000-2008**

The attacks of September 11, 2001, provided the basis for the Bush administration counterterrorism policy. The brazen re-attacks by al Qaeda on U.S. soil caused rapid and substantive changes to U.S. counterterrorism policy and foreign relations. The Bush administration formed the Department of Homeland Security (DHS) as a cabinet

level office charged as lead agency for protecting the territory of the United States from terrorist attacks, while the State Department and Department of Defense retained responsibilities abroad.[4]

Although there have been no successful terrorist attacks against the U.S. homeland since 9/11, a heavy cost in blood and treasure has been expended in the subsequent wars in Afghanistan and Iraq. Each conflict sought and achieved regime changes to protect the United Stattes from future terrorist attacks, but have expanded into drawn out insurgencies that have inspired greater resentment against the West and injected substantial financial and physical support for terrorist organizations and ideologies like al Qaeda and the Taliban. Regime change in and of itself failed to deter, and may, in fact, have contributed to the expansion of terrorism.

A significant outcome of the Bush years was that a widespread perception developed that viewed terrorism as a struggle between radical Muslims against the Western world. In some circles, U.S. policy came to be viewed as a war against Islam.

This distortion was fueled by the conflict being dubbed "The Global War on Terror" (GWOT), and the U.S. determination to hunt terrorists to the ends of the earth also had a polarizing effect that was exploited by radicals. Another damaging foreign policy blow to the United States was President Bush's 2002 State of the Union Address which named Iran, Iraq and North Korea as part of an "Axis of Evil." It sent a message that the United States was not looking to negotiate and consequently resulted in the invasion of Iraq and ignited urgency in nuclear weapon development by Iran and North Korea.[5] This new course was formally articulated in the 2002 National Security Strategy which introduced two key policy principles of unilateralism and preemption, which came to be known as the "Bush Doctrine."[6] These actions started reversing the groundswell of support the U.S. enjoyed after 9/11. The policy actions of the United States divided domestic and world opinion, while implying a message about U.S. intentions to unilaterally prosecute the "GWOT" against an enemy broader than just al Qaeda.

**Obama Administration, 2008 to Present**

The Obama administration has yet to introduce a formal counter-terrorism policy, instead continuing generally along existing policy lines; however, the administration has made significant changes in the strategies of the wars in Iraq and Afghanistan. The administration accepted responsibility for two wars mired in insurgency, struggling to rebuild infrastructure and establish democracy where it had not existed before. They made clear a desire to rapidly draw down U.S. forces in Iraq to divert resources toward Afghanistan, which they viewed as the "just war" and harbored those responsible for 9/11.

In outlining his strategy for Afghanistan, President Obama moved away from nation building and redefined the U.S. objectives in Afghanistan to: 1) deny al Qaeda safe haven, 2) reverse Taliban momentum and deny the ability to overthrow the government, and 3) strengthen the Afghan government and security forces.[7] In essence, the early actions of the Obama administration moved U.S. policy away from a GWOT, narrowed military objectives and expressed a desire to extricate from the conflict in order to concentrate on domestic issues. These changes are counter to previous policy to take the fight to the enemy, dismantle terrorist regimes and hunt terrorists relentlessly throughout the world; moreover, it moved toward repairing the U.S. image and foreign relations.

Over the past few decades, U.S. counterterrorism policy has been inconsistent; shifting between what critics might view as bureaucratic and soft, to a neo-imperialist imposition of western values, to an ambiguous mix of conciliation and waning resolve. When Afghanistan and Iraq transitioned from wars of liberation to insurgencies, the United States failed to adjust their national objectives in accordance with the new paradigm, instead adapting strategies to defeat the latest perceived threat. This incoherence is reflective of the counterterrorism policy trend over the years.

As the sole superpower, the United States wears a bull's-eye on its back and will face challenges by state and non-state actors. Is terrorism something that can be defeated through war in the same way an invading nation might be militarily conquered? That is a question that must be examined as the current war enters a second decade with no

discernible end in sight. A clear understanding of the threat is necessary to build a solid and consistent policy along with an effective strategy that transcends administrations and denies terrorists their objectives.

## Objective of Policy and Strategy

United States counterterrorism policy should define clear goals and represent the national interest. The corresponding strategy cannot simply be a reflection of a desire to preserve those interests, such as protecting democracy and self-determination. An effective strategy must obtain national interests, and therefore, must effectively overcome the threat. With the uncertain nature of the threat, the proliferation of weapons of mass destruction, and the distinction of being the most prominent symbol of anti-western enmity, it is well within the United States security interest to reserve the right to preempt and/or retaliate toward any aggressor that threatens American citizens or U.S. interests. This caveat is necessary due to the threat, but as a matter of policy, it should not be construed as an automatic declaration of war, but more as an instrument to eradicate threats based on prioritized interests. This is significant because some practitioners of global jihad have the expressed goal of attacking the United States simply to invite a war with the West.[8] This is the dichotomy of "fighting" terrorism; terror is a tactic and countering that tactic with the use of force often strengthens the cause of the terrorist. A well crafted U.S. policy and strategy should go beyond defeating the tactic, but address the root causes that inspire the use of that tactic, are consistent with the rule of law, and are more compelling than the radical alternatives espoused by terrorist ideologies and organizations.

## Clarify the Terminology

To develop an effective strategy, one must understand and clarify the terminology. This task is complicated, since there is no universally agreed upon definition of terrorism and it is unlikely that a consensus will ever be reached due to the significant nuances and implications a collective definition might generate. This illustrates why understanding terrorism is so problematic. If the very definition has multiple and varied interpretations, imagine the myriad of potential solutions the variously interpreted definitions might inspire. Expanding this concept, it is

instructive to examine how organizations representing the instruments of national power define terrorism.

Diplomatically, the U.S. State Department defines terrorism as, "a premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."[9] Militarily, Department of Defense defines terrorism as, "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[10]

In the Information realm, the United Nations has been unable to reach a consensus on defining terrorism primarily due to the standoff with the Organization of the Islamic Conference (OIC). The OIC seeks to insert into the Convention:

> *"The activities of the parties during an armed conflict, including in situations of foreign occupation....are not governed by this Convention." Or, as the Pakistani delegate describes the standoff on behalf of the OIC, there is a need "to make a distinction between terrorism and the exercise of legitimate right of peoples to resist foreign occupation." This claim purports to exclude blowing up certain civilians from the reach of international law and organizations. It is central to interpreting every proclamation by the states which have ratified these conventions in any UN forum purporting to combat terrorism.*[11]

Some would argue that one man's terrorist is another man's freedom fighter. It is the inherent right of societies to defend themselves against invaders; however, attacks on civilians clearly violate norms protecting non-combatants and cannot be justified.

Although not authoritatively recognized, but valuable in the context of this discussion; a November 2004 United Nations Secretary General report described terrorism as any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act."[12]

Clearly, terrorism is difficult to define and its elusive character has led to a basic misunderstanding of the concept. Many definitions are in agreement that the ***means*** of terrorism are manifested through violence in order to influence a desired outcome or ***endstate***. What is debatable is the ***ways*** of terrorism; or what is the distinction between an act of war, an act of terror, or the commission of a crime. Is this violence legitimate expression of self-determination? Can one define combatants and non-combatants in this type of struggle? Those answers go beyond the scope of this paper, but they underscore the implications of building a strategy based on an imprecise understanding of what terrorism is, and what it is not. In some instances, the terminology and concepts converge. I will use the terms extremist, radical Islamist, jihadist and terrorist interchangeably because they all share the same characteristic of attacking and instilling fear upon non-combatants.

**Implications of a "War on Terror"**

Consider the following: conventional warfare employs violence as a means to an end but the ways are determined by leaders, whereas terrorism is the infliction of fear and violence as the ways that all means will be brought to bear to achieve the ends. Therefore*, inflicting terror itself is a component of the desired endstate*, regardless of other considerations such as non-combatant status. Terrorism is a fear inspiring tactic that must be countered, not an enemy that one might defeat with force. Of the numerous definitions of war, the majority contain specific elements such as identifying the belligerents, the use of arms or violence, and an overall purpose or objective. For example, a typical encyclopedia definition of war explains it as:

> *[A]rmed conflict between states or nations (international war) or between factions within a state (civil war), prosecuted by force and having the purpose of compelling the defeated side to do the will of the victor. Among the causes of war are ideological, political, racial, economic, and religious conflicts.*[13]

The use of the word "war" in reference to a war on terror rather than a chosen enemy is essentially metaphorical to underline a resolve and rejection of any type of acquiescence. It expresses a conviction that terrorism is as destructive as war and the resolve to fight those responsible no less than wartime enemies. This has become problematic

because the use of the word "war" has gone far beyond metaphor to acquire a strategic reality.[14] The issue with automatically identifying terrorism with war is multi-fold. First, terrorism is not an enemy, it is a tactic. Second, the use of the term "war," legitimizes terrorists. It also allows them to conjure images of the crusades and colonialism. It permits radicals to twist Western actions into a war against Islam. An additional problem with the term "war" is that it is a reciprocal process: if you are at war with someone, then he is at war with you. As a result, the state of war confers a degree of common dignity on the belligerents, as well as certain rights, even if the belligerents do not abide by those rights.[15] Recognizing terror as a tactic, it then remains that an enemy must be identified. The Bush and Obama administrations, while fighting simultaneous insurgencies, struggled with specifically defining the "terrorist" enemy.

The enemy has grown from al Qaeda, Hezbollah, Hamas, Iraqi insurgents, Taliban, radicals in Pakistan and others to become subsumed into a single monolithic entity.[16] Unfortunately, this afforded great latitude for others to dictate who the enemy is, or more significantly to cloud what, or who the true enemy is. Al Qaeda presents the greatest transnational terrorist threat to U.S. interests in the near term, but rather than identifying a particular movement, the War on Terror was expanded beyond al Qaeda. By portraying the enemy in the context of global terrorism, the perception served to coalesce Islamic extremism writ large as a unified adversary, when previously it had been marked more by its schisms than its unity.

By properly identifying the enemy, one is better able to devise strategies to defeat that enemy; whereas, strategies to defeat a tactic will only alter the tactics and fail to produce a true endstate. The adversary will adapt but will not be defeated. By defeating the adversary, the tactic is rendered useless. In the sense that most western thinkers define war, end goals and aims constitute another dimension when dealing with terrorism. In the Westphalian system, states employ diplomacy or force to effect political or economic change. This is not necessarily true for all terrorist groups, whereas terrorism is not the means to the end, but the end in itself.[17]

A major distinction to be made in the discussion of warfare is to address a fundamental misunderstanding and intermingling of terms

such as guerilla warfare, insurgency, irregular warfare and terrorism. Insurgencies and guerilla wars are fought to achieve political objectives. Although their tactics may include unconventional warfare or terrorism, the use of force is the means to achieve political ends and asymmetric methods or terror are ways that an insurgent force or guerilla army might bring that force to bear. The ways and the means are not necessarily one in the same.

The confusion surrounding terrorism is exacerbated because activities we commonly associate with terrorism appear to bear many similarities with the forms of guerilla warfare. Such activities may, for the political actor who employs such tactics, possess many of the same objectives such as aiming to force the adversary to negotiate favorable terms.[18] It is also true that terrorism can form an adjunct to a number of so called unconventional practices of war. Yet there are distinct differences between guerilla warfare and terrorism, and it is important not to describe all insurgency warfare as terrorist in character.[19] As terminology and concepts are convoluted, the most significant nuances are lost. For instance, one might wage war against an insurgent group or a guerrilla army and deny their aims by militarily defeating their forces or negotiating a truce, in effect achieving victory. However, a war waged on terror defines the adversary by the tactic, distances strategy from objectives and distorts the focus from defeat of the enemy to extinguishing an ideology. State support for jihadist groups such as al Qaeda has essentially vanished. Rather than maintain territorial sanctuaries, such groups have melted away into their host societies to a point where "war" is both infeasible in practice and analytically misleading.[20] Within this framework, policy and strategy are unlikely to produce decisive victory when there is no military center of gravity to mass forces against and there is no distinguishable disposition of forces to be attacked.[21]

The basic argument for containment is twofold. First, a war on terror is misguided and is more a reaction to the environment rather than an effort toward shaping the future environment. Policy should ensure that strategy pursues appropriate aims, while strategy informs policy of the art of the possible.[22] Second, if the national interest and objectives are to combat terrorism, their achievement requires using all instruments of national power, guided by the direction of a clear policy supported

by a grand strategy to meet the national aims. This includes the use of force where appropriate, but force is best directed against a tangible enemy rather than ambiguously defined threats. Force alone has negligible impact against ideology, but the combined effect of national power has the capability to contain large-scale movements.

Declaring terror as an enemy creates frustrating non-sequiturs, but it also obfuscates a fundamental understanding that must be achieved prior to embarking upon war. Political and military leaders must understand the type of war they are fighting. As Carl Von Clausewitz said:

> *The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature. This is the first of all strategic questions and the most comprehensive.*[23]

It is in this endeavor that the United States would have been wise to consider the implications of waging war against a tactic that is so complex that it defies common definition, so widespread that it inspires enemies and sympathizers to multiply and splinter into indiscriminate factions, and so ambiguous that neither the enemy nor the battlefield is readily discernible. In this type of fight, defeat is much more measurable than victory.

**Reshaping the Understanding of the Problem**

It has taken years to recognize the power of the words that built policy, but it appears that the U.S. leadership is realizing that a new mindset is necessary to combat terrorism. In March of 2009, the Obama administration announced that the term "Global War on Terror" would be dropped in lieu of "Overseas Contingency Operations."[24] This announcement was made with little fanfare, but it punctuated a notable shift that began late in the Bush administration from the terminology that critics claimed, including some within the U.S. military, mischaracterized the nature of the enemy and its abilities. For example, some military officers said that classifying al Qaeda and other anti-American militant groups as part of a single movement overstated

their strength. John A. Nagl, the former Army officer who helped write the military's latest counterinsurgency field manual, criticized the term "war on terror" when he said it:

> *...was enormously unfortunate because I think it pulled together disparate organizations and insurgencies. Our strategy should be to divide and conquer rather than make of enemies more than they are. We are facing a number of different insurgencies around the globe – some have local causes, some of them are transnational. Viewing them all through one lens distorts the picture and magnifies the enemy.*[25]

Nagl's point is insightful; however, not all insurgencies are terrorists in nature and not all terrorism is the result of insurgency. Unfortunately, the two protracted insurgencies in the Middle East have created a myopia that blurs this distinction, while radical Islamism requires a much broader discussion than simply a collection of insurgencies. The significant difference between an insurgency and a terror campaign is that terrorist tactics are applied to non-combatants.

If not through a war on terror, then how might the United States effectively combat terrorism and achieve national security objectives? Clearly identifying and understanding the problem is a good first step and secondly it is necessary to fully understand the threat. Nations have been increasingly preoccupied with devising strategies to defeat terrorism. Where these strategies fall short is that they focus on the symptom vice the cause of terrorism; that is, they are transfixed on the violence. In some ways, these strategies are well founded and practical. By many definitions, terrorism is a crime, and commission of a crime invites justice upon the perpetrator. Retaliation and use of force has a significant deterrent effect against those that would take human life and inflict severe mental distress on those deemed to be "innocent."[26]

But again, it addresses only the symptom. For many, this introduces the intrinsic ethical dimension to terrorism which raises questions relating to concepts like "Just War," and non-combatant immunity, but from which a source of much debate and definitional difficulty arises.[27] The threat of, or the actual use of force is a valuable tool in the arsenal to combat terror, but it is not the only one. Effective instruments against terrorism address root causes, not just the symptoms.

## Determining the Underlying Causes

Terrorists are generally driven to commit acts of terrorism due to a variety of factors, whether rational or irrational, in which extreme forms of violence are used to express specific grievances and demands. Root causes are the factors and circumstances underlying movements that radicalize and drive terrorists into carrying out violent actions.[28] One underlying cause is the people's struggle against a corrupt or oppressive government. This generally involves non-state actors seeking to achieve their political aims primarily through terrorist violence. The wars in Iraq and Afghanistan began as operations to remove repressive regimes and were generally well received by the population initially. However, the formation of new regimes did little to improve the basic condition of the battered societies. The inability of new governments to ameliorate grievances and provide security and basic services enabled radicals to exploit social dissatisfaction within the transforming environment and shift momentum against the United States. Meanwhile, groups mobilized resistance against the new governments and security forces utilizing a common tactic of a weaker force versus the stronger – terrorism. The removal of the Taliban and Saddam Hussein regimes failed to address the underlying societal needs, but rather, exposed the condition of marginalized people responding to ideologies that promise deliverance from their miserable circumstance.

Misreading the environment is understandable given the complexities involved, but successful policy is dependent on sorting through those complexities to get it right. The environment has an unforgiving propensity to penalize bad reads. Afghanistan and Iraq are instances where terrorist tactics and insurgency tend to be incorrectly homogenized because the fight is characterized by conventional and unconventional forces versus embattled governments engaged in a counterinsurgency campaign. Strategist Colin Gray observed a similar trend with the Vietnam War:

> *…the U.S. strategy bore the hallmarks of counter-insurgency faddism that was naively captivated by the "cult of the guerrilla" and the aura of Special Forces. The resulting preoccupation with military technique came at the expense of the acute appreciation of the social and political conditions stoking the violence, causing, in particular, the weakness and corruption of the South Vietnamese*

> *state to be overlooked and the populist appeal of the elements of the Vietnamese communist message to be misunderstood."* [29]

In other words, the military and the policy makers misread the environment in Vietnam, and therefore, did not understand the problem. The lack of attention to the political and social conditions led policies and strategies to be built on flawed assumptions designed to curtail the violence or protect the population but did little to strike at the basic motivation of the adversary or their networks.

Examination of the social condition in the Middle East reveals strong doubts that the United States and to some extent, Europe, is serious about democracy in Muslim countries. Western influence has been undermined by what is perceived to be a double standard in promoting democracy. The United States and many of its allies have a long record of supporting authoritarian regimes and failing to produce democracy in the Muslim world as they did in other regions after the fall of the Soviet Union. As former Ambassador Richard Haass acknowledged in a speech on December 4, 2002: "[T]he U.S. government has for decades practiced "democratic exceptionalism" in the Muslim world, subordinating democracy to other U.S. interests such as accessing oil, containing the Soviet Union, and grappling with the Arab-Israeli conflict."[30]

Without overstating the case, democratic exceptionalism disadvantages the United States as it wages an opposing battle for the hearts and minds of Muslim people courted by the radical extremists that tap an overwhelming source of moral and spiritual support from marginalized sectors of the Middle East. In this context, it is important to distinguish that while we face a global transnational extremist movement, it is one that is often triggered and fed by local conditions and difficulties that have little to do with the West. By failing to appreciate this point, we are likely to focus unduly on the idea of an all-embracing Islamic identity shared by our adversaries that would miss the nuances of their sectarian, ethnic, linguistic or tribal identities and differences.[31] Widespread disenchantment in the Middle East does not cause terrorism, but it provides fertile ground for terrorist actors to radicalize, recruit, seek funding and operate.

American intervention in the Middle East has stoked tremendous resentment and inspired Muslims to take arms in a sacred cause to battle Western occupation of the Holy Land. This conflict has given rise to a view that violence is the only language the terrorist understands. However, meeting force with force is problematic when the objective of the terrorist is to perpetuate violence as a means to achieve their aims. Al Qaeda mastermind Abu Musab al-Suri noted that the jihadi movement has metastasized into a self-sustaining movement in which battles and bombings are more important as a means for recruiting and radicalizing a new generation of followers than as a means to a political end.[32] This underscores the impact of using religion to radicalize and incite violence. Throughout history close ties between religion and politics have existed in societies and leaders have used religion to recruit members, to justify their actions, and to glorify fighting and dying in a sacred struggle.[33] Separating religion from violence is an essential component to a solution.

The debate about the centrality of religion to radical Islamist ideology reveals that while religion is an important motivator in the radicalization process,

> *it is also being used to legitimate a very specific worldview that has been shaped by many factors external to Islam, such as a general sense of anger and humiliation (which radicals can tap into) in reaction to events of foreign origin over which they have no control. At the same time, domestic problems in Egypt, Saudi Arabia and other Muslim countries can feed that dissatisfaction and engender support for radicalism.*[34]

## Objectives and Strategy of a Terrorist Movement

The most significant transnational terrorist threats today are intertwined with Islamic extremism. The rationale of Islamic extremism is often viewed too narrowly as a religious movement, but it goes beyond that. Islamic extremists seek power, social change, control over laws and the authority to dictate how society will conduct itself. Islamic extremism manifests itself in the form of Jihad or "struggle." Although the term has been corrupted from its original context that describes the struggle to be a good Muslim, the concept of Jihad is a coalescing factor that extremists leverage to fuel their movements. In its purest

sense, Jihad is a peaceful, noble, internal pursuit of wholesomeness. In the extremist context, it expands the concept of struggle to take an outward manifestation of violence to achieve its ends.[35] It is in this context that the Jihadist ends align with the ways (terror tactics) to manifest violence as the means to overcome the struggle. Jihad in and of itself is not terrorism, but terror is the preferred tactic of the Jihadist.

Al Qaeda plays a leading role in a larger political and military movement called "global jihad." Global jihad is an extremist splinter group within Islamism, a broad religious movement that seeks to instill a stricter observance in politics, economics, and society.[36] Al Qaeda has codified their objectives into long and short-term goals:

> *[T]he movement has a number of short-term aims including the eviction of foreign forces from the Islamic world, and the termination of corrupt and pro-Western regimes in countries such as Saudi Arabia, Egypt, and Pakistan and a number of others that form a cluster termed "the near enemy." They also bitterly oppose the state of Israel. All of these are short-term goals, but still measured in decades rather than years – much longer than typical Western political timescales.*[37]

For al Qaeda, the ultimate long term goal is the establishment of a new state, or global caliphate.[38] The political and physical form of the caliphate starts with a collection of like minded Islamic emirates, or mini-states that are not necessarily organized under one leader or government. This forms the basis for the true Islamic caliphate, a single political entity governed as the Prophet guided the early Muslim peoples.[39] Extremists view the U.S. policy of promoting democracy in the Muslim world as another assault on Islam. Global jihadis oppose secularism in any form: democracy, nationalism, communism, and any other un-Islamic system or philosophy.[40] The establishment of a caliphate is a goal requiring generations of struggle and it also pits the Muslim world against the non-Muslim world. For this reason, some believe the Muslim world to be at war with the West, which is as inaccurate and distorted as equating the GWOT to a war against Islam. The majority of Muslims do not support al Qaeda and Islamic extremists are in the minority.[41] In fact, a Gallup World Poll found that:

> *[B]oth politically radicalized and moderate Muslims admire the West's fair political systems – democracy, respect of human rights, freedom of speech, and gender equality. Looking at their own countries, a significantly higher percentage of the politically radicalized (50 percent versus 35 percent of moderates), contrary to popular belief, say that "moving toward greater governmental democracy" will foster progress in the Arab/Muslim world.*[42]

This research indicates that extremists, in zeal to pursue their agendas, are also guilty of failing to understand the environment and address the underlying causes of a frustrated, angry, and marginalized people from whom they hope to draw support. One of the complexities of extremism is that many of the terrorists are drawn from the resident population they seek to assail. Among the many advantages this affords, it enables groups like al Qaeda and the Taliban to melt away into society to avoid military defeat.[43] This phenomenon also presents flaws in the extremist movement that the United States has yet to fully exploit. Radical ideologue Abu Bakr Naji raised concerns about clerics challenging the legitimacy of the movement and siphoning off recruits, excessive use of force against fellow Muslims, and similar to the 9/11 attack, targeting the wrong people at the wrong time would turn the masses away from the movement.[44] Al Qaeda associate Abu Mus ab al-Suri, an astute observer of Western strategic thinking, worried that jihad had failed in the past because it ignored ethnic minorities, failed to keep clerics involved, and propaganda threatened the legitimacy of the jihad movement.[45]

In his call for "holy war," Osama Bin Laden has argued that the Muslim world was subject to aggression from a host of enemies to include Jews, crusaders, Western society and the "apostate" governments of the Arab world. His dictum for the violent emancipation of Muslims all over the world knows no boundaries.[46] Extremists, in declaring "jihad" against all that do not practice their militant beliefs have united these disparate enemies against them. Just as the specter of a GWOT created a polarizing consequence, the rhetoric of militant jihad casts the enemy as a broad cooperative entity. This effect has unified disparate parties and provided them with a cohesive purpose to oppose extremism with the combined might of their assets and collective will.

**Recommendations for a New Course**

An effective U.S. counterterrorism effort should begin with more enlightened thinking to understand the multi-dimensional complexities of the environment. New policies and strategies ought to shape the environment over generations rather than reacting to it in the near-term. Addressing the wider global issues has greater effect in countering terrorism than wielding military might to crush it as it materializes. The instruments of national power have been applied disproportionately to the problem and must be brought into balance in order to undercut support for extremism and provide viable solutions.

In attempting to determine the nature, cause and sources of the terrorist threat, the United States has been hampered by binary thinking:

> *Western thought views things as black or white, good or evil and us and them. Thinking of terrorism simply as evil does not provide a useful understanding of the enemy and this vagueness blurs the strategy. Thinking in terms of complementary opposites, for example, there is no day without night better illustrates the yin and yang of concepts that are not separate, but are two parts to make a unified whole… defining radical Islam as an ideology of hate is a binary view that implies that extremists can only explained as the opposite of peaceful, loving and law abiding.*
>
> *This obstructs an understanding of why Muslims would sympathize or support al Qaeda… an ideology that appeals to things they value most – God, Islam, their brethren, justice and honor.*[47]

Appreciating the duality in the nature of the problem is important in stemming the tide of extremism. Resentment of the West or the pursuit of religious purity does not make one a terrorist. They represent but a few layers of underlying causes that must be understood and addressed to prevent adoption or support of terrorism. Policies should seek a middle ground, not an either-or type of solution. The Palestinian problem has long been a lightning rod of Muslim-Western tension, with the United States being more sympathetic toward Israel at the expense of Arab states. A more moderate stance on the Arab-Israeli conflict is paramount to improved Muslim relations with the West and channeling the anger and humiliation it inspires into more constructive discourse. Notably, the United States has played a significant role in

Middle-Eastern politics, and as a major actor, is held liable for political defects.[48] Aggressive multi-lateral engagement encouraging Middle-Eastern governments to enact progressive reform is necessary to reduce the political repression, and ameliorate the stigma of democratic exceptionalism to enhance America's image. There is also a need to push the jihadists into defending themselves, and answer the question of what precisely they have done of late to help solve the problems of Iraq, Afghanistan, or Pakistan. Keeping the pressure on in this way could go a long way toward publicizing the Islamists' lack of vision.[49]

Terrorism is not a new phenomenon; if it was born as a last resort instrument of politics for the out-group, then creating new political outlets for terrorist groups may possibly assuage them. Offering political alternatives as part of a containment policy makes terrorist acts less attractive and potentially forces terrorism into a dormant state.[50] As the United States seeks international cooperation to advance its security agenda, a shift from preemption towards containment is likely more accepted and falls well within the norms of international law and consequently generates greater support.[51]

Regardless of the motivation or justification of the U.S. incursions into Afghanistan and Iraq, those wars have global implications and must be fought on their own merit to national strategic objectives. Each represents regional security and foreign policy interests and do in fact play a part in combating terrorism. Abandonment or defeat would provide a tremendous boost to extremist worldwide and leave the region vulnerable to chaos. Neither conflict provides an avenue to strike a decisive blow against terrorism; however, successful outcomes may result in local stability and improved security in one of the world's most volatile regions. U.S. victory is more readily attained if those wars are de-linked from a fight against terrorism and proceed with strategies to defeat the adversary they are engaged with. The United States and its allies need to pursue those operations for what they truly are; counterinsurgencies to establish governance and stability in a region of vital strategic importance to national and global interests.

Combating terrorism is like eating an elephant – it can be done, one bite at a time. It requires patience and singular purpose. A war against terror is like trying to eat a stampede; the infeasibility of the task invites the risk of being trampled by the herd. Like the metaphorical stampede,

the "war on terror" can no longer be perceived as the war to eradicate terror. Terrorism can be limited, but it cannot be eliminated by force.[52]

The United States can, however, contain terrorism through a comprehensive national strategy that leverages all aspects of U.S. power; and where necessary, that of its regional allies and partners. Policy should inform strategy and both must address the long term threat, which is measured in decades and generations, not in years. Focusing on root causes that inspire terrorist movements enables policy makers and strategists to evaluate the environment more clearly and accurately.

Terrorists have agendas designed to meet their objectives. Terrorists seek to influence policy or political outcomes in terms that are favorable to their interests. Terror is the tactic, it is not the agenda. Effective strategies neutralize the agenda rather than the tactic, by addressing underlying causes that create marginalized societies. If those root causes are not addressed, the disenfranchised Muslim populations of Europe or Africa may present the next challenge. A policy of containment offers a greater chance for success and is more likely to secure international consensus than war. Policy backed by deeds, has the potential to reduce anti-Western sentiment and improve foreign relations.

Acknowledging the distinction between the institution and practices of Islam from the radicals that practice terrorism increases the potential for cooperation and partnership between the West and the nearly two billion Muslims in the world. A smaller military footprint and the lack of spectacular battles to rally the public against would cripple the recruiting and radicalization efforts of extremists. It also frustrates the primary purpose of local jihad, which is not the overthrow of the West, but the training and indoctrination of the rising generation of jihadis.[53]

Reframing the problem reveals that containment applies a better balance of all instruments of national power in a more effective manner than a military-centric solution, and is sustainable over a longer period of time. Containment will not defeat al Qaeda, neither will the current strategy. A containment policy is more in line with the art of the possible, which is the component that strategy provides to policy. After ten years on the offensive against terrorism, extremists still plan

and attempt attacks against the United States. It is time to address the reasons why they try.

# Systems Analysis, Centers of Gravity and Homeland Security

**Lieutenant Colonel David Rodriguez**
United States Air Force

SINCE THE TERRORIST ATTACKS on September 11, 2001 (9/11), there have been more than 30 different terrorist plots foiled by the combined efforts of the United States federal, state and local governments.[1] Al Qaeda's recently foiled attempt (November 2010) utilizing cargo bombs aboard United Parcel Service cargo planes illustrates their continued intent to attack U.S. interests and an increasing sophistication in the terrorist group's targeting methodology.[2]

An analysis of these foiled plots reveals a wide array of targets to include bridges, major financial institutions, the New York Stock Exchange and various critical infrastructure assets.[3] The Department of Homeland Security (DHS) in an effort to provide security in such an uncertain environment, has aggressively instituted a broad set of security procedures aimed at providing multiple layers of protection using the capabilities of the federal, state and local governments. Nonetheless, despite DHS success in quickly establishing a robust program, improvements are still necessary.

The United States Government (USG) has adopted a war fighting posture in the battle against terrorism, and consequently the techniques utilized for achieving success in traditional campaign planning can be adapted to provide a useful mechanism for improving the nation's security. By identifying the U.S. strategic centers of gravity and incorporating a comprehensive systems assessment, a useful framework can be added to the existing DHS toolkit for identifying critical targets and conducting comprehensive analysis of the risks posed by terrorist groups such as al Qaeda.[4]

This paper reviews the traditional center of gravity (COG) concept as espoused in the Joint Publication (JP) 5.0, *Joint Operational Planning*, and then examines Colonel John A. Warden III's theory

(Five Ring Model) of viewing the enemy as a system. Next, the existing methodology utilized by the DHS for critical infrastructure protection will be reviewed, followed by a discussion of how an adaptation of Warden's Five Ring Model can be used as a viable framework to assist in a more comprehensive risk assessment methodology. Finally, a hypothetical scenario will be offered to illustrate the value of systems thinking in homeland security.

## A Persistent Terrorist Threat

Although the security measures the USG installed following the 9/11 attacks have been successful in protecting the United States from subsequent attacks, it is not altogether clear that the existing methodology adopted by DHS is sufficiently forward looking regarding new and emerging threats.[5] The most recent National Intelligence Estimate continues to identify al Qaeda and its affiliates as a persistent threat against the United States and its interests.[6] Since 9/11, the panoply of security measures instituted were a reaction to an existing and known threat, but al Qaeda has continued to adapt and evolve while still being able to recruit new members worldwide.[7]

Homeland Security Secretary Janet Napolitano has publicly articulated in a DHS report her belief in an increasing homegrown terrorist threat to include returning U.S. veterans, which if accurate, poses an even more difficult security challenge.[8] In either case, the reported threat from both external and internal terrorist groups continues to pose a serious challenge to DHS security planners. Within this context of a persistent threat from terrorist groups and the increasing attempts by terrorists to cause death and destruction in recent years, prudence dictates planners conduct a comprehensive review of existing security measures. Germain Difo, an analyst for the American Security Project, argues that now is the time to determine which methods have been effective, which methods are too costly, and the best way to adapt and prepare for the future.[9] Given the size and complexity of the political, economic, military and social systems in the United States, the potential targets are virtually endless. Consequently, not every target can be protected with limited resources, forcing leaders to make hard choices concerning risk management.[10] Security planners need to

adopt a methodology that produces a security structure that is not only cost effective and sustainable in the long term, but also one that can be justified to the public.[11]

**Traditional COG Analysis**

When developing a comprehensive strategy to protect the U.S. homeland, planners should consider security planning synonymous to military campaign planning. In military planning, joint doctrine requires commanders and their staff to identify and analyze adversary COGs.[12] A COG is defined as: "a source of power that provides moral or physical strength, freedom of action or will to act. It's what the Prussian theorist Carl von Clausewitz called 'the hub of all power and movement, on which everything depends.'"[13] One can reason that if it is good practice to identify and analyze an adversary's COGs, then it should also be good practice to analyze one's own COGs. In fact, joint doctrine specifically requires that when conducting campaign planning, the commander identify not only adversary COGs, but also friendly COGs.[14] It is this process of identifying COGs that serves as a foundation for identifying sources of power as well as sources of critical vulnerability.[15]

Adapting this COG concept to the United States for homeland security is not necessarily intuitive, however it would provide policy makers with a better understanding of the nation's power centers and apply protective resources accordingly.[16] In attempting to adapt this COG concept to the context of homeland security, one must remember that Clausewitz envisioned the enemy acting as one single entity and that by overcoming an enemy's COG, they would then collapse completely.[17] Planners must determine how the United States acts as one entity and then specifically identify the one decisive COG that once overcome, would cause the United States to collapse. Since the United States as a whole is a very complex entity in terms of governance, economic systems, military forces and national infrastructure, one has a very difficult time attempting to identify one decisive point. It is precisely at this stage in the planning process that the traditional COG framework becomes seemingly difficult to adapt for homeland security and one may be tempted to abandon further efforts. Nonetheless, Clausewitz's

theory of COG when properly applied using the enemy as a whole, or system, is still valid and applicable.[18]

**Using Systems Analysis in COG Determination**

This principle of understanding the enemy as a whole, or as a system, is the key to making the COG concept a useful tool for homeland security planners. In the case of the United States, a country composed of numerous complex systems, a more refined application of Clausewitz's COG theory is needed. Colonel John Warden's theory of viewing the "enemy as a system" and associated Five Ring Model, used during the Desert Storm air campaign, is a useful tool in the homeland security environment. Warden advocates that when thinking strategically, one must think of the enemy as a "system composed of numerous subsystems."[19] On initial consideration, one might argue using Warden's enemy as a system concept for COG determination in the United States does not apply since the situations encountered by DHS are not the same as Desert Storm. After all, Warden's Five Ring Model was the concept used for a massive aerial bombing campaign and not necessarily applicable when dealing with a group like al Qaeda that does not possess an air force. However, the utility of the Five Ring Model in determining critical targets is not dependent upon the method of ordnance delivery but rather the targets attacked.

Warden's Five Ring Model is based upon the premise that all human organizations including societies are designed similarly and share certain characteristics.[20] Warden asserts these organizations all share a leadership function, an organic essential or function that converts energy in some form; an infrastructure; a population and a defensive system of some form.[21] Graphically, these shared characteristics of a system are depicted as Warden's Five Ring Model (Figure 1).

Warden configured his base model to apply to any country by identifying the applicable system components in each ring. For leadership, the obvious component is the existing government of that country; the organic essentials would be composed of power production facilities such as electrical grids, nuclear power plants, and infrastructure correlating to bridges, railways or other key assets.[22] Warden also adapted his base model for a non-state actor such as a

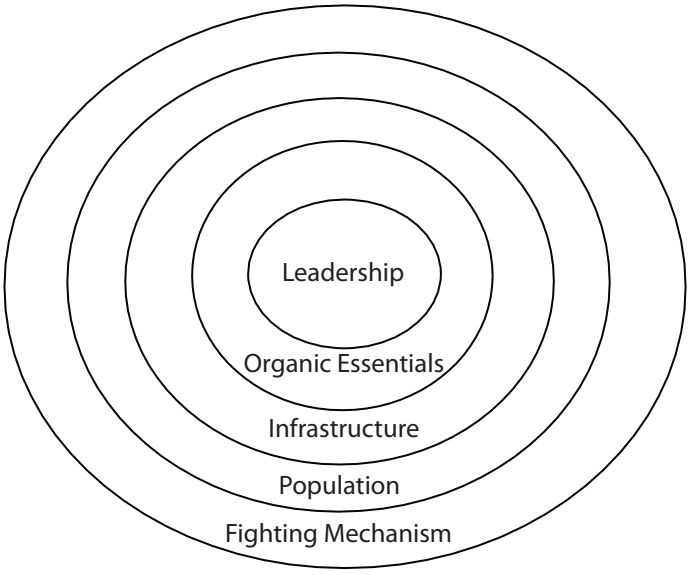



**Figure 1: Warden's Five Ring Model**

drug cartel, where the organic essential is changed from a traditional concept like a power plant to a drug processing center or laboratory and its associated infrastructure as its distribution network.[23] Using this adaptable Five Ring Model, a useful framework for identifying U.S. key COGs emerges and, more specifically, a potential framework for identifying critical vulnerabilities as well.[24]

In addition to proposing the basics tenets of the Five Ring Model, Warden and other air power theorists also advocated the concepts of strategic paralysis and parallel war. The concept of strategic paralysis is based upon an understanding of an entity as a system, composed of the five rings, where those specific parts of the system that are controlled externally and results in the system as a whole being unable to act as it wishes, or in other words, is paralyzed.[25] To achieve strategic paralysis, parallel warfare is utilized, where each major system component in each of the five rings is brought under simultaneous or near-simultaneous attack.[26] These concepts of parallel war and strategic paralysis were combined during the Desert Storm air campaign and were arguably successful in achieving the desired effect.[27]

However, in the realm of homeland security, anticipation of an aerial bombardment like the one conducted by the largest coalition of attacking forces in modern history is not likely. Nonetheless, the systems analysis methodology, the Five Ring Model, and the concept of parallel attack can be useful in refining existing homeland security strategy. When utilizing these elements, it is absolutely critical to understand the United States as an entire system, composed of various subsystems.[28]

Particularly for a complex entity like the United States, identifying COGs is rather difficult since multiple COGs will exist and they all have an interrelated impact, making it difficult to isolate one decisive point.[29] As a result of the interrelated connectivity and complexity of the U.S. homeland, terrorist attacks should not be analyzed in isolation but rather they should be analyzed in relation to the entire system and pertinent subsystems.

In conventional offensive military operations, control or damage to enough systems at the operational level can paralyze an adversary at the strategic level, without destroying the entire system.[30] In the context of terrorist attacks, one can conceive of a purposeful design to achieve a particular effect on a system rather than simple destruction of a target or the direct and immediate consequences resulting therefore.[31]

For instance, if there was a terrorist attack on the port in Long Beach, California, could the port be effectively shut down for an extended period of time without being totally destroyed? If this effect were achieved, the total economic impact would be dramatically more significant than simply the physical destruction or loss of life during the attack. The effects of such an attack would ripple through the shipping sector and any associated manufacturing sector negatively affected by a stopped or slowed exchange of goods. But what if such a terrorist attack were combined with other attacks that were nearly simultaneous, designed to disrupt various subsystems that support the U.S. economic system?

Using a systems approach provides a more complete understanding by examining the impact of the attacks on the entire economic system, not in isolation or limited to a particular sector like shipping.

Attackers can exploit the initiative by incorporating the concept of parallel war, across three dimensions: time, space and the various levels of security to include local, state and federal.[32] Defending against the threat of potential, sequenced terrorist attacks requires the same measures as defending against parallel war. These measures include the identification of the enemy's real target and better coordination of all our military, law enforcement, political and economic actors to develop a comprehensive and integrated defensive strategy.[33]

**Current Homeland Defense Security Protection Plan**

Armed with an understanding of a systems framework in COG determination, it is also helpful to understand current homeland security policies, strategies, and plans. From the outset of its existence, the DHS utilized a broad-based approach that sought to increase security awareness by making decisions about priorities that were based upon consequences, most importantly, the impact on the American population.[34] In 2006, then DHS Secretary Michael Chertoff directed utilization of a risk-based approach in making resource allocation decisions.[35] Even with a greater emphasis on risk analysis, developing adequate security measures still presented a formidable challenge in comparing threats across so many targets as well as determining accurate consequences of a potential attack.[36]

When attempting to make risk-informed decisions, there is no certain and correct method available to measure risk accurately and completely.[37] The Rand Corporation published a report in 2005 espousing a method of risk analysis that defined risk as a function of three components: threat, vulnerability and consequence.[38] Mathematically, the RAND model of component of risk is represented as: R(Risk) = T(Threat) x V(Vulnerability) x C(Consequences). This construct provides a coherent method for applying an analytical approach in establishing security measures. Given a near infinite number of possible terrorist targets, some mechanism to identify risk and allocate resources must be used.[39] Using the RAND risk framework, one can analyze each of the variables of risk to determine the overall level of risk. For instance, if the threat to a particular target has a high probability, then the level of risk is greatly increased. Additionally, the vulnerability of the target

and the consequence of the target being destroyed factor into the calculation. Unfortunately, determining the actual level of threat, or more accurately, determining the probability of an attack is difficult and often unreliable.

Intuitively, if the probability of an attack is zero, then the corresponding risk is zero. Additionally, if the consequence of the total destruction of the target is zero, then the corresponding risk is zero. More often than not however, the true risk to a target is somewhere between the extremes and deriving values for each individual risk variable is not simple. As a result, scholars in the security field, such as John Mueller from the Ohio State University, argue for security measures that overlap across the broadest potential target set possible because there is a great deal of uncertainty and variability in the component risk variables.[40] The DHS has to some extent, adopted this same approach. Beginning with the Clinton administration and its Presidential Decision Directive (PDD)-63, the protection of key infrastructure components essential to the nation was specifically designed to prevent and minimize any significant disruptions in services.[41] This was further refined by the Bush administration in 2003 with the Homeland Security Presidential Directive (HSPD)-7, where the U.S. policy was to include protection of U.S. critical infrastructure and key resources "from terrorist attacks."[42] The resulting National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (CIKA) underscored the need to develop a "comprehensive, prioritized assessment of facilities, systems and functions" for the entire nation.[43]

The Congressional Research Service (CRS) conducted a recent review of U.S. infrastructure protection measures and identified the efforts of the DHS to protect various sectors to include public health, shipping, agriculture as well as chemical facilities.[44] The CRS concluded that as a matter of policy, federal efforts should be focused toward those targets that posed the greatest risks.[45] Although seemingly obvious, previous policy documents such as the PDD-63 or HSPD-7 contained virtually no instruction regarding the incorporation of risk. Nonetheless, the basic dilemma of correctly identifying risk based on the uncertainty and variability of factors is unknowable and makes prioritization of resources difficult. Since risk measurement for homeland security is

not in the same class as auto accidents derived from reliable statistical data, determining how much to spend on protecting a potential target is still a daunting task.[46]

So how much should the taxpayer be willing to pay to mitigate risk on potential terrorist targets, especially when the probability of an attack is widely variable?[47]

Reportedly, the DHS spent 34% of its budget on lowering the vulnerability of potential targets.[48] In the DHS risk analysis equation of R(Risk) = T(Threat) x V(Vulnerability) x C(Consequence), the DHS has, in essence, opted to reduce the one variable it can quantifiably control, the vulnerability variable (V). The risk analysis methodology employed in practice in essence becomes: R = V x C. Hence, some security analysts argue that security measures should have a "dual or collateral benefit" where vulnerability across a broad group of targets is reduced.[49] Another school of thought in the security community advocates focusing on the worst case scenario where the emphasis is placed on the consequences of an attack.[50] According to the CRS, existing risk analysis by the DHS places an assessment of target vulnerability and consequences of an attack on an 80 point scale and then adds it to the probability of an attack on a 20 point scale (R = V x C + V).[51] In this manner, since the factors of vulnerability and consequence are added to the threat component, the threat or probability of an attack on a specific target is still accounted for but given significantly less weight. Taken to the extreme, the threat factor (T) to a target can be zero, but the assigned risk factor can still considered relatively high, leading policy makers to allocate resources to protect it.

The most recent National Infrastructure Protection Plan (NIPP), released in 2009, champions the utilization of a risk analysis that combines the factor of threat, vulnerability and consequence information as a function where R = f(C,V,T).[52] In fact, the new NIPP significantly expanded the discussion of risk analysis and advocated the use of cross sector analysis to measure impacts across various critical infrastructure sectors.[53] While these modifications by DHS in its methodology more closely approach a comprehensive systems approach, it still falls short. For instance, the updated plan is still focused on an "asset, system, network or functional basis, depending

upon the fundamental characteristic of the individual sectors."[54] As a result, this approach does not begin at the highest level, starting with the nation as a whole system or with the economic system as an integrated whole, composed of numerous sectors. The current DHS plan allows for systems consideration but only specifies sector systems such as communications and informational technology systems, indicating that the strategy still does not consider an assessment of the entire economic system and is limited to particular infrastructure subsystems.[55]

This methodological limitation manifests itself in the assessment of risk by not accounting fully for the potential consequence of attacks or parallel attacks. The NIPP divides consequence analysis into categories of population impact, economic impact, and psychological impact as well as governance impacts.[56] Specifically, the economic consequences are calculated based upon damage to infrastructure with respect to physical asset destruction, with a focus on the, "cost to rebuild asset, cost to respond to and recover from an attack, downstream costs resulting from disruption of product or service…."[57] This construct does not incorporate any possible synergistic effects resulting from parallel, system-designed attacks aimed at a higher, national level effect, such as the overall economy of the United States. Even the fifteen National Planning Scenarios call for a governmental response that deals with the impacts of a specific type of attack.[58] None of the published scenarios contain a methodology where shocks are combined in multiple, cross-attack scenarios to obtain a desired effect on a national system such as the American economy. Even if multiple, simultaneous natural disasters are assumed to be rare, this does not account for a combined natural disaster and one or more terrorist attacks. The DHS acknowledges in its most recent NIPP that "nearly all sectors share relationships with elements of the energy, information technology, communications, banking and finance, and transportation sectors," but it still does not directly discuss how to consider or measure sector impact on the overall economic system.[59]

Additionally, the USG established the National Infrastructure Simulation and Analysis Center (NISAC) to provide advance modeling of simulated attacks and provide data on their associated impacts

on the nations critical infrastructure, measured in terms of their "dependencies and interdependencies," but there is no indication the focus rises above the infrastructure asset itself to the overall economic system of the nation.[60] The initial National Asset Database last updated in 2006 had more than 77,000 entries of key national assets identified for some measure of protection.[61]

Lastly, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* acknowledges terrorists "may choose to target critical infrastructure and key assets as low-risk means to generate mass casualties, shock and panic."[62]

However, what is not addressed is that terrorists may also choose to attack critical infrastructure targets and key assets for a broader, more strategic effect. Terrorists may choose to attack a national COG such as the U.S. economic system, and terrorists may use a systems approach combined with parallel attacks. Thus far, neither USG policy nor security planning seems to incorporate a comprehensive systems approach.

**Indicators of Growing al Qaeda Sophistication**

The current conventional wisdom concerning al Qaeda's targeting indicates a propensity to select targets with a high population density to achieve a desired effect, cause disruption and display a symbolic consequence.[63] But will this existing propensity always be the standard? Since it is also commonly understood that the 9/11 attacks were highly sophisticated and involved numerous targets, attacked nearly simultaneously, why should one reasonably expect al Qaeda to continue using the same targeting methodology? Al Qaeda has already demonstrated a willingness to conduct extensive research and pursue creative operational capabilities such as learning to pilot commercial aircraft.[64] When considering future attacks by al Qaeda, the National Security Council has reported that al Qaeda is aggressively pursuing weapons of mass destruction (WMD) such as nuclear devices or chemical and biological agents.[65] If al Qaeda is successful in employing weapons of mass destruction, then the previous targeting methodology is not necessarily limited or necessarily required. Although the USG

has fielded a more robust system of security since 9/11, utilizing a systems framework can assist in anticipating al Qaeda targeting.

On what basis should we expect al Qaeda's targeting to diverge from traditional high population, maximum disruption targets? The U.S. Secret Service has conducted research revealing that when conducting threat assessments, "all targeted violence is the result of an understandable and often discernable process of thinking and behavior."[66] Additionally, the Secret Service discovered that individuals who committed acts of targeted violence also demonstrated a pattern of certain behavior before the event.[67] A review of foiled al Qaeda attacks and plans has shown methods that include assassination attempts on governmental officials, attacks on infrastructure to include nuclear power plants, financial centers, refineries and even military bases.[68] Al Qaeda also exhibited these behaviors to included communication about specific organizational intent.[69]

In a review of public al Qaeda communications, security officials acknowledge that al Qaeda has designs on "crippling our economy" but these same officials boldly claim, "no enemy of the U.S. should think a city or region can be put out of business."[70]

However, a survey of existing literature on the intentions and designs of al Qaeda reveals a "coherent long-term strategy" depicting the organizational struggle in terms of "economic war."[71] More striking is Abu-'Ubayd al-Qurashi's claim, a jihadist leader and aide to Osama bin Laden, who declared: "It is clearly apparent that the American economy is America's center of gravity…aborting the American economy is not an unattainable dream."[72] What is particularly striking is not just the emphasis on the U.S. economy as the target, but rather the terminology used – Center of Gravity. This is not a term used in common parlance, but indicates a certain familiarity with military concepts. One security analyst reports al Qaeda makes "strategic decisions with detached, methodical precision, constantly assessing alternative approaches as well as seeking additional means or methods."[73] Al Qaeda's familiarity with military concepts combined with a tendency to adapt organizational behavior means that anticipating a more robust understanding of COG analysis by al Qaeda can prevent a strategic shock. In fact, the incorporation of systems analysis and COG determination is explicitly

and widely available in JP-5.0, via the internet.[74] Such a methodology of anticipating target selection by past behavior and communicated intent is in keeping with research conducted by the U.S. Secret Service. Consequently, it is not necessarily a stretch to think that al Qaeda's strategy may evolve as they attempt to accomplish what they propose publicly and vociferously.

**Extrapolation from the 9/11 Attacks**

The attacks of 9/11 were reported to have resulted in the loss of over one million jobs and caused a three percent drop in U.S. Gross Domestic Product (GDP).[75] A CRS report claimed the direct effects of the 9/11 attacks were not significant enough to cause a long-term economic impact to the nation as a whole.[76] Although the specific macroeconomic impact is not concretely identifiable due to the economy previously beginning to show signs of slipping into a recession, it is difficult to deny the attacks had a large, negative effect on various economic sectors such as the aviation industry and the local economy, particularly the city of New York. Even though the CRS report dismissed the long-term macroeconomic effect of the 9/11 attacks, many economists believe the attacks had a detectable, negative impact on the U.S. economy at the macroeconomic level in the short term.[77]

Nonetheless, the CRS provides a "blue print" for what an attacker needs to do to have a significant macroeconomic impact. Specifically, the CRS states an attack would have to cause major indirect effects, principally in the areas of consumer confidence, a form of financial panic that leads to decreased foreign investment and increased spending on security, as well as introduce a price shock via energy costs.[78] The CRS report also noted that in times of international crisis, investors typically seek safety for their assets in the United States. However, in the instance of the 9/11 attacks, the international crisis was occurring in the United States. Consequently, there was a "short run decline in the net purchases of U.S. assets by foreigners."[79] Although there was no panic selling and no run on the dollar after the aftermath of the 9/11 attacks, all trading of U.S. Treasury securities was stopped for two days, and the stock market was closed for six days.[80] As witnessed during the recent mortgage and banking crisis leading to the current

U.S. recession, the role of the Federal Reserve in preventing a complete financial collapse was instrumental. The same was true after the 9/11 attacks, when the Federal Reserve issued the following statement: "The Federal Reserve System is open and operating. The discount window is available to meet liquidity needs."[81] The CRS report credits this action by the Federal Reserve with prevention of a potential financial panic. However, this particular vulnerability from the 9/11 attacks can be expanded and exploited using a parallel attack on the U.S. economic system.

Some might argue al Qaeda was only able to coordinate the 9/11 attacks as the result of luck. Perhaps luck was involved, but regardless, if al Qaeda is indeed seeking to attack the U.S. COG (economic power) as it claims, then a feasible strategy can be devised by extrapolating from existing information to achieve a devastating, direct effect on the U.S. economy. As the CRS report indicated, a parallel attack to achieve a desired negative macroeconomic effect would need to achieve a loss in consumer confidence, a financial panic that leads to decreased foreign investment, and a price shock by way of increased energy costs. Adapting Warden's Five Ring Model as previously discussed, and the concept of parallel attacks, al Qaeda would need to attack economic leadership, economic organic essentials, key economic infrastructure, the population and defensive system.

Specifically, Warden's Five Ring Model can be adapted to show a crude methodology that could be used by an attacker, based upon the requirements outlined by the CRS report to inflict damage on the U.S. economic system.Although this type of attack involves more complex planning, the attacks do not need to be a precision operation occurring at the same time, but can be near-simultaneous to have the desired effect. Various attack methods could be combined that have already been used or have been planned for use by al Qaeda. For instance, al Qaeda has previously attempted to use political assassination, hybrid vehicle-bombs, shoulder fired anti-aircraft missiles and planned to acquire and use WMD.[82] These foiled terrorist attacks illustrate a propensity by al Qaeda to attack significant targets that individually, could have a large economic effect. If the individual attacks were conducted in parallel

specifically intended to disrupt the economic system of the United States, the indirect effects could be catastrophic.

| **Warden's Five-Ring Model** | **Adapted Construct** |
|---|---|
| Leadership | Assassination of the Federal Reserve Chairman and the Treasury Secretary |
| Organic Essentials | Cyber-attack(s) on the U.S. financial system and New York City (Manhattan). |
| Infrastructure | Exploding a WMD (Dirty Bomb) at major shipping port, U.S. oil refineries or electrical grid. |
| Population | Random attack(s) on airport terminal or subway. |
| State/Local Security Network | Attack(s) on first responders. |

**Table 1.**

In this hypothetical scenario, the first and most difficult task involves an attack designed to affect the leadership of the U.S. economic system. In this case, it would involve the assassination of the Federal Reserve Chairman who is appointed to his position by the President of the United States and confirmed by the Senate. Replacing the Federal Reserve Chairman could be done in an expeditious manner following an emergency. Unfortunately, the new Chairman certainly would not inspire the same level of confidence to foreign investors when assuring the market of an ability to meet liquidity needs following a successful assassination. This particular scenario is not far removed from the reported planned attempts of Khalid Sheikh Mohammed to assassinate Pope John Paul II and former President Bill Clinton.[83]

Second, a cyber-attack on the U.S. financial banking system would affect the organic essentials or second ring of the U.S. economic system. The U.S. Secret Service in a study of potential cyber threats determined, "most incidents required little technical sophistication" and were conducted easily by inside employees.[84] Such a direct attack to the financial system or even an indirect attack similar in scope to a

Wiki-Leaks disclosure may compromise consumer confidence to such an extent the entire financial system might be paralyzed.

A third attack to the third ring or economic infrastructure could be utilized to further erode consumer confidence by negating the use of a U.S. major shipping port or power generation plant. A 2002 west coast longshoreman strike was estimated to potentially cause $19.4 billion in economic losses during a 10 day shutdown and $48 billion for a 20 day shutdown of the affected ports.[85] Aside from the direct economic impact, the potential indirect effect to the economic system as a whole must also be considered. A dirty bomb might contaminate a port access chokepoint preventing workers access for a significant period of time or affect the cargo cranes thereby severely limiting trade. This type of attack with a dirty bomb was the same method attributed to Jose Padilla during his arrest in 2002 as well as the disrupted plan involving Dhiren Baroot in 2004 against a target in the United Kingdom.[86] Additionally, an attack on an oil refinery such as the foiled plot involving Michael Reynolds who planned to destroy gas pipelines and energy infrastructure in 2005 would drive up the price of gasoline and oil. An increase in gasoline and oil prices would qualify as an energy price shock that would ripple through the economy increasing costs to businesses dependent upon any form of transportation. The CRS analyzed the economic impact on the Gulf region following Hurricane Katrina and noted there is a correlation between most recessions and higher oil prices.[87]

As for attacks on the fourth ring, the U.S. population, random attacks in malls, subways, etc., would be detrimental to consumer confidence, but perhaps not as much as an attack at a major airport terminal. Since most of the Transportation Security Administration (TSA) security and screening is geared for protecting the airplanes from being hijacked or destroyed in flight, a significant economic effect could be achieved by attacking a busy airport terminal where the ticket counters are located. An attack on a large airport terminal such as Atlanta Hartsfield or Chicago O'Hare would have an enormous impact on the entire air travel system. The airport might not be destroyed but the airport and others around the nation would be severely disrupted and possibly, temporarily shut down.

The fifth ring involves attacking the U.S. defensive system. In this example, attacks on the first responders would slow down recovery efforts, affecting governmental response to any crisis. An attack on first responders following an initial attack would add confusion to recovery efforts, exacerbate the effects of the initial attack and cause untold indirect effects.

In outlining such a hypothetical scenario, the main point is to highlight the severe impact of parallel attacks combined with a systems-designed targeting approach. This hypothetical scenario is not provided to determine the most probable method of attack or to provide a commentary on the probable next target. One should not however, given the history of al Qaeda's tendency to adapt organizational behavior, be surprised if parallel attacks are used in the future and combined with a systems approach for targeting U.S. COGs. In this hypothetical scenario, each of the individual targets selected using the Five Ring Model is based on a published, foiled al Qaeda attack. Additionally, given al Qaeda's use and understanding of military concepts, one can anticipate more sophisticated enemy thinking in the future.

**Conclusion**

By incorporating a systems approach and the concept of parallel attack to existing methodology, the DHS strategy can fully leverage their stated risk components of consequence, vulnerability and threat ($R = f(C,V,T)$).[88] Although Warden's Five Ring Model was utilized in the Desert Storm air campaign, it certainly can be adapted for use in homeland security planning. By doing so, security planners can better understand the potential consequence of multiple, critical infrastructure or key resources being destroyed or neutralized for a short period of time particularly with respect to the economy as a whole. The Five Ring Model also provides planners with a methodology for greater understanding of system vulnerability and how parallel attacks might affect larger economic systems or even the entire national economic system, transcending individual sectors. Finally, security planners can better assess targeting probabilities should al Qaeda attack the U.S. COG espoused by al Qaeda leaders, the U.S. economy. Al Qaeda has shown a keen ability to adapt and evolve, and the security community

in the United States must be able to do the same. The combination of systems thinking and parallel war can help planners more effectively secure the homeland against future attacks.

# Electromagnetic Pulse: A Catastrophic Threat to the Homeland

**Colonel Robert Oreskovic**
United States Army

IN HIS OPENING STATEMENT to the Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security on August 4, 2010, Senator Jon Kyl (Republican-Arizona), made the following statement:

> *One threat to which the government is particularly ill-equipped to respond is the threat posed by an electromagnetic pulse or EMP attack. When a nuclear weapon is detonated hundreds of miles above the earth, the resulting radiation would interact with the Earth's atmosphere to produce an electromagnetic pulse. The resulting EMP waves would cause severe damage to electronic devices and just a single weapon could affect much of the United States. People aboard planes and those on life support systems at hospitals would be the first casualties. However, without power for medical care, food refrigeration and water purification and delivery, the death toll could climb to staggering proportions.*[1]

Dr. Peter Pry is president of EMPACT America, a bipartisan non-profit organization concerned with protecting the United States from a nuclear or natural electromagnetic pulse (EMP) catastrophe. He was also a charter staff member of both the 2004 and 2008 congressionally mandated commissions chartered to study the EMP threat. Dr. Pry stated "based on eight years of research and analysis, 50 years of data from nuclear tests and EMP simulators, and never-before-attempted EMP tests, the commission found that any nuclear weapon, even a low-yield one, could potentially pose a catastrophic EMP threat to the United States, mainly because of the great fragility of the electric grid."[2]

All modern societies are dependent upon electrical power to function. The long term loss of electric power would have cataclysmic consequences on the welfare and survival of the residents of the United States. Our

modern society is not structured or resilient enough to meet the needs of its population without electricity. A full-up electrical grid is necessary to run the infrastructure of the country, from sustaining water supplies, food production, processing of waste, providing heat for warmth and cooking, providing cold for food storage, telecommunication, and for essential transportation and distribution of goods. The electric power grid is singularly the most vulnerable component of our infrastructure to an electromagnetic pulse type attack or event. Such a strike could destroy our electrical power grid for years, and it is estimated that within one year up to two-thirds of the population would die from starvation, disease, and societal breakdown.[3] The impact of EMP producing weapons or events cannot be overstated. Regardless of the debate on the level of the potential threat, the result of an attack or event would prove devastating to the Homeland.

**What is an Electromagnetic Pulse?**

In 2009 the North American Electric Reliability Corporation (NERC) and the United States Department of Energy (DOE) partnered in a study to address what they labeled "High-Impact, Low-Frequency risks to the North American bulk power system."[4]

Their report identified and explained the risks posed to the power grid from an electromagnetic pulse. According to the report, an electromagnetic pulse could occur from two principal sources. First is a manmade high altitude detonation of a nuclear weapon over the United States. The second is caused by the sun in the form of a solar geomagnetic storm. In both cases, an electromagnetic pulse is generated which could be very destructive to the electrical power grid.

A high altitude electromagnetic pulse (HEMP), caused by the detonation of a nuclear weapon well above the earth's surface, produces not one single pulse, but essentially three different waveforms pulses referred to as E1, E2, and E3. The E1 pulse is an extremely fast and brief component of a nuclear EMP. It can quickly produce very high voltages in electrical conductors which will damage sensitive electrical equipment.[5] An E1 pulse is produced when gamma radiation from a nuclear blast knocks electrons from the atoms in the upper atmosphere. The electrons travel at near the speed of light, and produce a very brief,

measured in billionths of seconds, electromagnetic pulse over a wide area. The higher the altitude of the detonation, the wider the affected area will be.[6]

A second type of pulse is labeled E2. This pulse appears a fraction of a second after the E1 pulse. The E2 has many similarities to the electromagnetic pulse produced by lightning and electronic systems normally have protection in place (for example surge protectors). But according to the EMP Commission, the potential threat of the E2 is that it immediately follows the E1. As a result devices which might normally have been protected from E2 type pulses are not because they have likely been damaged from the E1 pulse.[7]

The third form of pulse is the E3, which is very different from the previous pulses. The E3 component of the pulse is of a longer duration, and has the greatest impact on the electrical power grid because power transmission lines serve as receivers or antenna. The transmission lines absorb the E3 pulses and conduct the energy to vulnerable power transformers situated along the electrical grid. The E3 type pulse has properties similar to a geomagnetic storm which is associated with solar flares and the coronal mass ejections which the sun expels. In some cases solar storms and their E3 type waves could pose as big a threat to transformers and the electrical grid as high altitude nuclear detonations.[8] A principal reason the electrical grid is most vulnerable is the concept of "cascading failures." That is if one node in the electrical grid fails the electrical load is transferred to another node, often causing an overload of the next node in line, and so on. In an EMP situation any undamaged elements of the power grid would probably be overwhelmed causing a widespread cascading shutdown.[9]

**Historical Events**

One of the difficulties with predicting or estimating the potential effects of an EMP event is that conducting actual tests, with nuclear weapons at high altitude for example, would obviously be extremely problematic. The same is true for geomagnetic storms. It is very difficult to recreate EMP on a large enough scale to draw reliable conclusions. But history has provided us with a few historical events to learn from.

In 1962 the United States detonated a nuclear weapon about 400 kilometers (250 miles) above Johnson Island in the Pacific Ocean. In Hawaii, about 850 miles away, electronic and electrical systems were affected. Street lighting failed, circuit breakers were tripped, and telecommunication relay systems were damaged.[10] On the surface, the impact or damage appeared minor, but there were a few factors to consider. First, the 850 miles distance of Hawaii from the detonation is a significant distance. Second, the manner in which the electromagnetic pulse interacts with electrons has much to do with the Earth's magnetic field at the location of the blast. The Earth's magnetic field is much stronger in the Northern Hemisphere then it is in the middle latitudes such as the Hawaiian Islands. Thus, the electromagnetic pulse from a nuclear warhead most likely would be much stronger and have a much greater impact in the Northern Hemisphere, such as in the United States.[11] And the third factor to consider is that the types of electronic circuit board systems used today are much more sensitive and vulnerable to EMP than the solid state, vacuum tube systems used 50 years ago.

Additionally, in 1962 the Soviet Union conducted a series of high altitude nuclear tests, exploding 300 kiloton nuclear weapons at approximately 60, 150, and 300 kilometers above their test site in South Central Asia. Information is limited and most was never made public, but damage was observed to both above ground and below ground cables, fuses, and a power supply components. In fact, the EMP from the 300 kilometer test started a fire in a city power plant some 600 kilometers away.[12]

Historical examples of the effects of an electromagnetic pulse are not limited to manmade nuclear explosions. Pulses are also created when the sun has a solar flare, which results in a coronal mass ejection. According to a 2008 report from the National Research Council of the National Academies "The effects of space weather on modern technological systems are well documented in both the technical literature and popular accounts. Often cited is the collapse within 90 seconds of northeastern Canada's Hydro-Quebec power grid during the great geomagnetic storm of March 1989, which left millions of people without electricity for up to 9 hours. This event exemplifies the

dramatic impact that extreme space weather can have on the technology upon which modern society in all of its manifold and interconnected activities and functions critically depends."[13]

The largest solar storm ever documented took place in September 1859. It was crudely recorded by an astronomer named Richard Carrington. On Earth the northern auroras (Northern Lights), which are normally only seen from the Arctic Circle and above, were observed as far south as the Florida Keys and in Cuba.[14] Around the world telegraph operators received electrical shocks, telegraph paper caught on fire, and operators had to disconnect their equipment because of electrical arcs.[15] A geomagnetic storm at the level of the 1859 Carrington storm has never been experienced in modern society. Such a storm illustrates the potential threat the sun poses to the electrical grid, and ultimately the Homeland.

**The Threat from Manmade Sources (Other Countries and Non-State Actors)**

Any country with nuclear weapons and a delivery system could use a high altitude EMP strike to cripple the United States. The Arms Control Association, a national nonpartisan organization dedicated to promoting public understanding of and support for effective arms control policies, lists eight countries as currently possessing nuclear weapons. They are the United States, Russia, China, Great Britain, France, India, Pakistan, and Israel.[16] In addition, North Korea has worked steadily toward developing nuclear weapons and has conducted two known open source tests. The first was on October 9, 2006 and a second on May 25, 2009, both with inconclusive results.[17] A tenth country, Iran, is widely believed to be developing a nuclear weapon capability.

In an interview on February 13, 2011, former Secretary of Defense Donald Rumsfeld expressed his concern about the threat from an electromagnetic pulse attack from countries such as Iran and North Korea. His specific comments were "so that cyberwarfare, and electromagnetic pulses and the things that can avoid competition with large armies and large navies and large air forces clearly have leverage, an advantage. And because of that, they're attractive."[18]

What former Secretary Rumsfeld was referring to was Asymmetric Warfare. The type of tactic used in warfare when the weaker side employs unconventional means to offset the strength of the stronger side. It is widely recognized that no country or terrorist group could compete successfully with the United States in a conventional war; therefore, they would seek a method to gain advantage, or look to exploit a weakness. An electromagnetic pulse attack offers this asymmetric option.

If used, the employment of an EMP type weapon is more likely to be used by a country with a limited number of nuclear weapons, or a rogue organization or terrorist group. A high altitude EMP strike allows an aggressor to inflict long term damage to a wide area with as little as a single warhead. According to Dr. Peter Pry, president of EMPACT America, "A single nuclear weapon detonated at an altitude of 400 kilometers over the United States would project an EMP field over the entire country, as well as parts of Canada and Mexico."[19] Smaller warhead yields and/or warheads detonated at lower altitudes would still be very destructive, but to a lesser degree. Other factors related to the effectiveness of a nuclear EMP weapon are the distance from the detonated weapon, and any geographical features such as hills or mountains which may block the electromagnetic pulse. And finally, the strength of the Earth's magnetic field remains a factor, primarily because the EMP effects would be greater in the Northern Hemisphere as previously mentioned.

Another possible threat scenario could be for rogue nation(s) and terrorist group(s) to fire Scud type missiles with nuclear warheads from freighters or container ships off each coast, and a third from the Gulf of Mexico in order to inflict enough EMP damage to cover the continental United States. Simple Scud type missiles are fairly common and easily accessible.

It is acknowledged that Iran and North Korea possess a large number of missiles and continue to improve and test on the basic design. North Korea also continues to develop longer range missiles. In addition to Scuds, North Korea has developed the Nodong missile with a range of about 1,300 kilometers, a Taepodong-1 missile with a range of about 2,900 kilometers, and the Taepodong-2 with range of between 4,000

and 10,000 kilometers.[20] All of North Korea's long range missiles currently have reliability and design problems, and all must be launched from a fixed site. However, all have the potential to carry large enough payloads high enough to be used in an EMP attack.

Iran's most developed ballistic missile is the Shahab-3 with a range of about 2,000 kilometers. In September 2009 Iran successfully test fired this missile.[21] In testimony before the House Armed Services Committee on July 10, 2008, Dr. William Graham, who was the Chairman of the 2008 Congressional EMP commission, made the following statement in reference to Iran: "Iran, the world's leading sponsor of international terrorism, has practiced launching a mobile ballistic missile from a vessel in the Caspian Sea. Iran has also tested high-altitude explosions of the Shahab-3, a test mode consistent with EMP attack, and described the tests as successful. Iranian military writings explicitly discuss a nuclear EMP attack that would gravely harm the United States."[22]

**The Threat from the Sun**

According to Dr. Richard Fisher, who is in charge of the National Aeronautics and Space Administration's (NASA) Heliophysics Division, "The sun is waking up from a deep slumber, and in the next few years we expect to see much higher levels of solar activity. At the same time, our technological society has developed an unprecedented sensitivity to solar storms."[23]

Geomagnetic storms due to solar emissions have always occurred, and they are somewhat cyclical. There are two factors converging which together pose a threat to the United States. The first is that the sun is entering into period of increased solar activity. When the sun becomes more active the threat of a major solar flare with an accompanying solar coronal mass ejection is increased. The second factor is the high level of societal reliance upon modern technology. The 1859 Carrington geomagnetic storm demonstrated the power of electromagnetic pulses. In 2008 the engineering consulting firm Metatech Corporation conducted a study on the impact of geomagnetic storms upon the United States electrical power grid. The study was requested by the Congressional EMP Commission and the Federal Emergency Management Agency (FEMA). The conclusions were that severe

geomagnetic storms posed a risk of long term power outages to major portions of the North American power grid. The study's main author, Dr. John Kappenman, stated that "not only the potential for large-scale blackouts but, more troubling,...the potential for permanent damage that could lead to extraordinarily long restoration times."[24] The study also concluded that "while a severe storm is a low-frequency-of-occurrence event, it has the potential for long-duration catastrophic impacts to the power grid and its users."[25] The most significant problem is that the EMP could damage electrical grid transformers and "these multi-ton apparatus generally cannot be repaired in the field, and if damaged in this manner, they need to be replaced with new units, which have manufacture lead times of 12 months or more."[26]

**Electrical Power**

The detonation of one or more high altitude nuclear weapons over the United States, or an extremely powerful geomagnetic solar storm, would cause little physical damage to either citizens or structures on the ground. But in the case of a nuclear weapon EMP the blast would create an electromagnetic pulse which, at a minimum, would result in the overload and destruction of a significant number of electrical systems and high technology microcircuits known as Supervisory Control and Data Acquisition (SCADA) systems. SCADAs are automated monitoring and control systems which, in most cases, have replaced human supervisory control. Our reliance on SCADAs has increased our vulnerability to an EMP because, if they become disabled, no back up exists to replicate these essential functions.

The level of damage from an EMP is dependent upon a number of factors previously described, such as the height, strength, and distance from the blast. Also affecting the EMP impact is the amount of geographic shielding and the Earth's magnetic field where the blast occurred. Because of these variables and a limited amount of testing it would be difficult to accurately predict the effect of the E1, E2, and E3 pulses on individual systems, such as automobiles, personal computers, computer networks, cell phones, and radios. Therefore, for the purposes of discussing the consequences of an electromagnetic pulse, I will narrow the focus to the electrical power grid. By focusing

on the electrical power grid I will simplify the discussion without minimizing the potential effects. Electrical power is the cornerstone and foundation of our modern society. It impacts virtually all other infrastructure and services. Without electrical power almost all the tools of our modern society will eventually become useless.

The electrical power grid is a complex and interconnected system responsible for supplying electricity throughout the United States. The sources of electrical power generation in the United States are coal (45%) followed by natural gas (23%), nuclear (20%), and hydroelectric (7%).[27] A very small percentage of power is generated from "green" technologies such as wind and solar. Electricity is moved from the various power plants via transmission lines. Transmission lines are mostly above ground, but some, especially in urban areas, are below ground. Connecting the transmission lines are substations, or nodal points, where several lines meet. Within the substations there are transformers, which change the power from one voltage to another and move the electricity along the distribution system to the end user. Also located with the transformers are protective devices such as circuit breakers, meters, and data transmitting and control systems. In most cases these protective systems successfully safeguard other parts of the power grid from isolated problems such as power surges and lightning strikes.

Transformers are the critical link in the electric power grid. They are large, expensive, and custom built. None of these large transformers are built in the United States and delivery times for newly built systems under normal conditions are from one to three years. About 2,000 are in place throughout the Homeland, and only about 100 new ones are produced worldwide each year.[28]

The primary reason the electrical power grid is vulnerable to both manmade and solar electromagnetic pulses is because of long-distance and aged above ground electrical transmission lines. These transmission lines serve essentially as antenna for the pulse, especially the E3 component. All transmission lines lead to and from electrical transformers. The transformers are the key nodes of electrical power and they are the most vulnerable. An EMP strike, whether manmade or from the sun, could overload and thus burn out transformers. The

result would be that electricity would no longer be transmitted, even if the actual power source was not damaged.

In the event of an EMP event and the loss of electrical transmission most power generation plants would be shut down. But the potential risk of nuclear power deserves special mention. In March 2011 an earthquake off the coast of Japan and resulting tsunami exposed the unique vulnerability of nuclear power plants. In emergencies a nuclear power plant cannot be quickly turned off. It takes days to shut down the reactors, and during this time coolant or water must be continuously circulated to keep the core from overheating. Diesel generators, with an abundant supply of fuel, pump coolant when a reactor is being shut down and no other outside source of electricity is available. In Japan, it appeared that at least one nuclear power plant had their backup generators at ground level. When the tsunami came ashore the generators were damaged and the means to keep the reactor cores cool was severely limited. This is a possible scenario following an EMP event, because the backup generators will most likely be damaged by the EMP. Another area of concern is the cooling of spent fuel rods. Spent rods still produce heat after use and are stored in large holding tanks filled will water. Without power to keep the tanks full, the water will eventually evaporate and radiation may be released. Even with fully functional generators pumping coolant to these critical areas, the requirement to eventually refuel the generators exists.

**Logistical Impact Resulting from the Loss of Electrical Power**

The long term loss of the electrical power grid would impact all logistical aspects of our modern society. Short of total nuclear war, the loss of electricity represents the most catastrophic threat to the Homeland. Some of the most important logistical functions in which our modern society relies upon are transportation, water, sanitation, health care, and communications.

The ground transportation industry is the key logistical component of our society and economy. The level of the immediate impact of an EMP strike on cars and trucks is unknown because the scope of EMP testing on vehicles is limited. In a worst case scenario, every modern vehicle with a microprocessor would be disabled. But even if many

vehicles still functioned following an EMP event eventually they would require refueling, and without electricity existing fuel could not be pumped from underground storage tanks into vehicles. Additionally, the loss of electricity would limit the ability to move previously refined gas either by pipeline or truck. Even if other options were developed for fuel distribution, the loss of electricity would result in refineries becoming non-operative and no new fuel being refined. The ground transportation system would be severely degraded and eventually grind to a halt.

The loss of commercial trucking in particular would be devastating. According to the American Trucking Association in 2006 there were three million large commercial trucks on the road in the United States, and those trucks accounted for 69% of all tonnage distributed.[29] In addition, more than 80% of United States communities depend solely on trucking for delivery of their goods and commodities.[30] For example, most grocery stores stock less than a week's supply of food, for some perishable commodities such as milk, much less. Even if new food could be processed without electricity, it would still be very difficult to distribute. Urban areas with dense populations would find themselves most vulnerable, and very quickly run out of food supplies.

Municipal sources need electricity to both purify and pump drinking water. The loss of electrical power would almost immediately be felt in any size urban areas which rely on pumping stations to move and distribute water. Those who may live in more rural areas, with gravity fed water tower systems, would have clean drinking water for some additional time. Even Americans with private wells would be impacted because electricity is needed to run the pumps which bring the water from underground. The lack of electricity would bring our modern water drinking supply system to a halt.

Without electricity, sanitation would quickly become a significant health issue. Through the power of gravity, or by pumps, water effectively moves waste materials from businesses and homes. Pumping stations then transfer the waste to treatment facilities where the waste is processed. Without electricity, human waste removal would cease to function due to loss of water pumping (pressure) capability, and the

non-operative SCADA systems discussed earlier. Once again, those in more urban areas would experience the impact sooner.

Similar health issues would occur if trash was not removed. Uncollected and deteriorating waste products create environments for the rapid growth of microorganisms, insects, and rodents. In such an environment it is likely that varied debilitating diseases would soon follow.

The modern healthcare system needs electricity to function. Hospitals have backup generators with a varied 3 to 30-day supply of fuel. Once the fuel is exhausted our healthcare system would revert back a hundred years in techniques and procedures. Additionally, new supplies of modern drugs could not be ordered, nor even manufactured, transported, or distributed. Existing supplies at hospitals and clinics would eventually run out. As a result, the medical field would experience difficulties treating new injuries and would not be able to respond to the increased diseases resulting from lack of clean water, sanitation, and altered diets. The young and old, and those with preexisting medical conditions, would suffer the most.

Another specific area impacted by an EMP event would be that of information and communications. Imagine an environment without working telephones, cell phones, email, any commercial internet communication, or television. These systems are all vulnerable to EMP and rely on electricity to operate. Command and control at the local, State, and even Federal level would be seriously impaired. The loss of communication would make it very difficult to coordinate aid and assistance.

While it is unknown how American citizens would respond in an environment where the electrical grid was lost, possibly for years, it is prudent to plan for the worst case scenario. Population centers, food production and distribution, housing, and almost every other aspect of life are built for a modern society relying on modern technologies and a full-up electrical grid. Civil unrest and the eventual breakdown of societal norms are almost certain as resources become scarce and governmental control is severely degraded.

**Measures to Reduce the Threat**

By now it should be evident that an electromagnetic pulse event has the potential to catastrophically impact the Homeland and affect our viability as a nation. Therefore, every possible measure should be taken to prevent a manmade EMP attack from occurring.

An EMP attack requires a nuclear weapon and the means to launch the weapon into a high enough altitude for the pulse properties to have effect. Nuclear non- proliferation is our national policy and it remains a top priority. But additional focus should be placed on missile and missile technology proliferation. The goal should be to prevent the sale of missiles, their components, and their technology to any nation not a firm ally of the United States.

**Measures to Mitigate the Impact**

If our intelligence services and Homeland defense systems are unsuccessful in preventing the launch of a nuclear missile, or a major electromagnetic solar storm takes place, there are procedures which can be taken to lessen the impact of an EMP strike, and measures to prepare the Homeland to better withstand the impact.

The absolute highest priority must be to modernize and protect the electrical power grid. As previously discussed, the power grid is the most critical component of our modern society. But in reality it is not possible to protect all of the numerous electrical systems from the effects of an EMP attack, as there are enormous amounts of components with assorted designs, ages, and manufactures resulting in varied levels of vulnerabilities. Therefore, initial priority should be to the most critical components of the electrical grid, the transformers and generators. Transformers and generators could be hardened with a surge protector type system which would absorb the EMP pulse and temporarily shut them down if struck. Additional critical components, spare parts, and generators should be ordered now, and stockpiled, and safely sheltered at locations geographically dispersed throughout the United States. Sheltering should be done in such a way to block harmful electromagnetic pulses. This could be done by putting as much mass as possible between the pulse and stockpiled equipment. Sheltering

underground or in tunnels would provide substantial protection. Another method of protection is to put equipment and components in what is known as a Faraday Cage. A Faraday Cage is a metal container built around the item to be protected. It serves as a shield and redirects EMP properties into the ground.

The objective of preparing safety mechanisms and stockpiles is to limit the extent and amount of time electricity is lost. The total cost of most protective measures is relatively small, especially when no cost can adequately be associated and compared to the potentially catastrophic result of the entire electrical grid system being shut down for a lengthy period of time.

Dr. John Kappenman, who was the primary author of a study requested by the Congressional EMP commission and the Federal Emergency Management Agency (FEMA), believes that it is very feasible to install a surge suppressor type system to the "several thousand major substations and other high value components on the transmission grid" and harden the most significant 5,000 power generating plants.[31] In July 2009 testimony before the House Committee on Homeland, Dr. Kappenman estimated the cost of the basic level of safeguards to the electric power grid to be between $250-500 million to protect the transformers and another $100-250 million to protect the power plants.[32] According to Dr. Kappenman, once installed, the surge protector type system would be capable of preventing at least 60% of nuclear or solar E3 type pulses.[33] Dr. Kappenman's plan would not protect individual electronic systems from E1 or E2 pulses, but it would at least provide a basic level of protection to the electrical power grid at a modest cost. And, Dr. Kappenman believes that such protection would mean the difference between a major inconvenience and societal collapse.

In June 2010 the House of Representatives passed HR 5026, the "Grid Reliability and Infrastructure Defense Act." The bill did not make it through the Senate and did not become law by the time the 111th Congress adjourned. The bill would have directed the Secretary of Energy "to develop technical expertise in the protection of systems for the generation, transmission, and distribution of electric energy against geomagnetic storms or malicious acts using electronic communications

or electromagnetic pulse that would pose a substantial risk of disruption to the operation of those electronic devices or communications networks, including hardware, software, and data, that are essential to the reliability of such systems."[34] The passage of HR 5026, or a similar type bill, would have eventually forced the modernization of the United States' electrical power grid. The result would be a resilient electrical grid much better positioned to withstand the effects of an EMP event.

The 112th Congress has taken a step forward with introduction of HR 668, the "Secure High-voltage Infrastructure for Electricity from Lethal Damage" or the "SHIELD" Act.[35] The bill was introduced in the House of Representatives in February 2011 by Representative Trent Franks, Republican-Arizona. The bill amends the Federal Power Act to protect the most critical components of the bulk-power system and electric infrastructure against the threat posed by EMP.

In conjunction with modernizing and hardening the electrical grid system, measures should be taken to keep the nation's transportation systems viable. As a backup to electrical power major fuel distribution points should have backup generators to pump fuel. Local gas stations should be required to maintain hand pumps. Oil refineries should have the backup capability to produce at least a minimal amount of new fuel in the absence of electrical power. And civil authorities must be prepared to control and prioritize the distribution of fuel.

Nationwide personal preparedness would greatly increase the resiliency of the Homeland. The Federal Emergency Management Agency (FEMA), in concert with State and local governments, should educate individuals and families about the importance of maintaining a minimum of a 30-day or more supply of food, and other emergency necessities. Americans must understand that they are responsible for their own well being from not only an EMP type event, but for natural disasters such as hurricanes and earthquakes.

Following an EMP event, contingency planning should be made to default command and control to the local level. Organizations such as the Army National Guard, Army Reserve, police, and fire departments will become the primary administrators at the local level, and should be

equipped, supplied, and trained accordingly. Increasing preparedness will be expensive and require additional manpower from the Department of Homeland Security and the Department of Defense, but it is well worth the cost and effort. The objective is to support the population until electrical infrastructure capabilities are reestablished.

## Conclusion

The detonation of a single nuclear weapon at a high altitude above the United States, or a major solar geomagnetic storm, has the potential to catastrophically impact the United States. The resulting scenario posed by an EMP type event is beyond comprehension for the majority of our leaders, and almost all of our citizens to grasp, because it is something we have never experienced on anything but a very small scale. Regardless, the threat is real and our modern electricity based society is extremely vulnerable. Reasonable and practical steps taken now by governmental agencies, in concert with utility providers, could greatly mitigate the consequences of such a devastating event. What is needed is a National level appreciation of the threat, and a National level effort to implement synchronized measures to do what is necessary to protect the Homeland and increase its resiliency. The challenges are not technical, but bureaucratic and regulatory. The solutions are within our grasp. The potential effects of inaction are catastrophic, and that alone should be enough cause for action.

# DIME Elements of Jihad

**Colonel Shirley J. Lancaster**
United States Army

> Islam isn't in America to be equal to any other faith, but to become dominant. The Quran should be the highest authority in America.[1]
>
> —CAIR founding Chairman Omar Ahmad

WHILE AMERICANS ARE ACUTELY AWARE of the dangers to our fighting men and women from radical Islam or Islamists in Afghanistan and Iraq, they rarely comprehend and even deny the possibility of an Islamic threat to our democratic way of life here in America by any method other than a violent terrorist attack like the one that changed our lives forever on September 11, 2001. As over nine years of protracted war with thousands dead and injured in two Muslim countries indicate, the enemy is adaptive, politically astute, and a savvy communicator. What he lacks in technological brilliance, he makes up for in patience, determination, and numerous methodologies for attacking America in methods of attack other than military or violent. While we pride ourselves in having state-of-the-art tactics, techniques, and procedures, (TTPs), we don't readily grasp that the enemy understands how we fight, and has incorporated our methodologies to use against us.

Within the military and diplomatic national security lexicon, the DIME instrument of power (IOP) tool is used as a construct to analyze any enemy's strengths and weaknesses. DIME stands for diplomatic, informational, military, and economic systems. In knowing how efficient and effective the enemy is with respect to these IOPs, planning can be done concurrently in several lines of operations (LOOs) to best exploit his weaknesses.

Along with asymmetric warfare, suicide bombers, Improvised Explosive Device (IED) attacks, and terrorist attacks against Americans both overseas and on American soil, Islamists are waging more than just

violent jihad against us. They are cognizant of the opportunities that come with globalization, and are using the DIME elements to attack us and weaken America from within, and challenge her constitutional and democratic way of life.

**Diplomatic Jihad**

Islamists based in the United States are diplomatically and politically using our open society and constitutional laws and freedoms to infiltrate our institutions from within. One of the most effective ways Islamists are accomplishing this is through their seemingly innocuous Muslim outreach programs. Many of the most successful of these diplomatic and political jihad efforts have spawned from the influence of the Muslim Brotherhood. The Muslim Brotherhood (MB) was established in 1928 in Egypt by Hassan al Banna. "Its express purpose was two-fold: (1) to implement sharia law worldwide, and to (2) to re-establish the global Islamic State (caliphate)."[2] The MB has gradually become more successful as Islam becomes more popular worldwide as a religion, and the Islamists exploit its violent tendencies.

The MB was the impetus for Egyptian Islamic Jihad, the Palestine Jihad and Hamas. It's also the parent organization of al Qaeda. Before joining al Qaeda, Osama bin Laden, Dr. Ayman al-Zawahiri, Khalid Sheik Mohammed, Blind Sheik Omar Abdul-Rahman, and other infamous terrorists were all involved in the trans-national MB.[3]

The MB has been working on its plan to Islamize the west for decades. According to Gaubatz and Sperry, in confiscated MB writings that were intended for internal use only, plans were detailed which basically sought to "take over the U.S. through mass conversion and political infiltration, not ruling out violent jihad when the time was right and the Brotherhood's infrastructure was in place and strong."[4] To that end, "the Brotherhood has set up jihad training camps inside America where its foot soldiers conduct paramilitary exercises, including firearms and other weapons training."[5]

The book *Muslim Mafia* is the story of a former U.S. Air Force Special Operator's son who infiltrates a major Muslim outreach organization known as the Center on American-Islamic Relations, or CAIR. The

son, whose name is Chris Gaubatz, infiltrated the organization and discovered thousands of pages of documents which clearly linked the outwardly benign objectives of CAIR to its real objectives which were to support violent jihad and undermine law enforcement – with the ultimate goal of eliminating and destroying American society from within. This "grand jihad"…requires infiltrating our political system and using our religious freedoms against us.[6]

According to the papers Gaubatz found, the MB stated that "if we put a nationwide infrastructure in place and marshaled our resources, we'd take over this country in a very short time."[7] The idea is to wage this cultural "civilization/stealth"[8] or DIME-based jihad now, and finish the job later with a violent jihad – once the proper infrastructure is in place.[9] The MB is spearheading a five step plan to Islamize America with the ultimate goal of implementing total sharia law and eliminating the American constitution from the face of the earth.

Initially, when Islamic power in this country is weak, the plan for the Islamic front organizations is to acquire power peacefully. When the brotherhood of Islamic organizations gets stronger, the plan is to take over the government by force and implement sharia law.[10] According to Gaubatz and Sperry, the five phases are:

> Phase 1: Establish an elite Muslim leadership, while raising taqwa, or Islamic consciousness, in the Muslim Community.
>
> Phase II: Create Islamic institutions this leadership can control and form autonomous Muslim enclaves (much like the Muslim enclaves we see in Europe which are formidable).
>
> Phase III: Infiltrate and Islamize America's political, social, economic and educational systems, and form a shadow state within the state. Expedite religious conversions to Islam, and manipulate the media. Insist American institutions sanitize any language that is offensive to Islam (which is already being done voluntarily).
>
> Phase IV: Openly confront U.S. policies with hostility, and commence continuous rioting. Flood the U.S. government with never-ending demands for special rights and accommodations for Muslims.

> Phase V: Initiate the final conflict and overthrow the constitutional government and replace it with sharia law.[11]

The brotherhood of Islamic organizations claims to be in Phase III right now, and with the administration censoring the language used to describe the enemy as anything but Islamists or Islamic extremism; it's not hard to believe that their being in Phase III is possible. Hedieh Mirahmadi, a Muslim community organizer based in Washington, DC, fears that political correctness has overcome the Obama administration, to the point where it is appears to be dissecting radical Islamism out of existence.[12] Mirahmadi experienced this trend personally as part of a steering committee for a conference on radicalization sponsored by the State and Defense Departments and the Rand Corporation in May 2010. According to Mirahmadi, during the discussions the draft report was titled "Defining a Strategic Campaign to…Counter and Delegitimize Radical Islamism."[13]

> *We made it all the way through the day of printing with that title. There were probably 15 drafts. But when the report was published, the title had been changed. The term radical Islamist had become violent extremism, even though the 97 page report which was made public on 14 June dealt almost exclusively with problems in the Muslim world.*[14]

According to Congresswoman Sue Myrick, co-founder of the congressional Anti-Terrorism Caucus, it's no secret what the radical Islamists are trying to do to this country. "They intend to infiltrate all areas of our society, and use the freedoms that are guaranteed under our constitution to eventually replace it with sharia law."[15] Elements of the U.S. government are very concerned about the Muslimization of Europe, and the fact that sharia law has gained significant footholds in such democratic European countries as the United Kingdom, France, and Norway to name a few.

Sharia law is Islamic law. While most people understand that the Quran is the Bible of Islam, according to Bill Warner from the Center for the Study of Political Islam, the foundations of Islam and sharia law are based on three books.[16] "The Quran and the Sunna, which is the perfect example of Mohammed found in two tests, the Hadith, and the

Sira. Each and every law is Islam must have its origins in the Quran and the Sunna. These three texts can be called the trilogy."[17]

According to Warner, "the Quran comprises only 14% of the total words or doctrine that is Islam. The text devoted to the Sunna (Sira and Hadith) is 86% of the total textual doctrine of Islam. Islam is 14% Allah and 86% Mohammed."[18]

"Sharia is the term used to describe the rules of the lifestyle ordained by Allah. In other words, sharia includes the do's and don'ts associated with Islam."[19]

> *Sharia is held by mainstream Islamic authorities…to be the perfect expression of divine will and justice and thus is the supreme law that must comprehensively govern all aspects of Muslims' lives, irrespective of when or where they live. Sharia is characterized as a complete way of life (social, cultural, military, religious, and political.)*[20]

It is critical to understand that Islam is not just a religion. Sharia makes it a complete lifestyle including very strict rules of compliance with respect to political, religious, social, military and legal behavior.

According to Warner, "political jihad is a political process with a religious motivation. Political Islam is the doctrine that deals with the non-Muslim, and sharia is the political implementation of the Islamic civilization."[21] Sharia law is completely incompatible with the United States constitution, in that there is no separation between church and state. While Congresswoman Sue Myrick was quoted earlier in the paper as saying that radical Islamists have told us that they intend to infiltrate our society by all means possible and use our constitutional freedoms against us and replace the constitution with sharia law,[22] many government agencies and lawmakers refuse to address this issue due to the fear of being called anti-Muslim or Islamiphobic. There are, however, some brave patriots who are trying to bring this frightening and critical issue to the public's attention. A group of top security policy experts deeply concerned with what they are calling "the preeminent totalitarian threat of our time," sharia law, have devoted nearly two hundred pages of a study to outline the threat of sharia law to the United States and particularly to the U.S. constitution. They deem the

threat at least as dangerous as communism was and considerably more stealthy. This report is called Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II.*

What makes this threat even more insidious is that people in the United States have become so afraid of being labeled anti-Muslim or racist, that they are literally afraid to question the motives and funding of these so-called benevolent Muslim outreach organizations. These organizations then basically have free reign to use their funds to promote terror and use our constitutional rights of freedom of speech and religion to manipulate us. Those charged with protecting our most precious liberties and our constitution are afraid to ask the tough questions because they fear being labeled Islamiphobes. Meanwhile, the Islamists get stronger and use their minority status to get more deeply entrenched in respectable American government, education, and corporate finance to wait for the right time to synchronize their DIME jihad. As we become more and more afraid of speaking up, they grow stronger.

**Informational Jihad**

Informational jihad is how the Islamists formulate and disseminate their strategic messages. The Islamists are extremely successful at articulating several messages using several different means of communication. They are masters of disinformation, "cherry picking" quotes from the Quran where it suits their purposes, and they have been absolutely brilliant in their use of the internet for the last decade. They have no qualms about lying to Americans regarding their peaceful religion and peaceful intents, because the Quran condones lying and pretending to assimilate into the practices and lifestyle of the non-believers, in order to rise up later and conquer the lands of the infidels for the greatness of Allah. This accepted form of lying is called taqiyya and can be loosely translated to mean lying for the sake of Islam. "It is based on Quran 3:28 and 16:106…which permits and encourages precautionary dissimulation as a means for hiding true faith in times of persecution or deception when penetrating the enemy camp."[23]

The *Reliance of the Traveler* is the most renown and accepted translation of Islamic sacred law into English endorsed by all major schools of

Islamic law including the four Sunni schools which include Hanafi, Maliki, Shafi'I, and Hanbali.[24] It also discusses various instances where lying is permissible. This is an important nuance as unlike the old and new Testaments, the Quran does not hold lying as a breach of a religious tenet. "Thou shalt not lie" is not stated as such in the Quran. The message that the Islamists are sending is that they want to be Americans. The underlying message that they are sending is that they want to change America to be a Muslim country under sharia law.

Walid Phares, an author of several books on jihad, discusses the Islamists' informational jihad in terms of three Wars of Ideas.[25] This paper will touch on the first two Wars of Ideas. The First War of Ideas (1950s-1990s) took place when the Wahhabis concentrated on taking hold in Saudi Arabia. As Saudi petro-dollars grew, the Wahhabis began to export their ideology outside of Saudi Arabia.[26] While this process was slow, these Islamists took advantage of the attention that the world was paying to the Cold War between the East and the West. The First War of Ideas was largely ideological and educational. The jihadists focused most of their efforts on increasing the numbers of impressionable youth using madrassas, mosques, orphanages, and hospitals.[27] From this they coined the slogan "la sharqiya, la gharbiya, umma wahda Islamiya" (no East, no West, one and unique Islamic Umma).[28] "It took the Salafists and the Khomeinists the bulk of the twentieth century to organize their movements and rise to influence."[29]

The Second War of Ideas (1990-2001) took advantage of the collapse of the Soviet bloc to strategically bring together the traditional Islamists currently in power with the emerging jihadists in order to target the West and crush any emergence of democracies in the Arab world. After watching the West, "intervene on three continents to 'back democracy,' towards the end of the Cold War, many of the Muslim world's regimes feared a similar repeat in their countries."[30] The jihadists were also successful in infusing the ever increasing number of petro-dollars to "form a consortium closer to cultural imperialism, targeting departments of Middle East studies, international relations, and history on American, European, and other Western campuses."[31] The idea of this movement was to "seize control of setting the curriculum, determine the issues to research and teach, and select the instructors and

scholars."[32] For all practical purposes, petro-dollar funding succeeded in virtually eliminating the study of human rights, democratization, minorities, feminism, and jihadist ideologies from Western academia.[33]

According to Brigitte Gabriel, some of our nation's finest universities such as Harvard and Georgetown "receive federal funds as well as millions of dollars from the Saudis for Middle Eastern studies programs."[34] Gabriel goes on to quote Sandra Stotsky, former director of a professional development institute for teachers at Harvard University as saying "most of these materials have been prepared and/or funded by Islamic sources here and abroad, and are distributed or sold directly to schools or individual teachers thereby bypassing public scrutiny."[35] The Saudi Government provides free textbooks to Islamic schools and free material to mosques. Much of this material preaches hatred towards Jews and Israel, and re-writes history to exclude any mention of the holocaust. It also misleads Muslim children to believe that Muslims inhabited the Americas centuries ago. While blatantly untrue, this fuels a simmering fire to convince impressionable children that they have rights to claim America as a country for their own as an Islamic state, now and for the future.[36] Due to increased Muslim immigration to the United States, "it is estimated that there are between two hundred and six hundred Islamic schools in America teaching almost fifty thousand students."[37] According to Gabriel, "many of these schools are breeding grounds for jihad in America and are funded by American taxpayer dollars."[38]

Other instances of tainted contributions to Islamic schools in the United States include the Islamic Academy of Florida which is a private school for grades one through twelve in Tampa Bay. "In 2003 the academy received more than $350,000 worth of taxpayer-funded school vouchers to help underprivileged children attend their school."[39] Later that year a federal grand jury in Tampa issued a fifty-count indictment against the academy for being an affiliate of the MB organization Palestinian Islamic Jihad (PIJ).[40]

This organization stems from the Middle East and targets Israeli civilians and others it deems enemies.[41] The indictment claimed the academy was helping the PIJ by raising funds through school vouchers and fund-raisers.[42] Also noteworthy is the fact that the school is owned

by the North American Islamic Trust, which is an Islamic investment group of the Muslim Brotherhood that manages the assets of the most deceitful and treacherous mosques in the United States, and was named as an unindicted co-conspirator in the Holy Land FoundationTrial (HLFT).[43] In 2007, the HLFT exposed many benevolent Muslim Brotherhood charities and outreach organizations that were linked together while HLF was caught funding Hamas and other terrorists organizations. While exposing this school might seem like a victory against informational or educational jihad it was not.

After this incident, another Islamic private school, the American Youth Academy, opened up next door to the old Islamic Academy of Florida. Unbelievably, "the schools shared the same books, desks, teachers and telephone numbers. In 2005, $325,000 of taxpayer money was given to the school for its elementary and secondary school program."[44] All this is happening right before our eyes. There are literally dozens more cases of Islamic schools teaching anti-American and anti-Israeli rhetoric in our country, and doing it with the luxury of our tax dollars to spend.

At the New Horizons School in Pasadena, California, another Islamic private school won a Blue Ribbon award for excellence from the U.S. Department of Education. While this may sound like a positive achievement, "the Bureau of Islamic and Arabic Education, which developed the school's academic program, has on its website its twist on the U.S. Pledge of Allegiance: As an American Muslim, I pledge alliance to Allah and his Prophet."[45] Another disturbing element of educational jihad as part of informational jihad is that "the Islamic Society of North America (ISNA), which has been named by the U.S. government as another unindicted co-conspirator in the HLFT, is the initiator and architect of all the New Horizons Schools in North America."[46] According to Gabriel, reports state that ISNA, which disseminates Islamic educational material to mosques and Islamic schools in the United States, is connected to domestic and foreign terrorist groups, and has invited Islamic radical extremists to speak at its events.[47]

According to the Team B report, even though the ISNA was an unindicted co-conspirator at the HLFT, "their subsidiaries are still the certifying authority for all Muslim chaplains for the department of defense

(DOD)."[48] Inexplicably, "they also were selected to provide training for U.S. Army senior enlisted personnel and officers to orient them about Islam prior to their deployments to Iraq and Afghanistan."[49] The report goes on to state that "the ISNA has become the U.S. government's leading partner for 'outreach' to the Muslims of America – including the FBI and DHS, the very organizations mandated by law to protect and defend us from domestic enemies."[50] If you are wondering how this can happen, it is all part of the stealth/civilization jihad. Our leadership is conned or in denial as to believing that the Islamists in this country are benevolent, even when they are faced with evidence to the contrary. We as Americans simply do not think in a manner that allows us to easily believe that our "so called" friends would lie to our faces, even though it is clearly spelled out in the Quran that this is permissible to achieve any and all ends for Allah. Our leadership is irrationally paralyzed with the fear of being politically incorrect and being called islamaphobic. Consequently, when law enforcement officers, military personnel, or other Americans who have sworn an oath to protect and defend the Constitution challenge their leadership with uncomfortable and inconvenient facts, the leadership is faced with a hard choice. They must either admit that they've been duped by a lack of understanding of the threat, or they must ignore or suppress the facts in the interest of protecting their careers.[51] I fear an increasingly large number of these leaders choose the latter.

**Military Jihad**

The military aspect of jihad is much more straight forward and consequently easier for most Americans to understand. The United States is fighting two wars in the 21st century, and they are both against radical Islamists, one in Iraq, and one in Afghanistan. As stated before, the Quran and the rest of the trinity serve Muslims not only as religious books, but as complete directives for how life itself is to be lived. The Quran also outlines how Islamists should wage war. The book by Brigadier S.K. Malik, of the Pakistani Army, *The Quranic Concept of War*, explains very clearly the thought processes behind how Islamists should conduct wars. It discusses the thought processes behind the decisions made and the actions taken. As America struggles to determine its future in Iraq and Afghanistan, it is clear that after

nine years of war with these militants that national policy-makers, strategists, and senior military advisors do not understand how Islamist extremists think, much less how they fight.

What is key to understand about the Quran as a guide to war and what makes it different from other works published on how to wage war, is that the Quran is a holy religious book and does not separate war from holy war. It is a book that by being religious presumes that every war is a religious war, and perhaps more importantly, believes that since the Quran is accepted by its believers as the literal word of God himself and not of man, the directions it contains are God's own and must be followed to the letter. This is significant because the United States does not fight holy or religious wars. We fight wars to protect our people, ensure our security and protect our national interests. The Islamists fight wars for Allah. The first Quranic revelation that gave Muslims permission to fight said, "to those against whom war is made, permission is given to fight because they are wronged; and verily, Allah is most powerful for their aid. They are those who have been expelled for no cause except that they say, our Lord is Allah."[52]

The Quran went on to provide guidance to Muslims on how to break treaties and alliances, and ultimately to give those living in Arabia who did not convert to Islam (Christians and Jews), the option to choose between conversion, submission or death. The Quranic meaning of submission refers to the jizya, a tax levied on those not converting to Islam but living in the Islamic state.[53] The Quran says, "fight those who believe not in Allah…even if they are of the people of the book, until they pay the jizya with willing submission and feel themselves subdued."[54] Here we see the underpinnings of the lack of tolerance Islam has towards other religions. What started out as entering a conflict voluntarily for self defense purposes has turned into killing non-believers, or collecting a tax from them until they feel subdued or beaten down.

It is crucial to understand the concept of the holy war versus the wars the United States fights over security or other national interests. The holy way or jihad, makes a Muslim citizen "answerable both to the state and to Allah in the fulfillment of this divine obligation."[55] The Quran also promises great gifts in the afterlife for those who fight for Allah,

and nothing for those who reject Islam. The Quran promotes the ideas of "life, death, reward, punishment and the afterlife."[56] Here the Quran instructs the faithful to "fight in the way of Allah with total devotion and never contemplate flight from the battlefield or fear death."[57] What is critical to understand, is that the Quranic method of war uses Allah to protect Muslims from psychological and moral attacks against the enemies of Islam.[58] In essence, the Quran, "helped Muslims conquer the fear of death, and become immortal and invincible."[59]

Malik also undertakes an ethical view of Quranic war stating that the Quran prohibits, "the decapitation of prisoners of war, the mutilation of men, the killing of enemy hostages, and resorting to massacre to defeat an enemy."[60] Clearly those extremists who beheaded Daniel Pearl were not adhering to the Quran. Explained further by Malik, Muslims had three principles to follow in executing war. "First… subdue the enemy and not take prisoners. Second, take prisoners only after the enemy had been thoroughly subdued. Third, once taken, treat prisoners humanely, choosing only between generosity and ransom."[61]

Applying these directives today, it would clearly appear that the members of al Qaeda, the Taliban, and numerous other Islamist extremist groups have either not read these passages of the Quran, or they are just ignoring them and "cherry picking" those portions of the Quran that suit their purposes. Malik goes on to say that "the term 'jihad,' so often confused with military strategy, is, in fact, the near-equivalent of total or grand strategy or policy-in-execution."[62] The *Reliance of the Traveller* says that Jihad means to war against non-Muslims, signifying warfare to establish the religion.[63] Malik goes on to say that:

> *Jihad entails the comprehensive direction and application of 'power,' while military strategy deals only with the preparation for and application of 'force.' Jihad is a continuous and never-ending struggle waged on all fronts, including political, economic, social, psychological, domestic, moral, and spiritual, to attain the object of policy.[64] Jihad aims at attaining the overall mission assigned to the Islamic state, and military strategy is one of the means available to do so. It is waged at an individual as well as a collective level, and at internal as well as external fronts.*[65]

The whole philosophy of Quranic war, according to Malik, "revolves around the human heart, soul, spirit, and faith."[66] The main objective is the opponent's heart or soul, and the idea is to "strike terror into the hearts of enemies."[67] Malik goes on to say that "so complete and thorough should war preparation be, that we should enter upon the 'war of muscles' having already won the 'war of wills.'"[68] Malik goes on to discuss how the military instrument of power is not the total strategy, only a part. "Military preparedness will yield the desired results only if it forms a part of the total preparedness."[69]

Malik emphasizes that the striking of terror into the hearts of the enemy and completely destroying his faith is not only the means of Quranic war, but the end in itself.[70] He goes on to state that once this happens, there is little else to achieve.[71] "Terror is not a means of imposing decision upon the enemy; it is the decision we wish to impose upon him. An Army that practices the Quranic philosophy of war in its totality is immune to psychological pressures."[72] The Quranic philosophy teaches that death is not to be feared because of the richness and rewards of the afterlife. This philosophy gives us great insights to why Islamists are willing to die as human bombs. They do not fear death, in fact quite the opposite. To die as a martyr to Islam, is an honor. Understanding these thought processes which are so different from ours, is the key to defeating Islamists militarily.

**Economic Jihad**

Economic Jihad is the process of introducing sharia compliant finance practices into western banking systems. These practices have grown greatly over the last 20 years, boosted by wealthy Arab nations with billions of dollars of petro-profits to invest. "The global market for Islamic financial products in 2008 was worth over 500 billion English pounds, and was expected to grow 15-20% per year."[73] "Islamic financial products are likely to account for 50-60% of the total savings of the world's 1.2 billion Muslims within the next decade."[74] While Islamists will insist that sharia compliant finance is a non-negotiable requirement for Muslims, the fact is that "sharia finance is a new phenomenon. This suggests that it is not in fact essential to the practice of sharia."[75] Timur Kuran, Muslim scholar and professor of

Economics and Political Science at Duke University, claims that sharia finance is an, "invented tradition of our times that does not go back to Muhammad's day."[76] According to Patrick Sookhdeo, author of the book *Understanding Sharia finance: The Muslim Challenge to Western Economics,* "even Islamic scholars of a century ago would have been very surprised at the modern version of Islamic economics."[77]

According to Sookhdeo, "sharia finance is facilitated to a large extent by the vast amounts of money in the oil-exporting states, money which needs investment outlets."[78] Sookhdeo goes on to say that "the concept of an Islamic economy was integrated into the discourse of the Islamist struggle to weaken the West in preparation for the ultimate phase of establishing Muslim political hegemony in the world."[79] What Western governments and financial institutions have done in their eagerness to embrace petro-dollars for investments is "introduced Islamic finance and banking into the western system and unknowingly encouraged the Islamist takeover by the Muslim world."[80] Sookhdeo goes on to state that "the main goals of Islamic economics are political and religious, not financial, namely to gain support for radical Islam and to promote Muslim separatism."[81]

According to Sookhdeo, Islamic economics was born out of modern Islamist movements, who derived the concept from several verses of the Quran, the hadith, and from early Islamic examples having to do with riba, which has to do with the practice of charging interest on financial transactions.[82] There is controversy over whether strict interpretation of the Quran and definition of riba forbids all interest payments or just what is known as usury, which is interpreted to mean excessive and exploitative interest charged.[83] If the interpretation of riba permits charging acceptable interest, there is no need for a separate Muslim finance system. If riba is interpreted as any non-allowed interest fee, that opens the door to a creation of a "separate and distinct Islamic economic system, confusing for non-Muslims and dominated by Muslims."[84]

According to Sookhdeo, Al-Azhar which is the preeminent center for Sunni religious studies, states that "riba is usury or exorbitant and oppressive interest, but has proclaimed moderate fixed interest permissible."[85] In Egypt, the religious establishment differentiates

between interest and usury as well, supporting a legal or socially acceptable interest rate.[86]

Modern Islamists have chosen to reinterpret riba in the strictest possible manner to mean any interest whatsoever. No interest of any kind is allowed. Islamists have taken various sharia elements regarding economic transactions and turned them into an economic-like system with detailed procedures.[87] The total ban on interest means that it is not possible to collect or pay interest on borrowed money as in conventional banking; for this reason sharia finance developed as an asset-based system.[88] This separate finance system has great appeal for Islamists who want to further separate Muslims from non-muslims and financially strengthen Islam and its ideology globally.

In reality, according to Sookhdeo, no economic system can function in reality without interest. The complex Islamic system involves thinly-disguised payments of interest.[89] "There is nothing really different about Islamic banks. The concept merely serves the Islamist need to enhance Islamic identity and cohesion."[90] In truth, "over 95% of the modes of financing employed by the Islamic banks entitle interest. Islamic bank practices differ only cosmetically from those of commercial banks."[91] According to Timur Kuran, in countries where conventional banks and Islamic banks operate next to each other, the returns on profits given by the Islamic banks are nearly identical to the interest-based returns of the conventional banks.[92] He goes on to say that this proves that Islamic banks, despite what they would have you believe, actually glean their profits on interest bearing assets and investments.[93] What is also troubling and revealing about sharia finance is that Islamic economics has done nothing to relieve poverty in Muslim lands, and in fact, the Muslim public is being exploited in the name of Islamic banking.[94] In 2006, Saleem Salam Ansari delivered the presidential speech at a seminar on Islamic banking in Pakistan. Ansari stated that the "Islamic banking system in Pakistan was providing huge returns for bankers at the expense of the poor. Customers were losing their savings while the banks were getting returns of 22% and more annually."[95]

Other effects of Islamic economic Jihad are the movement of petro dollars from western to Islamic banks. "In 1972 the U.S. spent $4 billion for Saudi oil, or 1.2% of our defense budget. In 2006 we spent

$260 billion or half our defense budget. Saudi oil revenue grew from $2.7 billion to $200 billion and with it grew its ability to fund radical Islam."[96] As Islamists become the loudest voice of Muslims and gain power politically, many governments are acquiescing to their demands for sharia finance. According to Sookhdeo, Sharia finance is stronger than before September 11th, and is, in effect "an economic jihad that mobilizes Muslims who are not ready for military jihad to share in non-violent jihad."[97]

The west has accepted sharia finance as a religious requirement for sharia. In its haste to be accommodating, the west has ultimately weakened moderate and reform minded progressive Muslims. It also has put pressure on Muslims in the west to use sharia finance whether they want to or not. According to the *Reliance of the Traveller,* it is also noteworthy to state that for Muslims, not only is giving to charity which is called Zakat, obligatory, it is also obligatory to give a percentage of the Zakat for Jihad, those fighting for Allah.[98]

Sharia finance is confusing to non-Muslims. Due to its complexities and its unpredictable changes, the Islamic banking system provides the ability to more easily conceal certain activities than it would be for conventional banks. "Often, potential profits are undefined, making it easier for the transfer of illicit money through a pool of colluding depositors."[99] This illicit money can be used to fund terrorism and can be laundered more easily than money in conventional banks. Another problem caused by sharia finance is the relationship between the Islamic banking system and the hawala dealers.[100] "Hawala is an informal funds transfer system common in Islamic societies. It involves a huge network of money brokers located mainly in the Middle East and Asia."[101] The hawala network is trust based and does not leave a paper trail. As the hawala dealers interact with Islamic banks, this provides a lucrative opportunity for illicit transfers and money laundering.[102]

There is no transparency in Islamic banking, and it has failed to establish any regulatory standards such as those found in western banks. "Corruption is often the most persistent problem."[103] Islamic banks are currently deemed sharia compliant by a group of specialist jurists in Islamic finance and sharia who sit on the boards of many financial institutions.[104] "Many of these board members also teach at

Islamist academic institutions, and sit boards of Islamist organizations linked to the worldwide Islamist network."[105] This should be very worrisome to the western banking world. "Why should western financial institutions be guided by religious boards basing decisions on Islamic religious standards subject to alteration and to alternate interpretations?"[106] In fact, why are western non-Muslim finance and government professionals letting themselves blindly follow the dictates of shaira finance?[107] Those in favor of sharia compliant finance intend to gradually grasp financial power from the western world to the Muslim world. The trinity does not state the need for a parallel financial system. It is economic jihad, part of the greater cultural and civilizational jihad that ultimately wants the western world to become part of the Islamic world.

**Countering DIME Jihad**

According to Dr. Tawfik Hamid, "the proliferation of violent Islam in Islamic societies has typically followed a standard pattern."[108] This pattern starts with the Salafi ideology of women wearing the hijab. The hijab becomes a catalyst for Islamism and helps to spread the ideology itself."[109] According to Dr. Hamid, this leads to passive terrorism, where attacks don't occur but there is silence which equals compliance. Here is where sharia law creeps in, and active terrorism attacks commence with anti-American and anti-Western rhetoric.[110]

In order to ensure that DIME jihad is not successful in the United States, we must first have the courage to acknowledge that it exists and that it is happening. Our country did not come by its constitutional freedom's easily, and it should not consider giving them up easily. The founding fathers were not concerned about being politically correct, neither should we. We need to admit who the enemy is, and let the world know that radical Islam is the enemy, and that we will call anyone enemy who wants to replace our constitution with sharia law. We need to act swiftly to identify those here in America and abroad, who wish to supplant our constitution with sharia law. There are several actions that we can take as a nation to ensure our liberty. The first thing we should do, is pass a federal law against any implementation of sharia law in the United States just like the state of Oklahoma did.[111]

Also, according to Robert Spencer, we need to stop espousing that Islam is a religion of peace. Our politicians don't need to discuss the nature of Islam at all, just ensure the world knows that anyone who tries to replace our constitution with sharia law is our enemy and will be dealt with as such.[112] Spencer also goes on to suggest that we "make Western aid contingent upon renunciation of the jihad ideology."[113] His point is that if we admit the plain truth about the desire for a global Islamic world, then states we support which incorporate radical Islamic teachings such as Egypt and Pakistan would have to reject those teachings and replace them with teachings of tolerance. Muhammad's claim to the world and supremacism do not have a place in our world.[114]

Make American Muslim advocacy groups work against the jihad ideology. "A 2005 report by the Freedom House Center for religious freedom found material in American mosques teaching hatred of non-Muslims and stating that apostates from Islam should be killed, in accord with Muhammad's directive.[115] Almost a decade after 9/11, "there are still no organized, comprehensive programs in American mosques and schools to teach against the jihad ideology or confront the elements of Muhammad's life that fuel jihadist violence and subversion."[116]

Brigitte Gabriel also has some positive actions that we can take as Americans to defeat the Islamist threat. She as well as Spencer stress that we must work harder to find an alternative energy solution. This will ultimately make us less dependent on Saudi Arabia. She also encourages us to join action groups and monitor our educational institutions and know what the Middle Eastern curriculum consists of. She also says we must define the jihadist ideology as terrorism and increase scrutiny on these Muslim associations and their funding.[117] We must "cut taxpayer funds or tax-exempt status from any school that teaches hate and violence against anyone."[118] Dr. Hamid also believes that education is the key to counterbalance the violent interpretations of the trilogy, and teach young Muslims peace. He emphasizes that "the curriculum should emphasize critical thinking in opposition to Salafist indoctrination."[119]

Dr. Hamid also believes that the efficient use of military force is crucial to success. He reminds us that "the civilized world could not combat

Nazism without defeating it first at the military level. Chamberlain did not overcome Hitler by appeasement, peace negotiations or mutual understanding; it was the devastating military power that ended his barbaric regime."[120] Dr. Hamid goes on to say that it was the military victory that paved the way for peace and democracy. World War II, he says, "furnishes us with an excellent example of the dynamic relationship between military force and ideological transformation."[121]

Along with the moderate or reformist organizations, moderate clerics must have the courage to understand that while the Quran was written centuries ago they must interpret it to work in the 21st century, just as those who interpret the American Constitution make allowances for the passage of time. For example, since the Constitution was adopted in the 1700s, slavery has been declared unconstitutional, segregated schools no longer exist, women and other minorities vote, and the right to privacy is now part of the Constitution.[122] The Quran is over one thousand years older than the Constitution. If societies have changed monumentally since the days of the founding fathers, think of how much they have changed since the days of Muhammad.

"If America can learn and change from 200 years of history, why can't Islamic jurisprudence learn from 1400 years of historical change?"[123] According to Ali A. Mazrui, "Muslims must always remember that while the word of God is infallible and immutable, the human interpreters of the word of god are not. New Muslim intellects should review the doctrines once again."[124] This is what moderate and reformist Quranic scholars must do with the Quran. They must treat it as a living and flexible document that can be relevant to the 21st century. They must have the courage to re-look the punishments for stealing, and adultery. They must deal with the very real existence of homosexuality and women's rights in today's world. If they continue to deny that the Quran is not tenable in the 21st century, the friction between the Western world and the Muslim world will never end.

According to Robert Spencer, courageous politicians like Susan Myrick, should make the so-called moderate Muslim organizations either produce genuinely moderate or reformist initiatives that teach tolerance and assimilation to American values, or stop posing as moderate groups.[125] Law enforcement personnel who have bought into

the lie need to have the courage to do the right thing as well. And while a show of solidarity from the moderates would be a good sign, it is also important to remember this fact about historical moderates:

> *Even though the majority of Muslims are peaceful, law-abiding citizens who do not wish to fight or declare jihad on their neighbors and colleagues, such moderates are irreverent in the war we are fighting. Most Germans were moderate as well. Their moderation did not stop the Nazis from killing 14 million people in concentration camps and costing the world 60 million lives. Most Russians were peaceful as well. However, Russian communists cost the world 20 million lives. The same goes for most Japanese prior to World War II. Yet Japan was responsible for the killing of 12 million Chinese. The moderate majority was irrelevant.*[126]

Until moderates actually speak out and enact change, and the Quran clerics accept the need to bring the religion into a realistic state for the 21st century, we as Americans must protect ourselves in our country, and we must revise immigration policies to ask potential citizens if they support the U.S. constitution or sharia law. They could also be asked other questions regarding women's rights, slavery, and democratic societies. Perhaps they will lie to get into the United States but if they are caught in a lie later, they can be deported, period. Just as enlistees into the armed services are asked if they have ever been a member of the communist party, new immigrants should be asked if they ever intend to overthrow the U.S. constitution for sharia law. Yes they may lie, but if caught later, they will be tried as subversive criminals. At least we get the strategic message out that people with these beliefs are not welcome in the United States.

We must be strong in our resolve to recognize and eliminate all the DIME elements of Jihad as they are threats to our country. We must forget political correctness, and hold those accountable who wish to take from us our constitutional freedoms, and never hesitate to use deadly force to protect our freedoms and our American way of life.

# Cyber Attack! Crime or Act of War?

**Lieutenant Colonel David M. Keely**
United States Air Force

HOW DO WE DISCERN A CYBER ATTACK that is a crime from one that is an act of terrorism, espionage or war? It is the goal of this paper to help readers make that determination. We will define terms and use national and international law, expert opinion and logic to discern the difference between crime, espionage, and acts of war in the cyber domain. We will look at examples and comparative analysis with non-cyber events to illustrate the arguments. While exploring a group of factors known as Schmitt's Analysis to further clarify how to respond appropriately to cyber incidents, we will use a brief case study of Estonia to test them. Finally, a short set of recommendations are made to help the U.S. government institutionalize an approach for making the determination between crimes and acts of war.

Why is this question important? It may seem like technocrats trying to count the number of electrons dancing on the head of a pin. But the definition of what is an act of war and what is not carries a great deal of importance in the United States. The Constitution very carefully divides powers between the Federal government and the states as well as internally among the executive, legislative, and judicial branches.

While the executive contains the powers of the "Commander in Chief" and grants the President war powers, many facets of cyber security (defense against cyber-attacks), lie outside of the traditional definitions of war. War powers likely do not permit daily control of the nation's networks as they lay mostly in the hands of corporations and other private sector entities. Therefore, if the President, and by extension the federal government, is to defend the nation from cyber intrusions or attacks, there must be a defined boundary of what falls under his authority as Commander in Chief and what does not.[1]

Before we explore national and international law on cyber attacks, we need to define what that and some related terms mean.

## Defining the Terms

Since Congress has created statutes to govern computer and network crime (Title 18 of the United States Code [USC], Section 1030), we are given legally enforceable definitions of what activities currently compose "cyber-crimes" within the jurisdiction of the United States. These currently cover areas such as computer fraud and abuse, identity theft, wire fraud, sexual exploitation of children, unlawful acts affecting commerce, fraud in connection with identification documents, authentication features, and information and fraud associated with access devices.[2]

Cyber attack and cyber war, however, are not so neatly defined in U.S. statutes. In fact, the terms of "Cyber war" and "Cyber attack" are often used interchangeably or are used to describe various computer crimes to include espionage. Place either of the terms in an internet search engine and the results will cover a broad spectrum from defacing social or corporate web pages to thievery to the clandestine collection of national security data. A good definition of cyber attack can be found in discussions of the Critical Infrastructures Protection Act (CIPA) of 2001: All intentional attacks on a computer or computer network involving actions that are meant to disrupt, destroy, or deny information.[3]

While this succinctly tells us the "What" of an attack, it cannot tell us the "Why"; it does not categorize the attack. How do we discern a cyber attack that is a crime from one that is an act of terrorism, or an act of war? The key factors are the motivation and identity of the attacker and, to a lesser extent, the impact or result of the attack.

If the motivation of the attacker is monetary gain, destruction of property, or espionage, then a crime has been committed.[4] If the desired result is, "to cause death or seriously bodily harm to civilians or non-combatants, with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act,"[5] then an act of terrorism has occurred. If the motivation is to wage or to assist in waging an "armed hostile conflict between States or nations,"[6] then an act of war has occurred.

We should note that a definition of "cyber attack" is not a matter of consensus. A RAND Project AIR FORCE study by Martin Libicki, for

example, defines it as: "The deliberate disruption or corruption by one state of a system of interest to another state."[7] This definition restricts cyber attacks to the realm of nation-states and would presumably use different terms to describe the same behavior and effects created by non-government activities. The RAND study's approach is that only actions that are possibly acts of war fall under this term and even excludes acts of espionage by nation-states from the term as "spying does not fall under the usually accepted norms for causes of war."[8] This is too narrow of a definition for the purposes of this paper to use.

Furthermore, the CIPA definition does not include attacks where the goal is not to disrupt, destroy, or deny use of the information but to steal it (crime or espionage) or otherwise use it in an unlawful way. It is important to define "cyber attack" as a general concept that encompasses all of the activities listed above because the targeted organization of the attack often has no idea for some time what the purpose of the attack is. It can take hours, days, weeks, or longer to determine the goal of the attacker. It can take even longer, if ever, to determine the attacker's identity.[9] Without knowing the purpose and identity, we cannot meet the RAND study or the CIPA definition and therefore could not use the term "cyber attack" to describe a cyber event.

Moreover, the word "attack" is used in non-cyber ways to include many non- military meanings. The commonly accepted usage of the word attack includes criminal, espionage, and terrorist activities in addition to military ones. People and Automated Teller Machines, for example, are attacked by criminals every day. Our nation's secrets are under attack by foreign intelligence services, and terrorists have attacked our embassies overseas and buildings within the United States. Therefore, we will use the CIPA definition with a few additional words that will include acts of espionage and crime: "All intentional attacks on a computer or computer network involving actions that are meant to disrupt, destroy, deny, or unlawfully use information."

This broader definition will allow the full complexity of the prime question we are attempting to answer – namely how to discern whether a cyber attack is an act of war or not. Otherwise, the definition of the very word would always lead one to conclude "yes" since the definition also meets the parameters of an act of war – nation-state involvement with the goal of destroying something of value.

Cyber war is defined by the RAND study as: "A campaign of cyber attacks launched by one entity against a State and its society, primarily but not exclusively for the purpose of affecting the target State's behavior."[10] This definition allows for the attacker to be anyone, not just a nation-state. The target, however, is limited to nations. Since this paper is to assist U.S. government policy-makers, that definition will suffice. It is important to note that cyber, like the other domains, may experience a war where most military actions are contained within the domain or it may contain a mere portion of the sum total of military actions. The closest analogy may be that of the air domain. Generally, airpower is used in support of land or sea domains but occasionally it is used almost exclusively in an air war, such as a no-fly zone.[11] Likewise, cyber war may be a component of an overall military effort or stand on its own.[12]

In either case, whether the act being evaluated is in a traditional domain or the cyber domain, the standard for determining if a *casus belli* exists should be the same. Nevertheless, a discussion regarding the characteristics of U.S. Cyberspace is important. A discussion of U.S. Cyberspace should start with a definition of the Cyberspace Domain: "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[13] U.S. Cyberspace can be then derived as that portion of the Cyberspace Domain that resides physically within U.S. territory or under the ownership or authority of U.S. government or citizens to include U.S. organizations such as corporations or non-profits. This leads us to explore some of the characteristics of the cyber domain that make it operationally unique from the air, land, sea, and space domains.

**Characteristics of the Cyber Domain**

The National Military Strategy for Cyberspace Operations has an excellent discussion on features of the cyber domain.[14] We want to focus on just the factors in the cyber domain that make determinations regarding *casus belli* more difficult than in other domains. First, it is harder to maintain situational awareness in the cyber domain than in any other domain.[15] We generally have a good idea of what other States, and many non-state actors, possess in terms of both offensive and defensive weapon systems in the space, air, sea, and land domains.

Open source information such as Jane's (published by IHS, Inc.) document these capabilities for all but the most hidden of assets.[16] Not only are most current systems and their capabilities known, but so are many systems in development. Contrast that with the cyber domain. While categories of cyber weapons are generally known (see Table 1 on the following page),[17] the exact effect of each use of those weapons is unknown. It would be as if we knew about the submarines an opposing navy possessed but not the payloads of its torpedoes or missiles. Second, a close watch is maintained on the intentions of the owners of those weapons in the other domains.[18] The United States maintains an extensive network of sensors in all domains to track deployment and employment of those weapons and the organizations that use and support them.[19] Both strategic and tactical surprises have occurred regarding intentions and uses but those are the exceptions rather than the rule.[20] Back to our analogy with the cyber domain, it would be as if we had some idea about the general (strategic) intentions of the owners of the submarines but little information on tactical intentions, and no idea of the submarine's specific locations to include their home ports. In short, determining a potential foe's intentions in the cyber domain is difficult.[21] Even after an attack is underway or completed, the intention of the attacker may not be known for hours or days or even longer.[22] The attack may have been an act of crime, espionage, terrorism or war.

Third, we have a fairly good idea of our shortcomings in our defenses in the other domains and try to compensate with a variety of tools to include alliances, adjusted techniques, tactics and procedures, or make plans accounting for the increased risk. We don't know what or where all of our vulnerabilities are in cyberspace.[23] Additionally, the vulnerabilities we are aware of often go unfixed and unmitigated for years. Adversaries intrude on our networks everyday using both known and unknown weaknesses.[24] The economic toll alone of these intrusions is significant. The estimated loss to U.S. businesses due to cyber crime in 2008 was $42 billion.[25] According to DoD, "more than 100 foreign intelligence organizations are trying to break into U.S. networks."[26] Costs of repair due to military network intrusions attributed to China alone over a six month period exceed $100 million.[27]

| Type of Exploit | Description |
|---|---|
| Denial of service | A method of attack from a single source that denies system access to legitimate owners by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet. |
| Distributed denial of service | A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target. |
| Exploit tools | Publically available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems. |
| Logic bombs | A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. |
| Phishing | The creation and use of e-mails and Web sites – designed to look like those of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. |
| Sniffer | Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text. |
| Trojan horse | A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. |
| Virus | A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate. |
| War driving | A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations to gain unauthorized access. |
| Worm | An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. |
| Zero-day exploit | A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no known fixes. |

**Table 1. Types of Cyber Weapons**[28]

Fourth is attribution of the attack. In the other four domains, either the direct observation of the attack or the analysis of physical evidence will usually determine who is responsible. Examples abound but the Chinese anti-satellite test in January 2007,[29] and the North Korean sinking of the South Korean patrol boat Cheonan,[30] both demonstrate the ability to accurately determine the method and source of attacks, even when the adversaries respectively initially remain silent or continuously deny culpability. This is much more difficult in the cyber domain. The Deputy Secretary of Defense, William Lynn, stated very succinctly:

> *Whereas a missile comes with a return address, a computer virus generally does not. The forensic work necessary to identify an attacker may take months, if identification is possible at all.*[31]

Even when the attack can be tracked to a point of origin while the attack is taking place, often the computer or server being used is not in the same State as the attacker. A frequent tactic is to use Robot Networks or "botnets" – computer systems used for attacks unbeknown to their legitimate owners.[32] Due to a number of factors such as current technology, the way internet communicates, and the use of willing and unwilling third parties, attribution of an attack to a nation-state aggressor is extremely difficult.[33]

However, there is one more salient point regarding domain differences that must be made. Any State may attack any other State in space, air, land, or sea if it so chooses. If the State is willing to bear the cost of developing the force and using it, the domain itself will usually permit it. This is not so with the cyber domain. Because of the low cost and current ease of attack in cyber, this statement may seem extremely odd. But attack in cyber is only possible because of vulnerabilities in the software code and the user's settings. Whoever gains illicit entry into a system only does so because a pathway exists. There is no such thing as a "forced entry" in cyberspace. A State and its inhabitants can only be attacked in the cyber domain if they allow it.[34] This fact is not lost on the Chinese who have undertaken an effort to secure their part of the internet with a unique operating system and designated choke points.[35] The U.S. Government also recognizes this which accounts for statements in the 2010 Quadrennial Defense Review like "DoD

must actively defend its networks." Or "Joint Forces will secure the .mil domain" in the 2011National Military Strategy. These observations lead us to explore the roles and responsibilities of defending U.S. Cyberspace.

## Defending U.S. Cyberspace

The defense of the non-.mil portion of U.S. Cyberspace is primarily the responsibility of civilian agencies and private entities. The Department of Homeland Security has the lead but is supported by the Department of Justice, the intelligence community, and others. Corporations are responsible for their own security but are encouraged to coordinate and cooperate with the government. It is worth noting the only entity that can take offensive actions (armed force) is the government. Private citizens, corporations, etc. are not authorized to stage cyber attacks of their own – not even in retaliation.[36]

A review of current United States Code gives a glimpse of the division of roles and legal responsibilities within the United States Cyberspace (see Table 2). This fractionalization of cyber defense creates a situation where no military service has primary responsibility for the domain – unlike all of the other domains. A plans officer pointed out that if we used this scheme of defense in land warfare, an "invasion of New Jersey would have to be fought by U.S. citizens and commercial entities with whatever weapons they happened to possess. DoD would only defend Ft. Monmouth and Dix."[37]

The ability to respond to an act of war, however, resides exclusively with the government of the United States. To date, however, this has not been well defined for the cyber domain. The 2001 Authorization for Use of Military Force, passed by Congress in the wake of the 9/11 attacks, does seem to grant the President some authority to conduct cyber defense efforts against cyber terrorism.[38] However, it contained little guidance regarding acts of war within the cyber domain. What can or cannot be done in the name of national defense by the executive branch then depends greatly upon this connection to the President's war powers.[39] This is another reason why an understanding of what constitutes an act of war in and out of the cyber domain is important.

| U.S. Code | Title | Key Focus | Principal Organization | Role in Cyberspace |
|---|---|---|---|---|
| Title 6 | Domestic Security | Homeland Security | Department of Homeland Security | Security of U.S. Cyberspace |
| Title 10 | Armed Forces | National Defense | DoD | Secure U.S. Interests by Conducting Military Operations in cyberspace |
| Title 18 | Crimes and Criminal Procedure | Law Enforcement | Department of Justice | Crime Prevention, Apprehension, and Prosecution of Cyberspace Criminals |
| Title 32 | National Guard | First Line Defense of the United States | Army National Guard, Air National Guard | Support Defense of U.S. Interests Through Critical Infrastructure Protection, Domestic Consequence Management and Other Homeland Defense-Related Activities |
| Title 40 | Public Buildings, Property, and Works | Chief Information Officer roles and Responsibilities | All Federal Departments and Agencies | Establish and Enforce Standards for Acquisition and Security of Information Technologies |
| Title 50 | War and National Defense | Foreign Intelligence and Counter-Intelligence Activities | Intelligence Community Aligned Under the Office of the Director of National Intelligence | Intelligence Gathering Through Cyberspace on Foreign Intentions, Operations, and Capabilities |

**Table 2. Cyber Roles**[40]

Of course, defining what the military is allowed to do in the construct of defending the cyber domain is greatly impacted by this understanding as well. A great deal of effort has gone into creating organizations, doctrine, and tools to defend military networks. When can the military use this expertise to help defend the nation's networks in general? During a war of course, but under what conditions is a cyber attack an

act of war? As you can see, the answer to this question is no longer of interest to just legal philosophers or war college professors.

Secretary of Defense Robert Gates acknowledged that the nation's dependence on cyberspace represented a new element of risk to our national security. To address this risk and to synchronize "warfighting effects" in cyberspace, he created the U.S. Cyber Command under U.S. Strategic Command. Cyber Command is now responsible for U.S. military cyberspace operations and provides support to domestic civil authorities and international allies.[41]

The President's direction is found in the May 2010 NSS: "We will work with all the key players – including all levels of government and the private sector, nationally and internationally – to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents. Just as we do for natural disasters, we have to have plans and resources in place beforehand."[42] This is a tall order considering that no one is completely sure where the boundaries lie between all of the agencies and levels of government. How can they? The cyber domain is characterized by a lack of boundaries. A fictional but very realistic example: Data stored on servers in Holland is used by engineers in the United States to research where the next oil well should be drilled in waters off the Nigerian coast. This research is then hacked by someone using an IP address assigned to a university in Russia and later a Chinese joint venture bids on the Nigerian oil lease drilling project with what appears to be the U.S. engineer's estimates. Was this a crime, an act of espionage, a threat to national security or all three? Who has the authority to defend against the attack, investigate the theft of data, and determine the culpability of any alleged parties to the attack? How does any one agency determine these answers?

Work done by James Michael and George Mason University has resulted in the creation of a decision matrix that helps organizations respond to cyber-attacks in a legally appropriate way.[43] The model breaks all cyber intrusions into one of three legal paradigms or categories: Law Enforcement governed by the U.S. Constitution and Titles 18 and 15 of the USC; Intelligence Collection governed by Title 50 USC and Executive Order 12333; or Military Operations governed by Title 10 USC. While the matrix is extraordinarily useful as a tool

for determining what the legal rules are before conducting a response to a cyber-attack, James Michael openly admits that the answers to the questions of who is conducting the attack and why are critical but are often unavailable, especially during and in the immediate aftermath of the attack.[44] This leaves us with the practical problem of who has the responsibility to make the decision regarding who responds to the cyber-attack.

**Who Determines Acts of War?**

Declaring that an act of war has occurred is not the same as declaring that a crime has taken place. In the event of a serious crime in the United States, police officers collect the evidence which is then often evaluated by detectives and technical experts. Suspects are identified, pursued, and arrested. The results of the investigation are delivered to the prosecutor who, after review, may file charges in a court of law. A judge determines if there is sufficient evidence to warrant a trial. If so, a trial occurs with a presentation of evidence before a judge and a jury of citizens who determine if guilt has been established beyond a reasonable doubt.[45]

Declaring that an act of war has taken place contains few of these elements. Some acts of war are investigated such as the Gulf of Tonkin (1965) or the 9/11 attacks (2001). Most do not require it as the facts on the ground make the action obvious such as Iraq's invasion of Kuwait (1990), Japan's bombing of Pearl Harbor (1941), and the North Korean invasion of South Korea (1950). Regardless if there is a formal investigation or not, who are these facts delivered to? What court has the authority to authorize a war? What jury determines if the alleged act has actually taken place and the suspected party is guilty beyond a reasonable doubt? What judge determines the punishment of the guilty party and using what guidelines? Who is to carry out the sentence?

The answers are that no court system or international mechanism exists to fill these roles. While some may point to the United Nations General Assembly and Security Council as sources of authority to conduct a war, these are political bodies and not judicial ones.[46] Facts are presented to the court of public opinion (national and international), and nations

take it upon themselves to carry out whatever sentence they feel is appropriate and capable of carrying out.[47]

So we return to the critical question of how to determine if a cyber-attack is an act of war or not. No international court will make the determination for us and the costs of getting it wrong can be severe. The mistaken belief that the U.S. Navy had been deliberately attacked a second time in the Gulf of Tonkin in 1964 provided the spark for the U.S. Senate passing a resolution approving the use of force against North Vietnam. While not the only factor causing the war, it was the galvanizing moment that authorized the President to send hundreds of thousands of American serviceman into combat.[48] The outcome, eight years later, was the waste of over 58,000 U.S. lives and 150 billion dollars.[49]

Multiply the confusion of that night in the South China Sea on 4 August 1964 by a magnitude of 10 and one begins to approximate the difficulty of making decisions regarding acts of war in the cyber domain. We must depend on international norms, conventions, and laws to assist us in that determination. Perhaps the most relevant document regarding acts of war with the widest acceptance among the nations of the world is the Charter of the United Nations.

**International Law**

It is essential to understand that the UN Charter does not prohibit the use of force. It does, however, prohibit the use of aggressive force.[50] There are four articles that bring light to this issue. The first, appropriately enough, is Article 1 as it enumerates the purposes of the United Nations (UN).

> *To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.*[51]

Even though this article does not mention war or even the use of force between nations, it has relevance. The member nations established the UN to maintain international peace. It makes the avoidance of, or failing that, resolution of breaches of the peace the primary purpose of the UN. If we construe cyber attacks as a breach of the peace, they then fall under the purview of the UN and its charter. Recalling from earlier the economic impact of cyber attacks on the United States alone, it is a fair assessment to state that peace has been breached.

The next Charter article of interest is Article 2(4). It states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state..."[52] It is noteworthy that this article offers no mechanism of relief from an aggressor. It does not authorize defense, retaliation, or any other response to force against your State. It merely prohibits force against another State.[53]

So is a cyber attack considered a use of force? We need to be careful in our response as this is a double edged sword. If someone is attacking the United States the temptation is to swiftly answer "yes." However, a finding that cyber attacks are indeed considered a use of force then the United States is forbidden from engaging in that activity itself under this article. To provide an answer to this question we must first understand what the UN Charter means by "force." Is it any kind of force such as diplomatic, economic, and military or is it just military (armed) force?

Michael N. Schmitt, a professor of International Law and former Air Force Judge Advocate published a research paper on this issue for the United States Air Force Academy's Institute for Information Technology in 1999. His analysis of UN documents, including minutes of the original 1947 meetings, as well as follow-on General Assembly Resolutions, other international treaties, and customary international law, concluded the term "force" under current international law most closely means "armed force" and not diplomatic, informational, or economic.[54] Other legal scholars concur in this interpretation, one using the term "aggressive force" in lieu of "armed force" but with a similar conclusion to Schmitt's.[55]

So now we modify our question to this: Is a cyber attack considered a use of armed force? We turn to Article 41 of the Charter which delineates all of the actions member nations may take against an aggressor nation that do not involve armed force. These actions include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[56] This indicates that at least some forms of cyber attack do NOT fall into the description of armed force – particularly the denial of service attack. The ramification of this is the United States could employ this form of cyber attack to temporarily block access to a website that posed a threat to U.S. interests without crossing the Article 2(4) prohibition of the use of force. Of course, that enables others to do the same to the United States.

We cannot, however, state unequivocally that all forms of cyber attack have been eliminated from the "armed force" category. For example, any cyber attack that aims to kill or injure people or cause damage to physical property clearly is a use of armed force.[57] This is exactly what many experts and policy makers are concerned about when they discuss Critical Infrastructure Protection (CIP) and Supervisory Control and Data Acquisition (SCADA) systems. A well executed cyber attack that is able to gain control of the system or the data it uses to control critical infrastructure (such as an electrical power grid, locks or gates of a dam, water supply system, transportation system) could quite easily cause widespread destruction and human fatalities.[58]

This is not a theoretical discussion – an incident of computer warfare from the Cold War demonstrates what armed force looks like when executed against critical infrastructure via software code. A former director of the National Reconnaissance Office, Thomas Reed, recounts the following incident from 1981 in his memoirs. The Soviets were years behind the West in computer technology. They had a desperate need to obtain hardware and software that could regulate natural gas as it was shipped from the fields to storage to pipelines and into Eastern Europe. Because this was a significant source of income for the Soviets, the KGB was tasked to steal the relevant software from a Canadian company. Tipped off by the French, the United States and Canada modified the software before the KGB "acquired" it.

> *Once in the Soviet Union, computers and software, working together, ran the pipeline beautifully – for a while. But that tranquility was deceptive. Buried in the stolen Canadian goods – the software operating this whole new pipeline system – was a Trojan Horse. (An expression describing a few lines of software, buried in the normal operating system that will cause that system to go berserk at some future date or upon the receipt of some outside message.) In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space. At the White House, we received warning from our infrared satellites of some bizarre event out in the middle of Soviet nowhere. NORAD feared a missile liftoff from a place where no rockets were known to be based.*[59]

This manipulation of the SCADA was not accomplished by means of a cyber attack but it clearly demonstrates the potential result from the insertion of malware via the internet. Had the trojan horse been delivered through a cyber attack, it clearly would have been an armed force and, possibly, a *casus belli*. In other instances of malware infecting a control system, the end result was not nearly so dramatic. So it is not the method of cyber attack that matters but rather the direct result of that attack.

We are beginning to develop some boundaries as to when a cyber attack meets the definition of armed force. Clearly some types of attack meet the definition while others do not. Before we further delineate which ones do, we need to examine one last article, Article 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations..."[60]

This article grants member nations the right to defend themselves using all means necessary – including armed force. Once the State is attacked, it may respond with its own attacks against the aggressor

without violating the UN Charter. This raises the ante in defining cyber attacks as armed force as that will enable an armed force response. There is no restriction in Article 51 as the type of attacks undertaken in self-defense. While proportionality is generally expected, the response does not have to be symmetrical. Forces in any domain may be used separately or together – the defense is not limited to the cyber domain.

It is clear that a State or the UN Security Council should take great care in labeling a cyber attack as something that amounts to an armed force. The situation could escalate to the level of an international crisis and possibly degenerate into armed conflict across the spectrum of domains. This is assuming that a clear and convincing case of attribution can even be made in the first place. As discussed earlier, finding the true culprit in a cyber attack is far more difficult than in the other domains. We should also note that espionage is considered a crime, not a use of armed force. Planting a trojan horse that extracts data is a cyber attack and punishable as a felony but it is not armed force or an act of war.[61]

In 1999, Schmitt made the observation that the UN Charter specifically forbids the use of armed force in most situations (permitted in self-defense and when the Security Council authorizes it to end a breach of the peace). But it intentionally excludes from this prohibition the use of coercive force types listed in Article 41. If economic and political coercion are not considered armed force then we have additional criteria to determine whether a cyber attack's effects cross the line of demarcation between a crime and armed force.[62]

Further refinement of that line requires additional criteria. It is time to introduce Dr. Schmitt's analysis and seven factors and then we will use them in a brief case study of events in Estonia in 2007.

**Schmitt's Analysis**

Schmitt's 1999 analysis was updated in 2010 and delineated seven factors that can guide a State to define whether or not a cyber attack meets definition of a use of force.[63] While there is a lack of consensus in this area,[64] his criteria provide an admittedly subjective framework to evaluate the cyber action as a potential *casus belli*. The factors are

severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.[65]

Severity is exactly what it sounds like – how significant were the effects of the attack? As discussed above, a denial of service attack is not going to meet the standard of armed force but a disaster like the Soviet gas pipeline explosion could. There must be harm to individuals and property. The degree to which the attack impacts the nation in terms of economic cost, societal cost, and length of time will affect the calculation of severity.[66]

Immediacy reflects the concern about the rapidity of consequences from the attack. An economic embargo, for example, has consequences that build slowly over time, allowing the affected State to make rational choices on how to avoid further harm. A cyber attack that has a similar effect would not qualify as an armed force. However, one that had immediate significant and severe effects could.[67]

Directness measures the connectivity between the initial act and the result. Again, to use the embargo as example, the eventual consequences of deprivation of a particular good are impacted by other market forces as well as innovation to replace the good. An armed attack, in contrast, results in direct harm to people and property.[68]

Invasiveness addresses the degree to which the aggressor has penetrated the State's sovereignty. The economic embargo entails no penetration, an air raid or land invasion involves the other extreme. The deeper the cyber attack resides within U.S. Cyberspace, the greater the invasive aspect, the greater the violation of sovereignty.[69]

Measurability concerns how well and accurately the State can quantify the damage it has suffered as a result of the attack. If it is difficult to point out visible damage in terms of destruction and death, then the State will find proving the negative consequences to the world community be difficult.[70]

Presumptive Legitimacy reflects the state of international law regarding permissive actions by States. In short, if it is not prohibited, it is presumed to be legitimate. Since international law "does not prohibit

propaganda, psychological warfare, or espionage, those activities in the cyber domain are presumed to be legitimate."[71]

Responsibility addresses the level to which the Aggressor State was involved in the cyber attack. This is directly related to problem of attribution mentioned above. The closer the Victim State can tie the attack to the Aggressor State, the more likely the cyber attack will be recognized by the international community as a prohibited armed attack.[72]

Now that we have defined Schmitt's seven factors, let's apply them to a real world situation and make a decision as to whether it was an act of war or not.

**Applying the Schmitt Analysis - Estonia**

Examining a historical example of a cyber attack may be the best way to illustrate how these criteria can be used to make a determination as whether a *casus belli* exists or not. On April 26, 2007, the Estonian government moved a World War II Soviet Army memorial out of the center of Tallinn, the capital city. This move was seen as anti-Russian and was extremely unpopular with the Russian public and ethnic Russians living in Estonia. The cyber attacks began on April 27 and lasted for three weeks. The attacks were primarily distributed denial of service attacks and disrupted banking, government communications, and e-mail services. Estonian news media, universities, and other government agencies were all victims of the attacks. Web defacement also occurred on official government websites.[73]

Although the sources of most of the attacks were from Russia, the Russian government denied responsibility. Despite accusations from the Estonian government, intense post attack investigations have yet to demonstrate a connection with the Russian government. One individual was identified, charged and convicted under Estonian law but the many others involved have escaped retribution.[74] So was this attack a use of armed force? Did the cyber attacks cross the line and become an act of war?

Using the Schmitt analysis, this author unequivocally believes that the answer is no because of a lack physical damage or death. Ironically, Schmitt himself wrote in a 2010 article that he believes the answer could be yes for the reason that the attacks frustrated Estonian government and economic functions.[75] While it is slightly intimidating to disagree with a renowned expert on this subject, let's go through the factors:

- ***Severity.*** While the 3 week length of time is considerable (especially for a cyber attack), there were no facilities destroyed or lives lost. Admittedly the annoyance factor was extremely high and many citizens' lives and businesses were significantly impacted but no permanent damage was done.[76] As Schmitt himself points out, this is the most significant of the seven factors and "consequences involving physical harm to individuals or property will alone amount to a use of force."[77] Since physical harm did not occur, ergo no use of force occurred and no *casus belli*.
- ***Immediacy.*** The attacks occurred without warning and less than 24 hours after the protested action (removal of the statue) took place. The effects of the attacks occurred with great rapidity.[78]
- ***Directness.*** It was quite clear that the negative effects of the attacks – loss of communications, etc. were directly caused by the cyber attacks and were not enhanced by indirect factors.
- ***Invasiveness.*** The cyber attacks were definitely within Estonian Cyberspace. The attacks clearly originated outside of the State and were flowing through Estonian servers and communications circuits. Proof of this was provided when Estonia cut all international data circuits coming into the country and nearly all cyber attack activity immediately halted.[79]
- ***Measurability.*** While economic harm can be somewhat quantified it is important to recall from our discussion above that economic coercion is not seen as a use of armed force by the UN. Schmitt himself agrees that this is the case "even though it (economic coercion) may cause significant suffering."[80]
- ***Presumptive Legitimacy.*** Since propaganda, psychological warfare, and espionage are not considered prohibited forces under international law – we must examine the actual effects of the attacks upon Estonia. Web defacement is a form of propaganda;

interruption of the mail and communications are not considered armed force by Article 41 of the UN Charter, and the continuous denial of access to these functions is a form of psychological warfare. While the conduct was criminal, it was not necessarily a use of armed force.[81]

- ***Responsibility.*** While a connection to the Russian government has not been proven, even if it was, the cyber attacks simply do not rise to the definition of armed force. If this was a State sponsored action, it would have certainly brought the declaration of a breach of the peace, but without physical injury or destruction of physical property, there is no armed force and thus no *casus belli*. It is also worth noting that although Estonia is a member of NATO, Article 5 of the North Atlantic Treaty (common defense of a member against an armed attack) was never invoked.[82]

We could repeat this exercise for any number of cyber incidents such as the Stuxnet Worm that damaged Iran's centrifuge machines that enrich uranium,[83] or the cyber attacks that accompanied the very kinetic land/air attacks in Georgia in 2008.[84] In each case we would derive a valid, even if subjective, answer. The seven factors of Schmitt's analysis can provide an answer to that ever elusive question: When is a cyber attack an actual act of war? We now turn to what we should do with this information in the form of some recommendations to the U.S. government and a conclusion.

**Recommendations**

Based on the preceding discussion and analysis, the United States Government should adopt the seven factors of Schmitt's analysis to evaluate the impact of cyber attacks upon U.S. Cyberspace to determine if a *casus belli* exists. Furthermore, if an offensive cyber action is considered, Schmitt's analysis should also be conducted to determine if U.S. actions would constitute an armed attack under the UN Charter.

First, Schmitt's analysis should be structured into a matrix with as many objective criteria inserted as possible to improve the rapidity and accuracy of decisions being made based on the seven factors. Each of the factors need to be refined with guidance and examples that narrow

the level of interpretation required as to whether the cyber activity in question crosses or does not cross the line of armed force. While the analysis is ultimately subjective, the more objective it can be made, the higher the fidelity of advice based on the model will be.

Second, the analysis needs to be included or referenced in a number of documents to become the framework that all government agencies reference when making recommendations. The National Strategy to Secure Cyberspace and the Comprehensive National Cybersecurity Initiative both affect multiple agencies across the government and should be updated with the analysis. One of the primary Department of Defense documents that should also reflect this change is the National Military Strategy for Cyberspace Operations (NMS CO). Changes to derivative documents like the NMS CO implementation plan, the USSTRATCOM Campaign Plan and the USCYBERCOM OPORD will bring the analysis to the operational levels of DOD. Based on the guidance contained in these documents, the Judge Advocate General (JAG) Corp will need to recommend amendments to the Standing Rules of Engagement (SROE) and any specific ROE that are currently being used in support of cyber operations. The need for this was reflected in a statement to Congress by the USCYBERCOM Commander, General Keith Alexander, in November 2010. He confirmed that there are still "no clear rules of engagement clarifying what cyber activity might trigger an armed cyber response from the United States."[85]

Finally, all military and civilian agency leaders who are charged with taking actions in cyberspace or will be advising the President regarding acts of war in cyberspace must be made familiar with the Schmitt Analysis. Even though opinions will vary among government leaders, having a common set of criteria to work with will standardize the reference terms, concepts, and understanding of the issues involved and will aid in rapid decision making.

## Conclusion

This paper addressed the need to determine if a cyber attack is a crime or act of war. It defined the terms of cyber attack and cyber war in such a way to support the idea that all attacks are not a *casus belli* but include a wide array of actions such as terrorism, espionage, and more

mundane crimes such as fraud. Characteristics of the cyber domain make situational awareness and attribution of attacks difficult. Though we are aware of the standard tools of cyber attacks, we are still plagued with vulnerabilities in cyberspace that are taken advantage of by criminals and adversaries.

A review of the statutory guidance revealed that each type of cyber attack is dealt with by a different agency within the government, even though during the attack, no one may be aware of which type of event it is. Indeed, the initial detection and notification is likely to be by private entities such as corporations. Regardless of what damage has occurred to whom, only the President as Commander-in-Chief may authorize the use of force in retaliation. But he has to be advised as to what types of force in the cyber domain are considered "armed force."

A review of international law revealed that cyber attacks can rise to the level of an armed force and thus be a *casus belli*. The seven factors contained within Michael Schmitt's analysis are a viable framework for helping decision makers reach that determination.

The vast majority of cyber attacks occurring against and within U.S. Cyberspace are criminal acts or espionage. But for those few events, either current or in the future, that has the characteristics of an armed force, recommendations and courses of action will need to be provided to the President in his Commander-in-Chief role. The foundation of those recommendations must be as firm as possible and the Schmitt analysis provides a method to do that.

# Securing Cyberspace: Approaches to Developing an Effective Cybersecurity Strategy

**Lieutenant Colonel Douglas S. Smith**
United States Army Reserve

CYBERSPACE HAS BECOME part of the fabric of the modern world. Internet usage is growing exponentially, from one million internet users in 1992, to 1.2 billion users in 2007, to over two billion in 2010.[1] Society increasingly relies on cyberspace tools to regulate infrastructure critical to daily life, such as electric power grids, global finance, banking, transportation, healthcare, and telecommunications. The nation's military depends on networks for command and control, communications, intelligence, logistics and weapons systems. Although few would deny the benefits that cyberspace has brought to nearly every facet of life, reliance on free access to cyberspace makes society vulnerable to disruptions caused by malicious attackers, cyber-criminals or even teenage hackers.

Protecting cyberspace is a national security priority. President Obama's National Security Strategy (NSS) acknowledges that threats to cyber-security "represent one of the most serious national security, public safety, and economic challenges we face as a nation."[2] The Quadrennial Defense Review (QDR) Report states that in the 21st century, "modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace."[3] These statements support the assertion that the United States has a vital national interest in cyberspace, with free and unencumbered access for innovation, global commerce and communications, and with robust security to protect the digital infrastructure that powers critical national functions. The NSS articulates the strategic objective that supports this interest: "[D] deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks."[4] A comprehensive cyber-strategy is needed to achieve this objective (ends) that includes conceptual approaches (ways) in three broad areas:

1. U.S. government and military policies for cyberspace defense
2. International influence in cyberspace
3. Deterrence of cyber-attacks

## The Nature of Conflict in Cyberspace

Development of a comprehensive cybersecurity strategy requires an understanding of cyberspace and the nature of conflict within it. This section discusses definitions for cyberspace, cyber-power, cyber-attack and cyber-exploitation and recent examples of how cyber-conflict has embroiled the physical world.

Since the term was coined in 1984,[5] *cyberspace* has been described in numerous contexts within science fiction, academia, government, and the military. Many sources describe cyberspace as a global operational domain and compare its qualities to the physical domains: land, sea, air and space. Human utilization of each domain followed from technological innovation. The space domain, for example, was unimportant to society before development of rockets and satellites. Today's communications would be impossible without operational capabilities in space. Advances in electronics and computers created cyberspace, the first man-made domain, and opened it to human exploration and exploitation.

The Joint Chiefs of Staff define cyberspace as a global domain within the information environment, encompassing the "interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] The domain is framed by "the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information."[7] The implication of this definition is that cyberspace represents not just the technical aspects of the medium, such as networks and computers, but also the information itself and the human element that shapes and interprets the information.

Protecting strategic interests in cyberspace requires effective application of cyber-power. Daniel Kuehl, Director of the Information Strategies Concentration Program at the National War College, defines cyber-

power as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[8] This definition is reminiscent of Mahan's concept of sea-power: "[A] nation's ability to enforce its will upon the sea."[9] The nation wielding sea-power has capabilities to guarantee free access across the oceans for its own purposes and interests and to prevent adversaries from impeding the same. Similarly, the nation wielding cyber-power has capabilities to patrol cyberspace and take actions to secure its own interests within cyberspace and prevent adversaries from impeding the same. Unlike the physical domains, however, cyberspace creates effects in all five domains. Consequently, cyber-power is applicable to all operational domains and all elements of national power.

Conflict in cyberspace can occur in one of two forms: cyber-attack or cyber-exploitation. Although there is no consensus of what constitutes a cyber-attack, all are comprised of a deliberate action taken to "alter, disrupt, deceive, degrade, or destroy" systems or networks in cyberspace.[10] The scale of attacks can vary widely, ranging from the inconvenience of being locked out of a network to complete shutdown of critical control systems.

Cyber-attacks share four important characteristics.[11] First, the indirect effects of the attack are often more consequential than the direct effects. An attack against the controls of a power grid, for example, could cause blackouts, similar to what might occur during natural disasters. The indirect effects might outweigh the direct effects, such as interruptions to commerce, creation of opportunities for crime, public outcry and reduced investment. For example, cyber-attacks to the power grid caused several wide-spread blackouts in Brazil and Paraguay in 2005, 2007, and 2009. Although the most recent outage only lasted for two hours, the incident created the perception that the infrastructure in South America is vulnerable. International perceptions disproportionately bruised Brazil's reputation, undermining confidence in their ability to safely host the 2016 Olympic Games and soccer's 2014 World Cup.[12]

Second, the technology to launch a cyber-attack is relatively inexpensive and readily available. As a result, non-state actors have adopted cyber-attacks as a weapon of choice. Small groups can develop sophisticated capabilities to conduct cyber-attacks against large, well

resourced entities for economic or political purposes. For example, a three-week cyber-war raged in Estonia in 2007. The dispute erupted when Russians protested the Government of Estonia's announcement that it would remove a Soviet war memorial, the "Bronze Soldier of Tallinn."[13] Russian hackers attacked numerous government agencies, banks, and news organizations, intermittently shutting down networks and disrupting life in Estonia.[14] The attacks appeared to be perpetrated by Russian individuals inside and outside of Russia, without proven support from the Russian Federation. The conflict illustrates what cyber-war may look like in the future: small, technically advanced groups attack the digital infrastructure of nations in pursuit of a political objective.

Third, cyber-attacks may be highly asymmetric. A common weapon in cyberspace is the *botnet*, a large number of infected computers remotely controlled by a master computer. A botnet grows when a virus infects ordinary computers across the internet, creating virtual links between them without users' knowledge. The perpetrator can remotely activate his army of computers against specific targets, to overwhelm networks, block or disrupt access to systems, or infect other computers and networks.[15] One example is the Mariposa botnet, made up of 13 million infected computers, created and controlled by just a few individuals.[16] After infecting an unsuspecting computer, the program monitored activity for passwords and banking and credit card information. The internet's openness allows a single user to amplify his influence.

Fourth, perpetrators can conceal their identities with relative ease if they seek anonymity. For example, the Conficker Worm is a propagating and mutating virus that has infected an estimated 10 million computers, creating the framework for a powerful botnet ready to launch an attack at its creator's signal. Despite unprecedented international collaboration and even a bounty offer standing since 2009, the identity and motives of the worm's creators remain a mystery. A botnet this large could theoretically, "paralyze the infrastructure of a major Western nation."[17]

Cyber-exploitation involves the use of offensive actions within cyberspace but unlike cyber-attacks normally does not seek to disrupt the normal functioning of the targeted network or systems. The objective of cyber-exploitation is usually to obtain information for illegitimate

purposes, including espionage, theft of confidential information such as credit card or personal information, or other criminal reasons.[18] For example, China has directed cyber-espionage efforts against the U.S. Department of Defense since 2002, with successful theft of 10 to 20 terabytes of data from military networks.[19]

As the world becomes more interconnected, cyber-power increasingly is "exerting itself as a key lever in the development and execution of national policy."[20] An effective cyber strategy will benefit numerous national efforts, including counter-terrorism, economic development, fighting crime, diplomatic engagement, and intelligence gathering.

**U.S. Government and Military Policies for Cyberspace Defense**

Governance of cyberspace is an elusive concept. The term *governance* is misleading because governments currently exercise little control over internet policy or protocols. Instead, an evolving collection of private and commercial organizations determine policies and protocols by consensus to keep the internet functioning smoothly. One such organization is the Internet Corporation for Assigned Names and Numbers (ICANN), a private, non-profit corporation responsible for assigning domain names, the unique identifier that gives information a place to exist on the internet ("www.microsoft.com," for example, is the assigned domain name for the Microsoft Corporation). ICANN has a government advisory committee open to any national government, but members may only advise ICANN's Board of Directors and do not have voting rights on board policies.[21] Other forums are responsible for other cyberspace functions, such as communications standards and core internet functions.[22] These organizations have evolved in an ad hoc manner driven mainly by the need to resolve technical issues. But where once technical problem-solving was an academic notion necessary for establishing cyber infrastructure, today the need to fight cyber-exploitation and cyber-attack lends a heightened urgency for proper conduct within cyberspace. Given the present state of governance, public policy-makers should seek to develop greater influence on certain aspects of cyberspace, rather than adopt true governance.[23] Government initiatives should include three approaches to cybersecurity:

1. A differentiated approach to security policy
2. A centralized approach to protect military cyber-assets under U.S. Cyber Command
3. A holistic interagency approach, as begun with the Comprehensive National Cybersecurity Initiative

First, the U.S. government should develop a differentiated approach to cybersecurity, with the intent of prioritizing the wide variety of cyber-attacks and cyber-exploitations and appropriately focusing counter-measures. The first step is to prioritize cyber-attacks and cyber-exploitations with regard to their possible consequences. On one end of the spectrum are the nuisance hackers who probe networks thousands of times each day. On the other end is the sophisticated cyber-attack that causes damages commensurate with an act of war. This approach should classify cyber capabilities as *indispensable*, *key* or *other*. *Indispensable* cyber would include critical military capabilities or civil security capabilities that the country could not be without even for a short time.[24] *Key* cyber also include critical infrastructure but for which temporary workarounds are possible. This may include electric grids, financial networks, transportation systems, and certain military or intelligence capabilities whose exploitation would damage national security. The vast bulk of cyber capabilities remaining would fall into the *other* category. Next, security measures should be tailored for each category. For *indispensable* cyber, the federal government should provide security directly. Activities should include actively monitoring for attacks, providing cyber defenses and redundant systems. For *key* cyber, the federal government should develop policies and regulations that require minimum levels of protection for cyber capabilities that reside with private or state control and provide adequate resources for law enforcement and security cooperation with entities that have responsibility for key cyber capabilities. For *other* cyber, the government could encourage improved cyber-security through education, incentives, or voluntary participation in government security programs.

Second, U.S. Cyber Command (CYBERCOM) has assumed responsibility for protection of critical government and military cyber assets. It achieved full operational capability on November 3, 2010, as

a four-star, sub-unified command under U.S. Strategic Command.[25] CYBERCOM's three-prong mission is to:

1. Operate and defend DoD networks
2. Prepare to conduct full-spectrum military cyberspace operations
3. Defend U.S. freedom of action in cyberspace[26]

CYBERCOM executes its first mission with a layered defense of the Global Information Grid (GIG). The outer most layer of protection is "ordinary hygiene," which includes keeping malware protection, firewall, and anti-virus software up to date on 15,000 networks within the .mil domain and seven million computers.[27] Diligent hygiene blocks about half of attempted intrusions. The next line of defense is "perimeter security," which monitors traffic in and out of DoD networks.[28] CYBERCOM has limited the number of access ports to DoD systems from the internet, creating cyber choke points where it can more effectively marshal defenses. Perimeter security blocks an additional 30-40% of attempted intrusions. Finally, CYBERCOM conducts dynamic defenses to block the last 10% of attempted intrusions. Dynamic defense systems act in real-time as "part sensor, part sentry, part sharpshooter."[29] They continuously monitor traffic, automatically identify intruders and block access. In contrast, static defenses, such as hygiene activities, wait and react to intruders after they have penetrated the network. The National Security Agency (NSA) leads the initiative to develop dynamic defenses. In addition to technical capabilities, NSA will incorporate foreign intelligence to anticipate threats. Effective unity of effort is possible with U.S. Army General Keith Alexander acting as both CYBERCOM's Commander and NSA's Director. A challenge remaining for CYBERCOM will be to develop mechanisms to extend cyber protection to key cyber capabilities that reside outside of DoD-controlled networks. Although General Alexander cites the importance of the principle, he admits that older cyber-systems powering electric grids, banking and transportation systems are inherently more difficult to defend.[30] The military also depends on commercial and unclassified networks for much of its communications and records-keeping. Lessons learned from CYBERCOM's efforts to protect the GIG should be applied to cyber-security for critical civilian sectors.

Third, the United States should pursue a holistic interagency approach to cybersecurity. The Comprehensive National Cybersecurity Initiative (CNCI) is an excellent template for success. The initiative was launched by the Bush administration in January, 2008, in response to a series of cyber-attacks on multiple federal agency networks. It was intended to unify agencies' approach to cybersecurity. Under the Obama administration, it has evolved into a broader cyber-security strategy. The CNCI defines 12 initiatives to facilitate collaboration among federal and state governments and the private sector that ensure an organized and unified response to cyber attacks.[31] For example, the Trusted Internet Connections program, an initiative led by the Office of Management and Budget and the Department of Homeland Security (DHS), consolidates access ports to federal government systems, much as CYBERCOM has done for military systems.[32] Fewer access ports are more easily monitored and defended. Another initiative involves deployment of an intrusion detection and prevention system for civilian government networks. Developed by DHS, the EINSTEIN 2 program was deployed to automatically detect unauthorized or malicious network traffic across U.S. Government networks and send real-time alerts to the U.S. Computer Emergency Readiness Team (US-CERT), the operational arm of the National Cyber Security Division within DHS charged with coordinating the federal response to cyber-attacks.[33] DHS is also working to pilot technology developed by the NSA as EINSTEIN 3, to conduct "real-time full packet inspection and threat-based decision-making" with the ability to automatically respond to cyber threats before harm is done.[34] Another initiative calls for connecting strategic cyber operations centers to enhance situational awareness across agency networks and systems and foster interagency collaboration and coordination. The intent is for the National Cybersecurity Center within the DHS to connect six existing cyber centers within DHS, DoD, FBI, NSA, and Office of Director of National Intelligence to share information with each other through relationships and liaison officers.[35] Together, the centers create common situational awareness among key cyber functions, including cyber-intelligence, counter-intelligence, cyber-crime investigation and law enforcement, civil and defense collaboration, and intrusion detection and response.

These initiatives show remarkable progress on creating a holistic, interagency approach to protecting government systems against cyber-attack. Like other interagency efforts, however, the CNCI will be challenged by competing agency interests, control of significant resources targeted for cybersecurity, and by public debate about the proper role for federal regulations. In 2009, for example, the Director of the NCSC resigned in protest of the increasingly prominent role played by the NSA in cyber efforts. He argued in favor of checks and balances by separating security powers among government agencies, and cited "threats to democratic processes…if all top-level government network security and monitoring are handled by any one organization."[36] This initiative continues amid public debate on the appropriate role that government oversight and control should play in balancing protection against cyber-attack with free and open access to cyberspace.[37]

**International Influence in Cyberspace**

Private sector entities and individuals have few effective and legal alternatives to respond to a cyber-attack or cyber-exploitation. The first line of defense is to strengthen their passive defensive measures, including dropping services that are targeted or closing firewall ports to deny access to key systems. These measures cannot completely protect systems against increasingly sophisticated attackers and deny the victim the benefits of key services or connections.[38] The second option is to report the cyber-attack or cyber-exploitation to the authorities for prosecution. Questions of global jurisdiction, however, complicate prompt investigation and prosecution. If a U.S. company is cyber-attacked in its Japanese offices by the Russian mob through a server located in Brazil, where does the jurisdictional authority lie for prosecuting the attack?[39] To improve effectiveness of cyber efforts in a globally connected world, the United States should exercise diplomatic means to seek common ground among countries and intergovernmental organizations for fighting against cyber-attacks and cyber-exploitation and to influence international partners to collaborate on core areas of cybersecurity.

Effective policy-making to encourage international cooperation requires an understanding of how different cultures give rise to different attitudes and norms about fighting cyber-attacks. The United

States, for example, prefers to engage international law enforcement to investigate and catch cyber criminals.[40] International cooperation could resolve jurisdictional issues when perpetrators conduct cyber-attacks across state lines. INTERPOL conducts a similar function for fighting international crime by providing liaison between law enforcement authorities among its 188 member countries.[41] It provides a model for international cooperation that could apply to cyber-crime, as well.

In contrast, Russia argues that the U.S. approach would lead to interference in its internal affairs. Russia jealously protects non-interference, an "immutable principle of international law," as a pillar of her sovereignty.[42] Russia tends to be wary of American motives, which it claims have political and ideological goals aimed at undermining Russian independence and its sphere of influence in Eastern Europe. Russia's actions and policies also conveniently protect its own population of patriotic hackers, an educated and empowered volunteer militia within cyberspace. These were the foot-soldiers during the cyber-conflict that occurred during the Georgia-Russia conflict of 2008.[43] One day after Russia invaded Georgia, the StopGeorgia.ru forum began conducting a series of denial-of-service attacks against Georgian government websites that disabled several key websites during the invasion. The StopGeorgia.ru forum was run by sophisticated hackers who published lists of vetted targets that patriotic Russian hackers attacked. Although the Russian Government distanced itself from the hacker activity, it clearly enjoyed the benefits and tacitly supported the community. International law enforcement cooperation, as espoused by the United States, could target these non-state hackers.

China has a third view. Chinese authorities closely monitor Chinese networks and take aggressive steps to filter or block what the government considers "politically troublesome content," such as references to democracy, civil liberties, Chinese political dissidents, and other concepts contrary to Red ideology.[44] The alleged intent of China's internet crackdown is to protect civil order. Supporters of free speech decry these practices as censorship and a pretext for the government to tighten its control over daily life and solidify its power. The three approaches illustrate the divergent attitudes toward cyberspace and

underscore the complexity in attempting to influence international norms and behavior.

With an understanding of cultural differences about cyberspace, American diplomatic efforts should seek common ground among countries to cooperate in promoting cyber-security and combating cyber-attacks. The United States should advocate that cyberspace is a global commons whose usefulness is contingent upon its security. Diplomatic pressure is needed to influence countries to adopt collaborative practices in finding and blocking cyber-attacks. One such collective approach is the Council of Europe's Convention on Cybercrime. Thirty countries have ratified the convention, including the United States and 17 others are signatories. The convention requires that signatories enact stringent laws against cybercrime and take steps to investigate and prosecute violators. The convention also directs participating countries to cooperate with one another in such matters as reciprocal law, extradition, and mutual assistance.[45] A weakness of the convention is that while it mandates public action, it establishes few means to verify compliance. The convention is currently open for signatures, but differences in cultural attitudes discussed above present barriers to wider acceptance. The United States should use diplomatic pressure to encourage wider acceptance of the Convention's principles.

The concept of a sanctuary state should be developed to bring international pressure to bear on states who fail to discharge their duty to prevent cyber-attacks. The 9/11 attacks on the World Trade Center and the Pentagon introduced a new paradigm for fighting terrorism. The resulting doctrine prescribed that the United States would not only fight terrorists but also the regimes that harbor and shelter them. Similarly, a state that fails to prosecute cyber-criminals, or who gives safe haven to individuals or groups that conduct cyber-attacks against another country, may be defined as a sanctuary state.[46] Policy makers should seek to develop a common understanding of cyber-sanctuary states within the international community and intergovernmental organizations. Diplomatic pressure or other actions could then be taken to coerce the sanctuary state to exercise its duty to prevent cyber-attacks against entities in other countries.

## Deterrence of Cyber-Attacks

The NSS states that one strategic objective is to prevent cyber-attacks.[47] But strategic documents and cyberspace initiatives focus on detecting and intercepting cyber-attacks, with scant attention on developing methods to deter cyber-attacks. Common arguments against the effectiveness of cyber-deterrence include the difficulties in accurately attributing the source of cyber-attacks, the murky legal status of cyber-attacks as an act of war, and the lack of proportionate response options that carry sufficient weight to deter a cyber-attack. Given the serious potential consequences of a successful attack against critical infrastructure, the United States should develop a robust defense strategy tailored to deter likely potential adversaries, include mechanisms for managing escalation during a cyber-crisis, and give due consideration to complexities such as the presence of "patriotic hackers."

The central concept for deterring an adversary from taking action against the United States is to influence the adversary's decision-making calculus, with the result that he perceives inaction as preferable to action. The U.S. Joint Operating Concept describes three core concepts for deterrence:

1. Pose a credible threat to impose costs to the adversary if he takes the undesired action
2. Deny the benefits to the adversary of the undesired action
3. Encourage restraint by offering consequences for inaction[48]

In the context of cyberspace, determining specific techniques to impose cost or deny benefits is complicated by the wide array of potential adversaries, which range from hackers set on breaking into sensitive systems for the sheer technical challenge, terrorist use of cyber-attack as an asymmetric weapon, to nation-state use of cyber-espionage or cyber-attack to support kinetic operations. The individual hacker's motivations and perception of risk are radically different from those of a nation-state. Effective approaches to deterrence, therefore, must be tailored based on a sophisticated understanding of the adversary's "unique and distinct identities, values, perceptions, and decision-making processes."[49]

In developing tailored deterrence strategies, policy-makers must first identify who is being deterred. A common perception holds that the difficulty of attribution (identifying potential or actual cyber-attackers) arrests any meaningful attempt to develop cyber-deterrence. The relative ease of concealing one's identity within cyberspace does introduce uncertainty in attributing attacks in real-time. But deterrence planning should be done within a larger geo-political context. Following the differentiated approach principle, deterrence should focus on potential high-end cyber-attacks. Low-end cyber-attacks, such as hackers defacing websites, may be adequately deterred with on-going efforts to improve defenses. The high-end attacks most in need of deterrence, however, are likely to be conducted within the context of a political or ideological agenda. Terrorist groups, rogue states, and near-peer states such as China and Russia will continue to develop cyber-power in the future. They will likely use cyber-exploitation and cyber-attacks as part of an overall strategy directed toward achieving political objectives.[50] Knowledge of potential adversaries and their motives and methods does not require real-time attribution during a crisis. Tailored deterrence strategies should be developed in peacetime for actors with known grievances against the United States. What America must avoid is facing a cyber-attacker whose identity is known but for whom an effective and proportionate response has not already been conceived and critically reviewed. A cyber-attacker would hope to catch the United States unprepared. A strong, declared policy, tailored to each important adversary, would begin the process of developing viable deterrence.

Should a non-state actor wish to remain anonymous, the difficulty of accurate attribution of the attack is a limitation to deterrence actions during a crisis. A non-state actor could launch a cyber-attack from within a covering state without its knowledge, complicating efforts to identify the attacker. A criminal group might use a botnet, for example, to launch coordinated attacks from hundreds or thousands of computers located in multiple non-hostile countries.[51] A retaliatory response in cyberspace might damage networks in non-hostile countries or unrelated systems. If the perpetrator launched the attack from within a sanctuary state, the victim would likely have difficulty discriminating the degree of the state's involvement. One scenario is

an attack launched with full approval of the sanctuary state authorities and carried out with state assets. Another possibility is an attack that is tacitly encouraged by the state but carried out with non-state assets. Responses would vary according to the degree of state involvement. Intelligence and diplomatic resources should be brought to bear to complement technical attribution. In under-developed states with little cyberspace integrated into society, an appropriate cyber-response may not be available, reducing the range of options for policy makers to economic, diplomatic or military responses.

The threat of retaliation (imposing costs) is the cornerstone of classical deterrence theory. Before considering options for retaliation, policy-makers must determine the legal status of a cyber-attack. CYBERCOM's commander affirmed that the "international Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace."[52] A full legal analysis of how the Law of War applies to cyber-attack is outside the scope of this paper. But deterrence planning must include a decision-making structure at the national level to assess cyber-attacks, determine their legal status as acts of war, and formulate a range of possible responses within the bounds of proportionality.

Deterrence by imposing costs or denying intended benefits to the attacker should consider all elements of national power, as well as actions purely in cyberspace, to calibrate a deterrent posture. Technical efforts to improve cyber defenses, by denying access to networks or deploying dynamic defenses to stop intrusions, may alter the adversary's cost-benefit analysis sufficiently to dissuade some cyber-attacks, particularly less sophisticated adversaries with fewer cyber resources. When an adversary fails to penetrate a targeted system and cannot deliver the expected results, he must decide whether to accept additional risk by escalating the attack. Deterrence plans should deny benefits by developing ways to degrade the effectiveness of messages. As a "creative and cultural commons," cyberspace is increasingly becoming the "predominant domain of political victory or defeat."[53] An extremist cyber-attacker, for example, may judge his attack's effectiveness by how widely his ideological message spreads, captures publicity and lends some degree of credibility to his cause. Indirect effects could continue

on blogs and forums long after the direct effects of a compromised system have been eliminated. A deterrence strategy should consider non-technical ways to neutralize the message, such as information operations and counter-messages. For significant cyber-attacks, policy-makers should consider using other forms of national power, such as diplomatic and economic pressure. These may deter states who have the potential to employ cyber-weapons, or who might shield groups within their borders from launching cyber-attacks. These tools could also be used to offer incentives for adversaries to refrain from cyber-attacks.

As with classical deterrence, cyber-deterrence planning should specify methods to manage escalation during a crisis, including transparency and signaling of intentions. A nation could in principle respond to a cyber-attack with a kinetic counter-attack, as a way to inflict unacceptable costs on a hostile opponent. Classical deterrence seeks to calibrate a response proportionate to the damage inflicted by an attack. For cyber-deterrence, the difficulty in discriminating indirect effects from direct effects and in linking physical damages with a digital attack clouds the ability to determine a measured and proportionate response. A kinetic response might therefore be viewed as overly provocative and could result in undesired escalation of hostilities.[54] In conventional situations, adherence to international norms of behavior benefits stability, such as pre-announcing large troop movements, maritime "rules of the road,"[55] diplomatic engagement, and treaties and agreements that prescribe accepted behavior among nations. In contrast, legitimate cyber-activities are completely intermingled with illegitimate cyber-activities. A cyber-attack may be difficult to distinguish from a cyber-exploitation or hacker. Military use of cyberspace may be indistinguishable from civilian use. A culture of secrecy pervades American cyber policies and compromises the ability to signal national intentions. The United States should pursue policies to make its cyber intentions and capabilities more transparent, while protecting its technical know-how. To start, a strong policy of deterrence against cyber-attacks should be declared and promulgated in the NSS.

Managing escalation during a conflict would be facilitated by a workable framework for cyber early warning. Ned Moran, Professor at

Georgetown University, proposed a useful five-stage model for helping to anticipate cyber-attacks:[56]

> ***Stage 1: Recognition and assessment of latent tensions.*** Both state and non-state actors manifest background tensions long before actual attacks. These should be assessed within a global geo-political context and with regard to capability to conduct cyber as well as physical operations.
>
> ***Stage 2: Cyber reconnaissance.*** Prior to initiating hostilities in cyberspace, adversaries are likely to probe one another, to discover vulnerabilities and strengths, just as adversaries would do on a conventional battlefield.[57]
>
> ***Stage 3: The initiating event.*** In the 2007 Estonian cyber-war, the initiating event was the removal of the Soviet memorial in Tallinn. It caused tensions to boil over in the form of riots in Moscow as well as in cyberspace.[58]
>
> ***Stage 4: Cyber mobilization.*** Following the initiating event, adversaries organize groups in cyberspace, recruit sympathetic supporters, and vet targets.

For example, Chinese hackers mobilize support for political causes on message boards and chat rooms. In 2008, Chinese users created an anti-CNN forum to refute "the lies and distortion of facts from the Western Media."[59] Keen observation of internet forums and blogs combined with foreign intelligence gathering could identify when cyber soldiers are mobilizing and proactively raise the cyber alert status. Stage 5 is the cyber-attack itself. The effectiveness of the attack depends on the sophistication of the perpetrators and the degree of reconnaissance and preparation performed. The United States should carefully observe the cyber activity of actors with known grievances against America to look for signs of one of the five stages of the early warning model. Responses taken earlier in the process will more likely prevent escalation of the conflict to a more serious stage.

The presence of patriotic hackers will complicate efforts for deterrence and managing escalation during a conflict. As hostilities build, both sides of a conflict are likely to experience a surge of patriotic hackers, who act independently or in grass-roots groups to harass the opposing

side. These activities are outside of government control but may be difficult to distinguish from a state-sponsored cyber-attack.[60] The cyber-war during the Russian invasion of Georgia in 2008 is an instructive example. The StopGeorgia.ru project was originated by a grassroots network of Russian hackers inside and outside the Russian Federation. Russia denied official involvement and direct support of the project, but it clearly benefited from the cyber-attacks during the invasion and did nothing to stop them.[61] A more worrisome scenario could occur with a phenomenon known as "catalytic cyber-conflict." This refers to a conflict where a third party instigates conflict between two countries by launching a cyber-attack disguised to resemble one country attacking the other.[62] This occurred in July 2009 when a number of U.S. and South Korean government websites shut down over the Independence Day weekend. Suspicion immediately fell on North Korea, and one U.S. congressman even called for a military counter-attack. The likely perpetrator was not North Korea, however, but a hacker community in another country.[63] The incident underscores the fragility of stability in cyberspace and the need for the United States to focus on major cyber threats from adversaries with known grievances against the United States.

## The Way Ahead

Protecting access to cyberspace serves American vital interests. A comprehensive cyber-security strategy, developed now while the United States is in a preeminent position in this newly evolving domain, will best utilize resources to solidify American cyber-power.

Government and military policies are needed to improve cyber-security of critical networks and systems. Key conclusions and recommendations include:

- The United States should adopt a policy of differentiation among cyber-attacks to prioritize response planning towards attacks that target more critical national assets.
- CYBERCOM and NSA's defense-in-depth of military and government systems illustrate an effective template for static and active cyber defenses.

- Best practices for cyber-security learned from CYBERCOM should be applied more broadly to critical civilian sectors.
- Initiatives under the CNCI show significant progress on creating a holistic, interagency approach to protecting government systems.

As cyberspace grows exponentially, the world becomes more interconnected and prone to shared vulnerabilities within cyberspace. The United States needs to exert international influence to encourage cooperation and collaboration in order to improve cyber-security.

- Cultural differences about cyberspace present barriers to international cooperation, norms and responsible behavior within cyberspace.
- The United States government should use diplomatic means to encourage wider acceptance of the principles promulgated in the Convention on Cybercrime.
- The international community should develop the concept of the cyber sanctuary state and pressure states who fail to prevent cyber-attacks that emanate from within their borders.

Policy makers should develop plans not just for improving cyber defenses but preventing cyber-attacks by implementing plans that include tailored deterrence against known adversaries with cyber-capabilities and tools to manage escalation during a cyber-crisis.

- Deterrence planning need not wait for accurate attribution real-time during a crisis, but rather should be developed within a broader geo-political context with regard to adversaries with known grievances against the United States.
- Attribution of non-state actors who wish to remain anonymous will be difficult. The state from which the non-state actor launches his attack may be complicit with the perpetrator, tacitly allow the attack, or be completely unaware of the attack.
- The presence of patriotic hackers complicates deterrence planning and crisis escalation management.

More complete development of these approaches to a cyber-strategy require study of the resources (means) to support the conceptual concepts (ways) discussed in this paper and to assess the degree of risk arising from identified gaps.

The importance of cyberspace to national security is growing commensurately with increasing bandwidth, faster computing power, and greater reliance on digital networks to power critical parts of modern society. The United States' cyber-strategy must evolve, too, to keep pace with innovative competitors in order to maintain freedom of cyberspace.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# History and Evolution of MalWare

**Colonel Jayson M. Spade**
United States Army

CYBERSPACE WAS CREATED IN 1969 with the launch of the Defense Advanced Research Projects Agency (DARPA) Internet Program. Nicknamed "ARPAnet" it was the first network of geographically separated computers.[1] Only two years later the first computer virus was created.[2] The first spam email was sent in 1978.[3] And by 1988 the first worm was loose in cyberspace.[4] It is an almost Biblical story: mankind created a domain with incredible potential for the sharing of knowledge; in short order, a few 'bad apples' introduced malware into this information Eden – software that will curse Internet users forever.

Cyberspace has expanded from the few systems on ARPAnet to a global network of smaller networks used by governments, institutions, businesses and individuals. Some two billion people use the Internet for business, research, communication, education and entertainment.[5] Globalization itself depends on the ability of people to interact in and through cyberspace, using online networks to exchange information, goods, and services around the world.[6] However, as cyberspace use has increased, so has the misuse of cyberspace. Criminals engage in cyber crime, exploiting the Internet and its users for illegal financial profit. Cyber punks and hackers engage in malicious activity, releasing viruses into the Internet just to see the effects, or cracking security systems for fame within the hacker community.[7] And nation-states conduct cyber attacks and exploitation: espionage, network reconnaissance, and acts of aggression against adversaries.[8,9]

Malicious software, or 'malware,' is the primary enabler for the misuse of cyberspace. Malware is software "inserted into an information system to harm that system or to subvert the system for uses other than those intended by the owners."[10] As information technology has improved and cyberspace has expanded, malware designers have kept pace, creating new programs to exploit software, hardware, and

network vulnerabilities. Malware, including worms, viruses, Trojans, rootkits and others, can disable security software, allow remote access to a system, damage at-rest information, and perform other functions – all without the owner's permission or knowledge.[11] An examination of the history of malware will demonstrate that malware developers will continue to adapt their programs to match and exploit new computer software and to take advantage of the uses to which people, businesses, and government put information technology.

Before the advent of the personal computer, computer programmers created viruses primarily for fun;[12] pranks that they played on one another. The viruses were largely experimental, designed to see what sort of programs could be written and how they could be disseminated. Early worms were designed to be helpful,[13] performing maintenance on networked computer systems.[14] The first recorded prank virus, the *Creeper*, was annoying, but caused no system damage and served as a proof-of-concept for a self-replicating, network travelling program. It also gave rise to the anti-virus program: the *Reaper* anti-virus was written to search for and delete the *Creeper*.[15]

Viruses broke out of the laboratory as computer use grew in the 1970-80s. At first, the viruses were like *Creeper*, non-malicious explorations of programming possibilities, jokes, and efforts to earn fame within the small computer-savvy community. In 1982, a high school sophomore wrote *Elk Cloner*, the first virus to propagate by disk. It loaded anytime a disk was booted into an infected Apple II computer, and then downloaded itself into other Apples whenever the infected disk was booted. Using prevailing technology, *Elk Cloner* was passed disk-to-drive, drive-to-disk, and infected thousands of computers.[16]

Like *Creeper*, *Elk Cloner* was basically harmless, but proof of a dangerous concept: that an Apple II computer's boot sector could be infected with unauthorized software. Apple II was targeted in 1985 with the first recorded Trojan Horse, the *Gotcha* virus.[17] Purely malicious, *Gotcha* masqueraded as a graphics utility program, but, when launched, wiped out all files on the computer's hard disk.[18] Other malware programs appeared quickly at the rate of several a year, and spread both through diskettes and nascent local area networks at universities and businesses. As more common-use programs were written, malware writers tailored

their programs to target specific software vulnerabilities. Programs varied from pranks, like *Cascade*, which caused displayed letters to fall from the top of the monitor to the bottom, to destructive, like the *Byte Bandit*, which caused serious data loss in the Commodore Amiga line of personal computers.[19]

The 1990s saw an even greater proliferation of much more sophisticated computer viruses, due to wider use of home computers, expanded use of the Internet, and the growing popularity Microsoft's Windows operating system and office programs. When IBM, McAfee, and Norton created anti-virus programs, malware writers adapted again.[20] They introduced 'polymorphic' viruses, encrypted to adapt and change byte patterns, thereby avoiding virus scans which searched for malware by their unique signatures. *Chameleon* was first in 1990 and quickly followed by *Tequila* and *Maltese Amoeba* viruses, which caused widespread polymorphic infections in 1991.[21]

The next year, the author of the *Maltese Amoeba*, under the alias 'Dark Avenger,' used the Bulgaria-based Internet Virus Exchange Bulletin Board (VxBBS), to distribute his Mutation Engine (MtE) to other virus writers, helping them to build their own polymorphic viruses.[22] Other designers followed, exchanging source codes, uploading their own mutation engines, and posting menu-driven toolkits to allow less skilled programmers to develop new viruses. A significant development, on-line bulletin boards allowed virus writers to collaborate, widening both the creation and circulation of malware.[23]

Microsoft's Windows, growing rapidly in popularity among personal computer users, was targeted in 1995 by the world's first macro virus, *Concept*.[24] Specifically designed to infect *Word for Windows 95*, each time the user opened an *MSWord* document, the virus was activated. While *Concept* was fairly benign, it started a trend.[25] Malware authors went on to develop over a hundred macros and dozens of other viruses for *Windows 95* and other Windows office programs. As Windows became the world's most widely-used operating system, malware writers developed macros which could cross operating platforms to infect both IBM compatible and Macintosh personal computers.[26]

Malware development and propagation since 1999 has kept pace with the Internet boom. The *Melissa* macro virus was posted as an *MSWord* document on a Usenet newsgroup. Promising names and passwords for erotic websites, it contained a macro virus that used the infected computer's *MSOutlook* to spam out 50 email copies of itself. Within three days it spread to 100,000 hosts, shutting down email services for companies using Microsoft Exchange Server.[27] Prior to *Melissa*, experts believed that just opening an email could not activate a virus. Only a year later, the *BubbleBoy* virus demonstrated that simply previewing an email could download a virus.[28] These two, and many viruses that followed (e.g., *Naked*, *LoveLetter*, and *Koobface*[29]) started a new trend in exploitation called 'social engineering.'[30] Playing on user curiosity and ignorance of IT security, social engineers use messages written to trick or entice the receiver to download a virus.[31]

The 2000s have seen increasing instances of malware being used to install attacker tools, such as rootkits, keystroke loggers, and backdoors.[32] There are blended attacks, like *Nimda*[33] and *StormWorm,*[34] which combine the use of viruses, worms, backdoors, and mobile code,[35] using multiple methods to bypass security programs.[36] *StormWorm*, identified in 2007, represents another new development, the use of malware to take control of computers and link them into botnets – remotely controlled networks of computers, frequently used for illegal activity.[37] Matching computer use, malware expanded its distribution means to include social networking websites like Facebook and MySpace.[38]

At every step of information technology development – boot drive to hard drive, intranet to internet, email to instant message, programs to applications – malware authors have developed a new way to infiltrate and exploit other people's IT systems for their own use. Malware, originally a joke between programmers, is now a tool for criminal activities and organized crime. It is used to collect passwords, credit card numbers, and other personal information which is used to steal identities or loot bank and credit card accounts.[39] Botnets can be used to attack networked systems as a means to extortion; repeated denial of service attacks until the website or server operators pay blackmail.[40] And malware adds to the cost of using cyberspace, in terms of buying security software, loss of productivity when malware brings a system

down, and cleaning and repairing infected networks. In 2006-07, Americans paid roughly $7.8 billion to repair damage caused by malware.[41]

At the national level, malware poses a danger to both critical infrastructure and national security. Most industrial supervisory control and data acquisition (SCADA) systems, which manage electrical power, water, and emergency services systems, where not designed for network security, yet are connected to the Internet.[42] This makes possible the disruption of critical services due to malware interference. For example, in 2003 SQL Slammer worm penetrated the safety monitoring system at a U.S. nuclear power plant.[43] Estonia and Georgia were both subjected to sustained dedicated denial of service attacks, conducted in part through botnets, which shut down their national banking systems and cut off their access to cyberspace.[44] In 2008, a variant of the Agent.btz worm accessed the U.S. Department of Defense's unclassified network, eventually infecting classified networks. It took Operation Buckshot Yankee nearly 14 months to finally remove the worm from all affected systems.[45] And the 2011 *Stuxnet* worm,[46] used to attack Iran's nuclear program, brought virus capabilities to a new level of complexity and specificity. Using stolen encrypted signatures, it traversed industrial control systems, through networks and non-networked systems, lethal only to one specific system made by one manufacturer.[47]

Since the creation of cyberspace, computer viruses and network worms have continuously evolved through a series of innovations, leading to current generation of fast-spreading and dangerous malware. Oftentimes critical vulnerabilities were caused by industry's rush to market new programs and applications, leaving unidentified security gaps in the software.[48] But industry is not solely to blame for the spread of malware. People design malware and most viruses and worms require some level of user interaction to activate. Through a combination of malicious intent, user complacency or ignorance of computer security requirements, and social engineering, malware continues to spread.[49]

At best, it is difficult to identify malware perpetrators; to trace a virus or worm to its creator. Even if the creator is identified and arrested, the cases are difficult to prosecute and sentences have tended to be light. Robert Morris, creator of ARPAnet's first worm, received three years

probation, community service, and a $10,000 fine. Police arrested Chen Ing-hau, author of the 1998 *Chernobyl* virus,[50] but none of the companies affected pressed charges. The 2000 *LoveLetter* virus caused billions in damages,[51] but author Onel de Guzman was not charged because the Philippines had no applicable computer laws. Jan De Wit was sentenced to community service for the 2001 *AnnaKournikova* virus.[52] The *Melissa* virus caused millions in damages, but creator David L. Smith was sentenced to community service and a $7,500 fine.[53] In 2010, McAfee detected an average of 60,000 new malware activities each day.[54] And none of this takes into account malware developments by and for the use of national governments in cyber espionage or cyber warfare. Without effective national and international laws, and global cooperation between law enforcement agencies, malware writers will continue to avoid punishment proportional to their actions and there will be no deterrent to the use of malware.[55]

Computers and the Internet are now essential to government, commerce, and even social life, perhaps to the point where the occasional malware plague is accepted as a fact of life. And malware is too lucrative for crime and too valuable as a weapon for any cyber criminal or cyber state to forgo. Like an arms race, where there introduction of a new weapon causes one's adversary to generate newer weapons in response,[56] the information technology industry and IT users are locked in a never-ending developmental cycle with malware designers. New software will beget new malware, which begets a new anti-virus or patch, which begets a new version of the malware, and so on. Once again, the situation is almost Biblical: "…I will put enmity between Snake and Woman, and between your seed and hers; He shall bruise your head and you shall bruise His heel."[57] Snakes and people, worms and users – a software curse that cyberspace will endure forever.

# Section Two

## Strengthening Defense Support of Civil Authorities


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Introduction

**Professor Bert B. Tussing**

Homeland Defense and Security Issues Group
Center for Strategic Leadership
U.S. Army War College

DEFENSE SUPPORT OF CIVIL AUTHORITIES, when it is required, is the most compelling mission of the American military in the eyes of the American people. It is then that the tremendous capabilities and capacities of the armed forces are harnessed, and brought home to the public in their hour of need. Unaware and uncaring as to whether those forces are Active Component, from the Service Reserves, or from the National Guard, in the moment of crisis the public expects its military to respond.

Moreover, the military wants to "be there" for the American citizenry in their hour of need. But the planning, resourcing, and a host of other requirements that must be met before the military arrives, are areas of frequent consternation for the Pentagon. Viewed against their "day job" of fighting and winning the nation's wars, preparations for *potential* domestic requirements often find themselves in the shadows of the active components' day-to-day focus.

This is not a deliberate abrogation of responsibility; but it should lead us to questions surrounding preparations for events whose likelihood is small, but whose consequences may be tremendous. In the Department of Defense, an enormous expenditure of manpower is properly devoted to developing contingency plans for combat operations we hope will never come. One has to wonder, then, how the military can be any less focused on developing plans for catastrophes we hope will never strike.

Of course, a significant effort is being expended by all components of the military in preparing for these ends; but in truth, the focus is relatively new when viewed against the history of the forces. Since 9/11, a number of students of the U.S. Army War College, in both the Resident and the Distance Education programs, have devoted extensive research regarding the military's role in supporting civil response to

disaster – be it natural or man-made, accidental or deliberately visited against our people. In this section the contributions cover a wide swath of issues faced in supporting civil authorities, including:

- Command and Control of Active, Reserve and National Guard forces in response and recovery operations
- Aligning military response with civil regional requirements in responding to disasters that transcend states' borders
- Attending to the delicate line of demarcation between the military and law enforcement when responding to the requests, or directives, of civil authorities
- Challenging the impetus that leads to unnecessarily applying federal assets, to include the military, in a "nationalization of disasters"
- Suggesting another strategic mindset to preparations for response to domestic crises, applying a center of gravity model to risk assessment requirements

For all its capabilities, capacities and competencies, the single greatest gift the military may bring to domestic security and emergency management is its inherent ability to plan. But plans must be empowered by contemplation, removed from the demands of urgent reaction, to contribute to solutions before they are required. The War College is a place for that kind of contemplation, and the editors of this volume are grateful for the contribution of the authors in this section.

# Reforming Disaster and Emergency Response

**Colonel Mark D. Johnson**
United States Army

> The Federal Emergency Management Agency's (FEMA) mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.
>
> —FEMA Fact Sheet

OVER THE PAST TWO DECADES, the Federal Emergency Management Agency (FEMA) has increasingly responded to routine natural disasters that had historically been managed by state and local governments. The increased federalization of disasters stands contrary to the basic premise that all disasters are local, and it does not matter how large an event is, but all response and recovery efforts begin and end with the local community. The trend also fails to reinforce the responsibility of states and local communities to prepare for, develop, and resource response plans for disasters within their jurisdictions. Furthermore, the impact of FEMA's involvement in routine disaster response and recovery at the levels it has sustained over the past two decades takes away from the time and focus it could devote towards preparation for truly catastrophic disasters. As states have increasingly grown to depend on federal resources, it can be argued that they may likewise fail to invest in their own capabilities for response, as the incentives to do so are reduced. Additionally, when federal disaster policy enables states to capitalize on a federal/state cost-share for response and recovery, where the federal government assumes a 75% economic burden, this serves as an incentive for states to rely on federal disaster declarations.[1] Another result of the nationalization or federalization of disasters is that a majority of the states end up funding a minority of the remaining states disaster costs, as those minority states receive federal disaster dollars in a disproportionate amount.[2] In order for the United States as a nation be able to better adhere to the vision of the National Preparedness Guidelines of being a "Nation prepared

with coordinated capabilities to prevent, protect against, respond to, and recover from all hazards in a way that balances risk with resources and need," Congress must relook current disaster relief and emergency assistance laws and policy, and refocus FEMA towards being an agency geared toward catastrophic disasters and emergencies.[3]

## Historical Context

President Jimmy Carter established FEMA by Executive Order 12127 in 1979. The creation of FEMA involved the absorption of several other agencies that had disaster-related responsibilities, to include civil defense responsibilities which were also transferred to FEMA from the Department of Defense Civil Preparedness Agency. Over the period of its existence, FEMA's focus and role, and our nation's disaster and emergency response policies have evolved and changed.[4]

Throughout the first 14 years of FEMA's existence, it managed a variety of disasters and emergencies, with national-level attention gained during the agency's actions through its response to events ranging from the contamination of the Love Canal, the Cuban refugee crisis, the accident at the Three Mile Island nuclear power plant, the Loma Prieta Earthquake, and Hurricane Andrew. In 1993, during the Clinton Administration, FEMA initiated reforms that both streamlined disaster and relief operations, as well as placed a new emphasis on preparedness and mitigation. With the conclusion of the Cold War, FEMA redirected its resources that had been directed at civil defense toward disaster relief, recovery, and mitigation.[5]

During the George W. Bush Administration, after the terrorist attacks of September 11, 2001 (9/11), FEMA focused on issues of national preparedness and homeland security, and was absorbed into what has become the Department of Homeland Security. As part of its focus on preparedness, and as a result of 9/11, FEMA was given an added responsibility for helping to ensure that first responders across the nation were trained and equipped to deal with weapons of mass destruction (WMD). Included in its efforts of helping communities face the threats of terrorism, FEMA incorporated its "all-hazard" approach to disasters towards homeland security issues. Subsequent to Hurricane Katrina, the Post-Katrina Emergency Management Reform Act was signed into

law, and FEMA was reorganized and given new authorities to remedy gaps and deficiencies that were revealed in the wake of that disaster. As a result of the Post-Katrina Emergency Reform Act, FEMA assumed a more robust preparedness mission.[6] Today, FEMA stands as an agency focused on four mission areas: prevention, protection, response and recovery. The scope and focus on each of these mission areas has evolved through time, and the level of effort and attention directed in each area has grown – perhaps not necessarily in relationship to an increase in catastrophic events.

## The Disaster Declaration Process

Local and state governments share the responsibility for protecting their citizens from disasters, and for helping them to recover when a disaster strikes. In cases where a disaster is beyond the capabilities of the state and local governments to respond, the Governor of the affected state may request federal assistance through a process established in the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). The Stafford Act was enacted in 1988 to support state and local governments and their citizens when disasters overwhelm them. The law, as amended, establishes a process for requesting and obtaining a Presidential disaster declaration, defines the type and scope of assistance available from the federal government, and sets the conditions for obtaining the assistance. The Stafford Act authorizes the President to issue major disaster or emergency declarations in response to catastrophes in the United States that overwhelm state and local governments. The Stafford Act reinforces the principles of federalism through the concept that with very limited exceptions, federal support is provided only at the request of a state. Furthermore, once provided, federal support is directed in support of and in coordination with the state through a mechanism and process established in the National Response Framework. Such declarations result in the distribution of a wide range of federal aid to individuals and families, certain nonprofit organizations, and public agencies. Congress appropriates money to the Disaster Relief Fund (DRF) for disaster assistance authorized by the Stafford Act, and FEMA administers most, but not all, of the authority of the statue.[7] There are five types of actions that may be taken under authority of the Stafford Act: Major disaster declarations,

emergency declarations, fire management declarations, the provision of defense resources before a major disaster is declared, and the decision to pre-position supplies and resources.[8]

**Federal Declarations**

Three of the five types of declarations may be made prior to a disaster or catastrophe. First, the president (at the request of a governor), may direct the Department of Defense (DoD) to commit resources for emergency work essential to preserve life and property in the "immediate aftermath of an incident" that may result in the declaration of a major disaster or emergency. Such emergency work carried out under this provision may only be carried out for a period not to exceed 10 days. The federal share of assistance shall be no less than 75%, with the state responsible for the balance of the cost. Reimbursement shall be made to the DoD from the DRF.[9]

Second, fire management assistance, including grants, equipment, supplies, and personnel may be provided to any state or local government "for the mitigation, management, and control of any fire on public or private forest land or grassland that threatens such destruction as would constitute a major disaster."[10] Under this provision, governors must submit a request for assistance while an uncontrolled fire is burning. To be approved, either of two cost thresholds established by FEMA through regulations must have been reached. The thresholds involve calculations of the cost of the individual fire, or those associated with all the fires (both declared and non-declared) in the state during the calendar year.[11] Under the cumulative fire cost threshold, assistance will only be provided for the declared fire responsible for meeting or exceeding the cumulative fire cost threshold and any future declared fires for that calendar year. The individual fire cost threshold for a state is the greater of $100,000 or five percent of $1.14 times the state population. The cumulative fire cost threshold for a state is the greater of $500,000 or three times the five percent times the state population.[12] In 2007 there were 136 federal disaster declarations (major disaster declarations, emergency declarations, or fire management assistance declarations), of which 60 (44% of the federally declared declarations for the year) were fire management declarations. The 63 fire management declarations

were spread among 16 states, with California having the greatest number of declarations (17 total).[13] During this same year, 12 states had individual fire cost thresholds of $100,000, and California had the highest individual cost threshold at $2,066,171. Similarly, 19 states had a cumulative fire cost threshold of $500,000, and California had the highest cumulative fire cost threshold at $6,198,512.[14] A declaration made under the Fire Management Assistance Grant Program provides a 75% federal cost share, and the state pays the remaining 25% for actual costs. Eligible firefighting costs may include expenses for field camps; equipment use, repair and replacement; tools, materials and supplies; and mobilization and demobilization activities.[15]

The third type of declaration that may be made prior to a catastrophe occurs is when a situation threatens human health and safety, and a disaster is imminent but not yet declared. In this instance, FEMA pre-positions employees and supplies, and coordinates with other federal agencies to do the same. In anticipation of an imminent disaster, FEMA will "monitor the status of the situation, will communicate with state emergency officials on potential assistance requirements, deploy teams and resources to maximize the speed and effectiveness of the anticipated federal response and, when necessary, performs preparedness and preliminary damage assessment activities."[16]

This type of declaration and pre-disaster activity is most commonly used in hurricane response, and to a lesser extent for larger-scale flooding response – both of which provide some notice of occurrence, and thus some limited time to position response resources in advance of a disaster. In recent years, most notably since Hurricane Katrina in 2005, FEMA has leveraged this type of declaration in order to facilitate federal responsiveness.

The Stafford Act authorizes the President to issue the remaining two types of declarations – major disaster and emergency – after an incident overwhelms state and local resources.[17] These two declarations are the two principle forms of presidential action to authorize federal supplemental assistance.

A major disaster declaration is made as a result of the disaster or catastrophic event and constitutes a broader authority that helps states

and local communities, as well as families and individuals, recover from the damage caused by the event.[18] Major disaster declarations and emergency declarations may be issued after the President receives a request from a governor of an affected state for a major disaster declaration.[19] Major disaster declarations may be issued after a natural catastrophe "(including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought) or, regardless of cause, after a fire, flood or explosion."[20] In 2007, 63 of the 136 disasters (46%) were major disaster declarations, and spanned a wide range of subtypes to include severe winter storms, severe storms and flooding, landslides and mudslides, tornadoes, inland and coastal flooding, and severe freeze.[21]

Factors that FEMA considers in evaluation of a governor's request for a major disaster declaration and subsequent public assistance include an assessment of the per capita impact of the disaster within affected states; insurance coverage in force; the presence and impact of hazard mitigation measures; the cumulative impact of disasters over the previous year; and whether federal aid authorized by statutes other than the Stafford Act would better meet the needs of stricken areas. Each year, FEMA determines the threshold to be used as one of the factors to be considered in determining whether public assistance or individual assistance or both will be made available after a major disaster declaration has been issued. Regulations establish a minimum threshold of $1 million in public assistance damages for each state. Major disaster declarations issued on or after October 1, 2005, would be expected to reach a threshold of $1.29 per capital for public assistance. The statewide threshold, however, is not the sole factor. Assessments consider concentrations of damages in local jurisdictions even if statewide damages are not severe. Countywide impacts from major disasters declared on or after October 1, 2005, would generally be expected to reach the threshold of $2.94 per capita for public assistance.[22] The impact of these thresholds is that a state with a smaller population will more rapidly reach the threshold than a state with a larger population because similar levels of physical damage will have higher per capita damage in a smaller populated state. For example, flooding along the Red River Valley that serves as the border between

North Dakota and Minnesota may cause similar levels of physical damage in each state, but because the population of North Dakota is significantly smaller than that of Minnesota, the per capita damage will be greater in North Dakota than in Minnesota, and thus North Dakota may qualify for public assistance, while Minnesota may not.

Emergency declarations are made to "supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a major disaster or catastrophe."[23] Emergency declarations are similar to major disaster declarations, but the criteria are less specific. Furthermore, emergency declarations may be issued if primary responsibility rests with the federal government.[24] Also, "specific thresholds or calculations of past averages are not considered, but FEMA officials do assess whether all other resources and authorities available to meet the crisis are adequate before recommending that the President issue an emergency declaration."[25] Emergency declarations are frequently made when a threat is recognized and are intended to supplement and coordinate local and state efforts such as evacuations and protection of public assets (such as was the case when emergency declarations were made for Hurricane Katrina prior to the hurricane making landfall). In 2007, 13 of the 136 disasters (slightly less than 10%) declared that year were emergency declarations. Broken down by subtype, the emergency declarations for 2007 included five issued for snow, four for severe winter weather, one for wildfires, one for drought, one for a bridge collapse, and one for a hurricane.[26]

**Disaster Relief Fund**

Once a federal disaster declaration has been issued, FEMA provides disaster relief through the use of the DRF. Congress appropriates money to the DRF to ensure that funding for disaster relief is available to help individuals and communities stricken by emergencies and major disasters. Funds appropriated to the DRF remain available until expended, and the DRF is generally funded at a level that is sufficient for what are known as "normal" disasters (incidents for which DRF outlays are less than $500 million). When a large disaster occurs, funding for the DRF may be augmented through emergency

supplemental appropriations.[27] Supplemental appropriations measures are generally required each fiscal year to meet the urgent needs of particularly catastrophic disasters.[28]

As the categories of aid and federal disaster assistance have expanded, there has been a corresponding increase in the cost of federal disaster assistance authorized by the Stafford Act. For example, over the past five decades assistance has been expanded in the areas of housing, grants for the repair of infrastructure, aid to individuals, loans to communities for lost revenue, and other needs.[29]

Disasters that occurred between Fiscal Year 2001 and Fiscal Year 2005 were especially costly. In Fiscal Year 2001 and Fiscal Year 2002 supplemental appropriations for disaster assistance exceeded $26 billion, most of which went toward recovery following the terrorist attacks of September 11, 2001. After the 2005 hurricane season, supplemental appropriations for disaster assistance increased significantly. From Fiscal Year 2005 through Fiscal Year 2009, Congress appropriated over $130 billion for disaster relief administered by many federal agencies. The majority of this funding was directed toward damages sustained from the 2005 hurricane season.[30]

The magnitude of these figures are somewhat skewed as they include federal funds expended for both the 9/11 terrorist attacks, and Hurricane Katrina – the two most costly disasters in American history. A more accurate snapshot of average disaster expenditures may be those that reflect the obligations during the period 1999-2010, and do not include either the 9/11 terrorist attacks or Hurricane Katrina. During this period, the average obligation per year for major disaster declarations and emergency declarations was $3.5 billion; and the average obligation per disaster was $81 million.[31]

The need for federal assistance after a disaster, particularly one of catastrophic magnitude, may foster government officials to pledge to do whatever it takes to restore an area to its pre-disaster condition, however, doing so requires a significant expenditure of federal funding that may arguably be used elsewhere for other urgent purposes. As the leaders at the national level wrestle with the competing demands of providing federal disaster assistance and controlling expenditures,

increasingly the question must be asked what the responsibilities are for the federal government, and what the responsibilities are for state and local government – and what are individual responsibilities.

**Incentives to Federalize Disasters**

Stipulations of the Stafford Act create significant fiscal incentives for states to request federal disaster declarations. Under the Stafford Act, the federal government pays 100 percent of the costs general federal assistance to "save lives, prevent human suffering, or mitigate severe damage."[32] Essential assistance to "meeting immediate threats to life and property resulting from a disaster" is reimbursed at not less than 75%.[33] The federal government also pays not less than 75% for hazard mitigation that reduces "the risk of future damage, hardship, loss, or suffering."[34]

Likewise, the federal government will pay not less than 75% for "repair, restoration, and replacement of damaged facilities – whether publicly owned, or a privately owned nonprofit facility that provides critical services."[35] Not less than 75% of the costs associated with debris removal may also be funded by the federal government.[36] Additionally, the federal government will pay 100% of individual assistance (up to $25,000 per household).[37]

Without a federal declaration, states and localities bear the full costs of the disasters, so the prospect of the federal government sharing the cost with the state is a tremendous incentive to states. Meeting the definitions for a federal declaration is fairly easy, and the financial thresholds are likewise relatively low. The disaster must be "of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments that federal assistance is necessary."[38] The financial threshold for storm-related damages of "$1.29 per capita, which for several states equates to less than $1 million in damages," is relatively easy to be reached.[39] While the guiding principle of disaster and emergency response is that all disasters are local, the economic incentive of federal assistance has increasingly driven states to seek federalization of disasters.

**Increasing Trend to Federalize Disasters**

Since the Stafford Act was signed into law, there have been nearly 3,000 federal declarations (major disaster declarations, emergency declarations, and fire management assistance declarations) – "most of which have not fundamentally met the act's definition of a disaster requiring federal intervention."[40] This trend of increased federalization of disasters began with the Clinton Administration, and has remained at high levels ever since. FEMA's response and recovery actions – thus "federalization" of disasters – during the first three Presidential administrations (Carter, Reagan, and George H. W. Bush) of FEMA's existence were relatively modest in comparison to the subsequent three administrations.

During the Carter administration the yearly average for declarations was 44 (with yearly highs of 56 in 1977 – two years prior to establishment of FEMA, and 55 in 1979 – FEMA's first year in existence). The Reagan administration averaged 28 declarations per year, with the highest number of declaration being 42 in 1984. The George H. W. Bush administration averaged 44 declarations per year, with a high of 53 in 1992. The yearly disaster declarations doubled the average of the previous administrations while President Clinton was in office, with a yearly average of 89 declarations, and had the highest number of declarations in a single year of any administration, with 157 declarations in 1996. The trend increased even further under the George W. Bush administration, which averaged 130 declarations per year, and had the second highest number of declarations of any administration in a single year, with 155 in 2005. There is a slight downward trend during the first two years of that President Obama has been in office, with an average of 112 declarations per year thus far, and a high of 115 declarations during his first year in office.[41] The tripling of the average annual number of federal declarations over the past three decades demonstrates the increased role and burden that the federal government has assumed in natural disasters, and begs the question of whether emergency management has shifted from a local and state responsibility, to a national responsibility.

**Majority of States Subsidize the Minority of States**

Two problems with the trend towards nationalization of disaster response are that a majority of states essentially subsidize the minority, and reliance on federal assistance may ultimately result in states being less prepared for disasters.

A 2009 report prepared by Matt A. Mayer of the Heritage Foundation comparing the number of federal declarations to state population demonstrates that the redistribution of the costs of disasters results in a majority of the states (29) subsidizing a minority of the states (21) for the costs of disasters (encompassing mitigation, response, and recovery). The analysis is based on the premise that states fund FEMA through taxpayer dollars, and in turn that money is spent on disasters. Calculating the difference between the amounts of money sent to FEMA, and how much money a state receives from FEMA in terms of disaster response funding shows that some states receive a disproportionate amount of disaster assistance. The results of Mayer's analysis reveal that 21 states end up as "winners" (have a higher percentage of disaster declarations as a percentage of total U.S. population); whereas 16 states end up as "losers" (have a lower percentage of disaster declarations as a percentage of U.S. total population), and 13 states "break even" (receive approximately the same proportion of disaster declarations as a percentage of U.S. total population).[42]

Surprisingly, in this analysis, several of the states that have the highest percentage of disasters, or maybe states that historically have catastrophic natural disasters, end up as "losers" or "break-even." For instance, Florida, Georgia, North Carolina, and Virginia are "losers," and South Carolina, Alabama, and Mississippi are "even" – despite perhaps a common perception that as hurricane-prone states they may benefit disproportionately from federal disaster relief. California, despite the catastrophic earthquakes and high-profile wildfires and mudslides it has suffered, is a "loser." Likewise, nearly all the upper Midwest states – with somewhat frequent severe winter storm or spring flooding – are also either "losers" or "even." States that are "winners" under this analysis include Texas and Louisiana (frequently struck by hurricanes), and North Dakota and South Dakota (both of which regularly experience spring flooding). Mayer illustrates the point of "winners"

compared to "losers" by comparing the federal disaster declarations for Oklahoma in relation to Michigan. Since 1993, there have been 90 federal disaster declarations in Oklahoma, which equates to five percent of all declarations, yet Oklahoma's population represents only one percent of the total U.S. population. During this same timeframe, there have been 14 disaster declarations in Michigan, equating to one percent of all declarations, yet Michigan's population represents three percent of the U.S. total population.[43]

A conclusion that may be drawn from Mayer's analysis is that the vast majority of states would be better off if they kept their disaster response taxes and funded their own disaster and emergency management operations. A counterpoint to this argument and one that may support current disaster policies is that there are more "winners" than "losers" (assuming that "break even" states don't care). Regardless of whether a state wins, loses, or breaks-even, however, federalization of a disaster takes some level of control of the disaster response away from the states and localities – the government entities that are ultimately accountable to their citizenry.

Incentivizing states to seek federal disaster declarations also undermines the preparedness of state and local emergency management agencies. As states and municipalities are threatened with fiscal challenges, to include some that may require a balanced budget, they may find it easy to cut back on their emergency management budget, and most certainly may not have the funds to set aside for a "rainy-day" fund that might cover required contingencies from a disaster response.

**Focus FEMA on Catastrophic Disasters**

As the federal government, and thus FEMA, has increasingly become involved in more and more disasters – many of which can be argued are truly not "catastrophic" – the federal government and FEMA does not spend enough time preparing for catastrophic natural disasters. By focusing much of its efforts on those disasters that are less than catastrophic, the likelihood that the Federal response for the next catastrophe will be insufficient, as it was during Hurricane Katrina is increased.

In December 2003, Homeland Security Presidential Directive (HSPD)-8 was issued, and established "national policy to strengthen the preparedness of the United States to prevent, protect against, respond to, and recover from terrorist attacks, major disasters, and other emergencies. HSPD-8 required the development of the National Preparedness Guidelines (Guidelines). These Guidelines define what it means for the Nation to be prepared by providing a vision for preparedness, establishing national priorities, and identifying target capabilities."[44] The Guidelines are based upon a capabilities-based planning process, and incorporate three planning tools: National Planning Scenarios, Target Capabilities List (TCL), and Universal Task List. The National Planning Scenarios establish national guidance for preparing the Nation for major all-hazards events, while the TCLs serve as a basis for assessing preparedness. Specifically, the TCL describes the capabilities related to the four core homeland security mission areas: prevent, protect, respond, and recover.

The TCL contains 37 core capabilities that provide national standards for building a national disaster preparedness and response system to deal with man-made and natural catastrophes.[45] Because the capabilities were derived from both terrorist and natural disaster scenarios, the TCL is an all-hazards tool featuring many dual-use elements. Furthermore, the TCL serves as a guide to addressing the priorities and achieving the Guidelines.[46]

The 15 all-hazards National Planning Scenarios, "serve as the foundation for the development of homeland security tasks, target capabilities… and standards against which capabilities and tasks will ultimately be measured."[47] Twelve of the fifteen scenarios represent terrorist attacks, and three represent natural disasters or naturally-occurring epidemics. The fifteen scenarios "form the basis for coordinated federal planning, training, exercises, and grant investments needed to prepare for all hazards."[48]

The Guidelines identify eight priorities to meet the Nation's most urgent needs, and adopts a capabilities-based planning process to define and build the capabilities to achieve the Guidelines. Two of the eight priorities are specifically related to disaster and emergency response, and should be used to focus the efforts and role of the federal

government, and define the role and responsibilities of state and local entities. The Guidelines identify implementation of the National Incident Management System and the National Response Plan, as well as strengthening planning and citizen preparedness capabilities.[49]

The vision of the Guidelines is a "nation prepared with coordinated capabilities to prevent, protect against, respond to, and recover from all hazards in a way that balances risk with resources and need."[50] The basic premise of disasters and emergencies is that all disasters and emergencies are local – and thus the responsibility for prevention, protection, response, and recovery is local as well.

The increased federalism of disasters, and the rising role and assumed responsibility of the federal government in prevention, protection, response, and recovery endeavors works contrary to the vision of the Guidelines. The potential end-state of the trend towards more frequent federalism of disaster and emergency response is that rather than being a nation prepared, the United States (and more specifically, the states and local communities) may end up being a nation ill-prepared.

**Recommendations**

Modify the Stafford Act. As the litmus test for federal disaster dollars, the Robert T. Stafford Disaster and Emergency Assistance Act fails to accurately determine which disasters meet the federal requirements and which do not. Congress should establish clear requirements that limit the types of situations in which declarations can be issued – eliminating some types of disasters entirely from FEMA's portfolio. Furthermore, Congress should reduce the cost-share provision for all FEMA declarations to no more than 25% of the costs. This will help to ensure that at least three-fourths of the costs of a disaster are borne by the taxpayers living where the disaster took place. For catastrophes with a nationwide impact, such as a 9/11 and Hurricane Katrina, a relief provision could provide a higher federal cost-share where the total costs of the disaster exceed a certain threshold amount.

Establish clear requirements that limit the situations in which federal emergency declarations can be made. One way to accomplish this is to align declarations with the various scales used for disasters (e.g.,

the Saffir-Simpson Scale, the Richter Scale, and the Fujita Scale). For example, limiting disaster declarations to category 1 hurricanes and above would eliminate all tropical storms that cause some damage, but are not "of such severity and magnitude that effective response is beyond the capabilities of the state and the affected local governments and that federal assistance is necessary."[51]

Another way to accomplish this is to raise the minimum dollar threshold for requesting disaster declarations. The current indicator that federal assistance might be warranted is when a state's storm-related damages reach $1.29 per capita. For several states that is less than $1 million in damages. That is hardly cause for deploying the full might of the federal government. Doubling the minimum per capita with a minimum damage threshold of $5 million (and a maximum threshold of $50 million) would significantly reduce the number of events that would warrant a federal disaster declaration.

Entirely eliminate certain types of disasters from FEMA's portfolio. For example, burdening FEMA with administering disaster relief after a freeze that destroys agriculture crops and does little else is highly inefficient. Similarly, droughts are tragic but generally affect only the agricultural community. Insurance markets and state and local governments can deal with these two types of disasters more efficiently than the federal government can. Finally, while severe storms and tornadoes tend to be localized events that cause property damage and cost lives, they rarely outstrip the abilities of state and local governments.

Restrict homeland security grants to funding only the 37 capabilities on the TCL, which is an all-hazards package that covers the prevention, protection, response, and recovery spectrum. This would contribute to ensuring that federal grants to the states help to preclude the need for federal assistance for routine disasters and to prepare states to work with the federal government in responding to catastrophes.

## Conclusion

Over the past two decades, FEMA has focused too much on day-to-day disasters, from snow storms to forest fires, tripling the number of disaster declarations and overstretching its resources. For too long,

FEMA has federalized disaster response to the point where every routine disaster receives an onslaught of federal funds. The yearly average of federal disaster declarations has tripled in the last twenty years. With the increase in federalization of disasters, the burden and responsibility (or at least the perception of that responsibility) for preparedness and response has migrated from the local and state level to the federal level. The reason for the increase in disaster declarations is largely related to the application of the controlling federal statute for disasters – the Stafford Act. Under this act, the federal government pays 75-100% of disaster response relief as long as a federal declaration has been issued. Meeting the definition for such a declaration is relatively easy, and the financial damage threshold is also low. The ambiguous provisions of the Stafford Act and low damages threshold create enormous incentives for states to seek these declarations rather than shouldering the lion's share of payment, especially as state budgets continue to decline. Returning the focus of disaster preparedness and response to states and local communities will require Congress to take certain actions. Making changes to federal disaster policy will ultimately realign the cost of disaster response and ideally eliminate the subsidy of the minority of states by the majority of states, and will align policy with the principle that all disasters are local.

The focus of FEMA ought to be reoriented to focus its efforts primarily on preparing to respond to catastrophes, not routine emergencies. Lessen the role of the federal government in state-level emergencies and emphasize greater responsibility among state and local communities toward for preparing and developing response plans for local disasters. FEMA should look to radically redefine what it does and what it doesn't do, with the aim of placing the responsibility for disaster and emergency preparedness and response back with states and local communities. Implement reforms necessary to ensure that states and localities regain their primary role in disaster response, and the federal government stops subsidizing the routine localized disasters. Demand that state and local governments pay greater attention to mitigating disaster risks and bear the consequences of responding to disasters exacerbated by poor policies. Place the burden of routine disasters on state and local governments where it belongs.

# Homeland Security Regional Unity of Effort

**Lieutenant Colonel Valery C. Keaveny, Jr.**
United States Army

> The final structural flaw in our current system for national preparedness is the weakness of our regional planning and coordination structures.
>
> —The Federal Response to Hurricane Katrina Lessons Learned[1]

A PRIMARY RESPONSIBILITY of the federal government is to provide security. This core interest mirrors our Constitutional interests: "…to ensure domestic tranquility, provide for the common defense, promote the general welfare, and secure the Blessings of Liberty to ourselves and our posterity…"[2] In fact, President Obama declared in his first Presidential Study Directive (PSD) that his highest priority is to keep the American people safe, combining a focus on Homeland Security (HLS) and national security to create an integrated, effective, and efficient approach to enhance U.S. national security.[3]

The United States government, in concert with state and local governments, has performed well in providing for the security of our people over the course of our nation's history. Following the surprise attacks of September 11, 2001 (9/11), the government reassessed threats and reframed problem sets; identified solutions; created and modified departments, agencies, techniques, and procedures; and significantly increased the effectiveness of those involved with security and defense of the homeland. As governmental organizations have adjusted to the post-9/11 world, interagency and departmental coordination has become more common – especially in the area of HLS. Due to the catastrophic nature of some potential terrorist attacks and natural disasters, multiple agencies and departments are now involved with HLS, along multiple tiers of government. The potential threats necessitate a "whole of community" approach, requiring collaboration and coordination in prevention, protection, response,

mitigation, and recovery. The whole of community includes federal, state, local, and tribal governments; the private sector; and national emergency management, public health, security, law enforcement, critical infrastructure, and medical communities.[4]

To the credit of those involved, many improvements have occurred since 9/11, but unresolved issues remain. One significant challenge is the government's ability to provide security and conduct incident management should the United States suffer a regional/multi-state natural or man-made disaster. There are many possible regional incidents which would require immediate response from federal and multiple state governments. In April of 2005, the federal government published fifteen (15) planning scenarios for local, state, and federal governments to use. The threats included terror threats in the form of explosive, nuclear, biological, chemical and radiological attacks as well as non-terror threats including cyber attacks, foreign animal diseases, pandemics, earthquakes, and hurricanes, any of which can take on catastrophic proportions.[5] "An incident of catastrophic proportions has the potential to imperil millions or people, devastate multiple communities, and have far-reaching economic and social effects."[6]

In each case, a delay of 72-96 hours in providing immediate life-saving measures would be far too long. Clearly, there is a requirement for an immediate regional incident response capability.

A common goal among those involved in disaster response is to achieve unity of effort, described as "coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization – the product of successful unified action."[7] Unified action is defined as "the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities…to achieve unified effort."[8] Homeland Security Presidential Directives (HSPDs) provided initial systems and processes designed to enable unity of effort in disaster response.

Two influential homeland security directives were published in 2003 – HSPDs 5 and 8[9] – which directed the creation of the National Response Plan (NRP) and the supporting National Incident Management System (NIMS) to focus response to terrorist attack,

natural disaster, or other major emergencies. They mandated the creation, coordination, and rehearsal of plans at the national, state, and local levels and associated collective training events. Each level of government is required to maintain the capability to provide oversight of the creation, coordination, and review of their plans, to control execution during rehearsals, and to manage response to an actual event. The Department of Homeland Security (DHS) is tasked with collecting and sharing lessons learned and best practices. In January of 2008, President Bush approved the National Response Framework (NRF) which replaced the NRP.[10] These systems meet the most basic threat scenarios and requirements, but they fall short in that they do not provide for a standing capability to immediately synchronize federal and state support should a catastrophic event simultaneously influence multiple states.

Hurricane Katrina exposed significant regional capability gaps between DHS and the fifty states' independent emergency operations systems. Although there have been some improvements since Katrina, the lack of a regional capability to immediately synchronize efforts remains. This paper studies the requirements for developing a regionally-based HLS collaboration and coordination capability – specifically, one that facilitates unity of effort in managing incidents at the multi-state/regional level. This paper first assesses foundational policies and strategies.

## Homeland Security Policy and Strategy

It wasn't until after the 9/11 terrorist attacks that policies specific to the homeland and its security were published. On 29 October 2001, President Bush issued the first HSPD, designed to communicate United States HLS presidential policy decisions. By November 2008, 24 HSPDs had been issued.[11] There are now a total of 25 HLS policy directives, all published by the last administration. It is under the G. W. Bush administration HSPDs that the Obama administration continues to operate. The current administration has published only one unclassified Presidential Policy Directive (PPD) which pertains to HLS, outlining the composition of the National Security Council without significantly altering national HLS policy.

HSPD-5, published on 28 February 2003, was designed to enhance U.S. capability to "manage domestic incidents by establishing a single, comprehensive National Incident Management System [NIMS]."[12] It identified the authorities and responsibilities of multiple federal agencies and departments and tasked the DHS Secretary to develop and administer the NIMS and to establish the NRP.[13] Prior to the directive, comprehensive national incident response was planned and coordinated by the Federal Emergency Management Agency (FEMA) through the Federal Response Plan (FRP).[14] HSPD-5 also specified authorities and responsibilities for the Secretaries of State and Defense, the Attorney General, and others associated with homeland security and defense.[15] It specified that the DHS Secretary would coordinate efforts when one or more of four criteria are met:

- Another federal entity requests DHS assistance
- State and local authorities are overwhelmed and request federal assistance
- More than one federal entity is involved, and/or
- The DHS Secretary is directed by the President[16]

To guarantee the continued balance of state and federal power as envisioned in the U.S. Constitution, HSPD-5 specifically states "[The] Initial responsibility for managing domestic incidents generally falls on state and local authorities."[17] HSPD-5 mirrors U.S. federal law concerning federal assistance to states during a natural disaster, specifically the Stafford Act. The Stafford Act outlines the hierarchy of efforts, request procedures, and control of federal assistance. It requires a State Governor to determine a disaster is beyond local and state capabilities and requires Federal assistance and it requires the Governor to request that the President declare a given incident a "major disaster." Alternatively, the President, if required by the scope and obvious extent of the damage, can unilaterally declare an emergency.[18]

The NRP and NIMS support the collective and coordinated response to disaster or emergency. The NRP describes the structure for HLS policy and federal authority and responsibility. It also provides the operational protocols for different threat levels; incorporates existing response plans; standardizes reporting requirements, assessments, and

recommendations; and directs continuous improvement through testing, exercising, and new technology. The NRP is specifically designed to become operational through the NIMS.[19]

The NIMS provides for "prevention, preparation, response and recovery from terrorist attack, major disasters, and other emergencies."[20] It is supposed to facilitate a collective approach to incident management in which all levels of government work together – federal, state, local, and tribal. The NIMS was designed to include NIMS core concepts, principles, terminology, and technologies; multi-agency coordination systems; training; resource management; qualifications and certifications; and the reporting and tracking of incident information.[21] The NIMS is the system that provides for collaboration, communication, coordination, and control during the preparation and execution of the NRP. However, though solid as a base system, the NIMS does not provide for immediate response at the regional/multi-state level.

On 17 December 2003, the Bush Administration published HSPD-8 as a "companion directive" to HSPD-5. This directive focused on strengthening and improving the overall coordination, preparedness, and capabilities of federal, state, and local entities. It defined "all hazards preparedness" as including terrorist attacks, major disasters, and other emergencies as referenced in the Stafford Act.

To facilitate preparedness, HSPD-8 directed the DHS Secretary to lead a federal, state and local effort to develop a national preparedness goal with measurable readiness targets, priorities, and assessment metrics. It further directed the initiation of standardization for nation-wide interoperability of first responder equipment standards; the creation and execution of a collaborative, interagency master training and exercise calendar; and the collection and dissemination of lessons learned. HSPD-8 outlines how the federal government awards preparedness assistance in the forms of planning; training; exercises; interoperability; equipment acquisitions; and information gathering, detection, and deterrence based on federally-reviewed, comprehensive preparedness strategies among the states.[22]

To summarize, President Bush directed in HSPD-5 and HSPD-8 the creation of a consolidated NRP and the NIMS through which the NRP would be coordinated and controlled. He also directed the standardization of goals, priorities, training, equipment, information sharing, assessments, and federal assistance. Both HSPDs provided a clear strategic vision of a system which unifies the capabilities of all federal, state, and local authorities in one synergized effort to provide for the common security, safety and general welfare. Both directives provided direction to achieve the strategic vision without creating a specific strategy, technique or procedure. These two policies empowered subordinate departments to develop strategies and programs which brought most of the original vision to fruition. Even though the contributions of these directives to domestic security are significant, Hurricane Katrina demonstrated significant shortfalls in the ability to synchronize the capabilities of the United States during a major regional incident.[23]

**Katrina Lessons**

> *The attacks of 9/11 and Hurricane Katrina were, respectively, the most destructive terrorist and natural disasters in our nation's history and highlighted gaps in the nation's readiness to respond effectively to large scale catastrophes.*[24]

Hurricane Katrina showed that the existing NIMS and NRP, emphasizing the primacy of state and local governments, "did not address the conditions of a catastrophic event with large-scale competing needs, insufficient resources, and the absence of functioning local governments."[25] These conditions significantly degraded the response to Katrina and highlighted the shortcomings with regional preparedness.

In the aftermath of Katrina, the federal government conducted an in-depth review and identified more than 100 recommendations for corrective action grouped within 17 major lessons. Three of the lessons provide for broad preparedness, including: Training, Exercises, and Lessons Learned; HLS Professional Development and Education; and Citizen and Community Preparedness.[26]

According to the lessons learned, national preparedness was a major challenge in that federal command centers had overlapping and unclear responsibilities, plans to replace destroyed local and state operations centers were not in place, support apparatus were overly bureaucratic, and the Joint Field Office (JFO) was not established until after the peak of the crisis.[27] "Our response to Hurricane Katrina demonstrated the imperative to integrate and synchronize our policies, strategies, and plans – among all Federal, State, local, private sector and community efforts and across all partners in the profession…"[28] Although incident response is a primarily a state and local responsibility, the federal government must be prepared to support or fill in for their efforts during a catastrophic event.[29]

> *After the Congressional inquiries and investigations into what went wrong with the response to hurricane Katrina….the majority opinion at the federal level is that [FEMA] needs to be strengthened with many parties advocating a broader role for the federal government and the military in regional disaster response.*[30]

The system, based on the precepts of federalism, required the federal government to wait for state and local governments to reach their limits, exhaust their resources, and then request federal assistance. This approach may be sufficient for most disasters, but did not meet the requirements of a catastrophic event. Current HLS threats demand that the federal government actively prepare and encourage the nation as a whole to do the same.[31]

Our federalist form of government is driven by the Constitution and Bill of Rights and they do not provide any federal authority or responsibility to direct or control a regional disaster response. "The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to States respectively, or to the people."[32] We operate by a state-centered philosophy, even if it is not the most effective way to respond to a major regional disaster or emergency.

The United States has grown and conditions have changed since the Bill of Rights was ratified 220 years ago. Our union has faced many challenges and has managed to maintain, and even strengthen, our

constitutional republic. As federal, state, and local governments have become more interconnected and capabilities have grown, the public's expectations of the federal government have grown exponentially. The federal government's size, responsibilities, and reputation are certainly greater today than they were following our revolution. Although not specified in our Constitution, the States and the American people have frequently come to expect federal response to major disasters.

Federal post-Katrina studies concluded that we must build up the regional structures, integrate state and local strategies and capabilities on a regional basis, and that regional offices should be the means to foster state, local, and private sector integration. They also found that regional offices were well suited to pre-identify, organize, train, and exercise JFO staffs and should be capable of rapidly establishing an interim JFO anywhere in their region.[33] These steps would enable the levels of government to obtain the capability to effectively respond to a catastrophic regional event like Katrina. All of these findings eventually resulted in the shift of responsibility from the newly-formed DHS back to its subordinate organization, FEMA, and its regional offices.

The Bush administration recognized the lack of regional unity of effort and began making corrective actions. In January of 2008, the Bush administration "overhauled the nation's emergency response blueprint… streamlining a chain of command that failed after Hurricane Katrina in 2005."[34] The new 90-page National Response Framework replaced a 427-page 2004 plan, restored FEMA's power to coordinate federal disaster response, and clearly delineated who is in charge and what responsibilities lie with the different tiers of government.[35]

Early on, the Obama Administration also recognized the seam between state and federal response for a regional/multi-state disaster and initiated a study of the issues in February of 2009 through PSD-1. In PSD-1, President Obama directed the review include how to,

> *…strengthen interagency coordination…of the full range of HLS and Counter-Terrorism policies…; ensure seamless integration between international and domestic efforts; ensure a seamless capability within the White House to coordinate planning for the federal government's response to domestic incidents of all kinds;*

> *and retain, within the White House the capacity to coordinate federal, state, local, and tribal efforts to respond to natural disasters, including as a result of hurricanes, floods, fire, and other incidents, if necessary.*[36]

Current policy lacks a specific vision or guidance on the desired interoperability between the federal government and multiple state governments when a major disaster or emergency spans multiple states/a region simultaneously. Policy must be updated to address the state and federal responsibilities and the requirements to respond to a regional catastrophic event in a timely and unified manner. This is an issue of effectiveness and efficiency.

Since Hurricane Katrina, challenges to unity of effort have drawn the attention of state and local governments and multiple federal departments. In February of 2009, DHS, along with United States Northern Command (USNORTHCOM), announced a new program "designed to make states devote more fulltime personnel to drawing up emergency response plans."[37] Teams of two to three fulltime employees were hired to develop plans for catastrophic events including earthquakes and hurricanes in coordination with USNORTHCOM and FEMA. Funding was provided through DHS preparedness technical assistance grants.[38]

In October of 2009, the FEMA Response, Recovery, and Logistics Management Directorates were combined under the office of Response and Recovery. The reorganization enhanced FEMAs ability to provide a more immediate federal disaster response. Within the new office, FEMA has a Planning Division focused on developing, integrating, and coordinating state and FEMA regional catastrophic response plans for earthquakes, hurricanes, nuclear attacks, and other threats.[39]

On 11 January 2010, President Obama signed Executive Order 13528 which established the Council of Governors as required by the 2008 National Defense Authorization Act. The council was created to advise and to collaborate with the federal government on issues related to national security, homeland defense, the National Guard, military support to civil authorities, and synchronization of state and federal military activities. The council consists of two co-Chairs of different

political parties and eight other State Governors. All are presidentially appointed for two years and no more than five members may be part of the same political party. Federal participants include the Secretaries of Defense and Homeland Security, various assistants to the President and Assistant Secretaries, the USNORTHCOM Commander, the Commandant of the Coast Guard, and the Chief of the National Guard Bureau.[40]

One area of friction between state and federal governments originates in HSPD-5 where the Secretary of Homeland Security is tasked to ensure the compatibility of local, state, and federal response plans. In addition to the challenges of interests, budgets, manpower, and priorities, there are more than 87,000 jurisdictions within the United States which complicate requirements.[41] Despite the improvements since 2003, our system has yet to develop standardized readiness metrics, reports, and assessments.

On 29 October 2010, the United States Government Accountability Office (GAO) issued a FEMA capabilities assessment titled "FEMA Has Made Limited Progress in Efforts to Develop and Implement a System to Assess National Preparedness Capabilities."[42] This assessment was a follow-up on FEMAs performance in establishing a national preparedness system, a responsibility assigned in October of 2006 as part of the Post-Katrina Emergency Management Reform Act.[43] FEMA reported that one of its evaluation efforts, the State Preparedness Report, has helped gather data but the data was subjective and open to interpretation. The GAO assessed that since April of 2009, FEMA had not developed capability requirements or an assessment framework and had made limited progress in assessing preparedness capabilities.[44] Without a system to uniformly assess capabilities and issues, obtaining common readiness or the ability to react across multiple organizations in a unified manner will be problematic at best.

Additionally, in October 2010, Representative Bennie Thompson (D-MS), then HLS Committee Chairman, released a statement in response to a DHS Inspector General report on disaster preparedness planning. His statement, validating a continuing shortfall in catastrophic disaster response and in coordination among the tiers of government, follows:

> *The report found that FEMA has made progress in responding to catastrophic disasters, especially with regards to emergency communication. Nevertheless, there still is substantive work to be done in terms of overreliance on contractors, staffing levels, contractor oversight, and coordination with state, local, and tribal leaders.*[45]

Threats and conditions have changed since the founding fathers drafted the Constitution and Bill of Rights and since 9/11. The challenge is to mitigate current threats through enhanced capability without infringing on our Constitution. HSPDs 5 and 8 partially met the challenge and enabled substantial growth in the interoperability of federal, state, and local governments while empowering and strengthening subordinate organizations. More refinement is required. A study of the current systems and threat scenarios is warranted to completely understand the requirements for regional/multi-state unity of effort disaster or incident response.

**Current Systems**

The 2010 National Security Strategy (NSS) states the federal government is integrating domestic all-hazards planning and preparation at all levels of government and, "encouraging domestic regional planning and integrated preparedness programs…"[46] That planning and preparation is conducted under the NIMS Framework as depicted in Figure 1 (see following page). The NIMS includes command structures only at the field level and command is designed to provide on-scene emergency management, even in the case of multiple incident sites.

Figure 1 also depicts multiagency coordination structures in two different tiers at the field, regional, and national levels. The top tier consists of the Joint Field Office (JFO) Coordination Group at the field level, nothing at the Regional Level, and the Incident Advisory Council (IAC) at the National Level. The National level provides strategic coordination, prioritization of assets between competing incidents, and issue resolution.

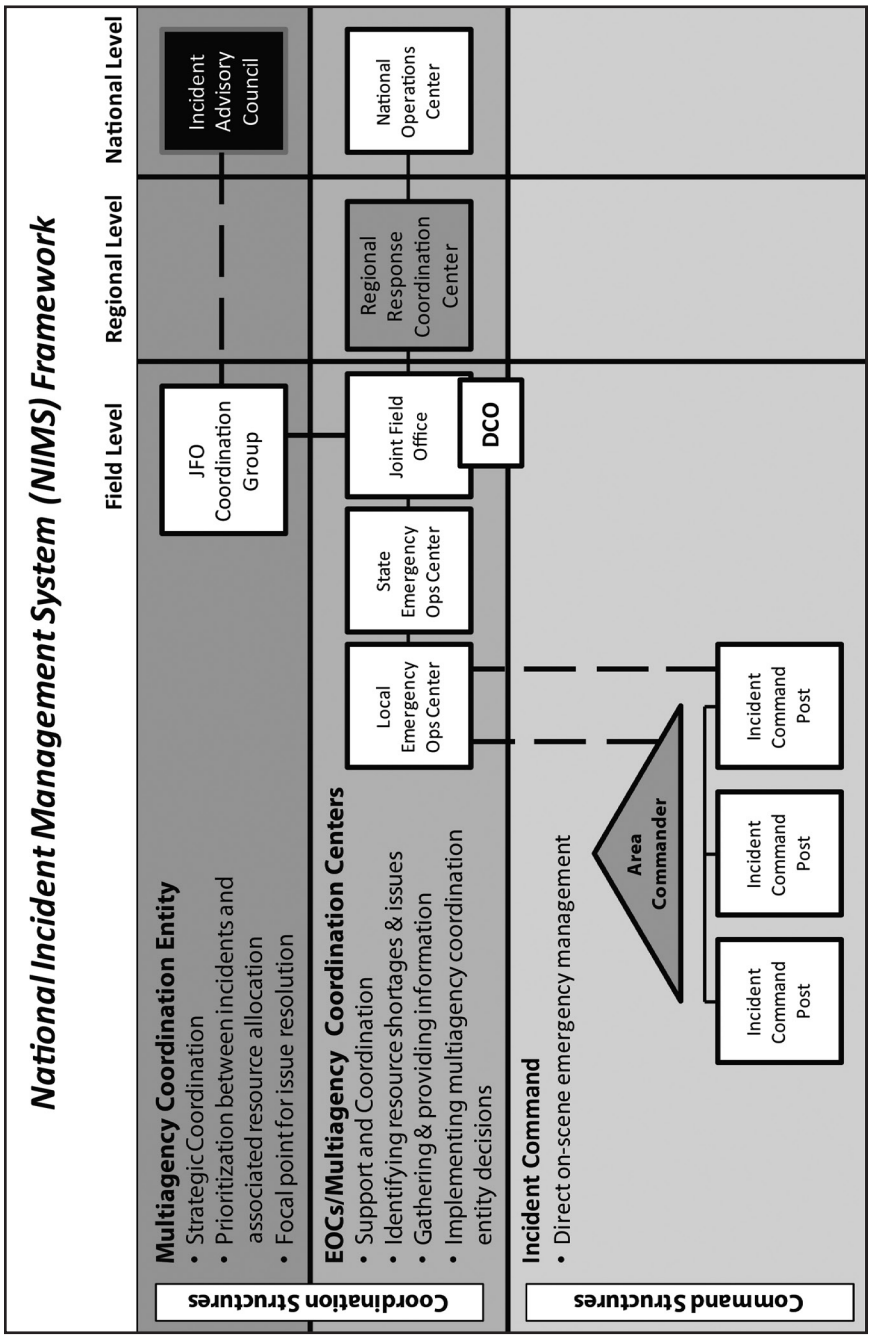



**Figure 1. NIMS Framework**

DHS has published a Standard Operating Procedure (SOP) titled *Joint Field Office Activation and Operations*.[48] The SOP specifies the JFO role in resolving policy issues and articulates that unresolved resource issues "may be handled by the Regional Response Coordination Center (RRCC), the National Operations Center – National Response Coordination Center (NOC – NRCC), the IAC, or may be forwarded through the respective agency chains of command…."[49] In other words, resource issues are managed and gain unity of effort at the middle tier – the tier with Emergency Operations Centers (EOCs) and Multiagency Coordination Centers. This tier warrants greater review.

The intermediate tier, between the on-scene command tier and the strategic policy tier, consists of operations or coordination centers at field, regional, and national levels. This tier coordinates and supports operations, identifies resource shortages and issues, manages information, and implements multiagency decisions. Within this tier, the field level includes standing local and state emergency operations centers and the JFO.

The NOC is a multi-agency operation center, operates continuously, facilitates HLS information sharing and a common operating picture (COP), and provides for coordination with governmental and non-governmental organization (NGO) partners.[50] Within the NOC, the National Response Coordination Center (NRCC) is FEMA's primary operations center and operates continuously to monitor potential incidents and support regional and field elements. The NRCC can immediately increase staff in response to an event to cover the full range of Emergency Support Functions (ESFs).[51] The 15 ESFs are the primary functional areas for assistance.[52] "ESFs provide staff to support the incident command sections for operations, planning, logistics, and finance/administration, as requested."[53]

FEMA provides a regional structure through 10 regional offices which provide continuous representation to and access for states and communities. FEMA deploys people to the offices when state governments request federal assistance.[54] The regional offices are staffed by many of FEMAs most experienced personnel and mobilize federal assets and teams in response to an event. Each office includes a continuously-operating RRCC that expands to become an interagency

facility in preparation for or response to an event. "Ongoing RRCC operations transition to a Joint Field Office (JFO) once it is established, so that the RRCC can remain ready to deal with new incidents."[55]

The JFO is a temporary federal entity, the primary federal incident management field structure, and has primary responsibility for response and recovery. It provides centralized coordination of governmental, private sector, and NGO organizations, but does not provide on-scene operations management. The JFO is staffed by request, based on the incident requirements and may include federal, state, law enforcement jurisdictions, private sector, and NGO representatives. Multiple JFOs may be established if an incident or multiple incidents impact the entire country or multiple states or locations.[56] The JFO is supported by the Regional Defense Coordinating Officer and Element (DCO/E) which serve as the conduit for Defense Support of Civil Authorities (DSCA). Of course, DSCA timeliness is a concern in the case of a major homeland regional incident.[57]

To recap, the current NIMS framework consists of a command system at the field level on the bottom tier, policy arbiters at the top tier, standing mid-tier state EOCs, and ad-hoc mid-tier RRCCs and JFOs. It is worth noting that the only standing organizations at the field level are state entities. This framework is not an issue if the incident and time allows for a deliberate creation of federal capability. The current framework assumes that state and local authorities will desire to and be capable of handling the incident for the first 72-96 hours – an assumption that becomes less valid should a multi-state or regional disaster or emergency occur. In fact, current timelines reflect local, state and National Guard involvement preceding and immediately after the event while the first federal civilian involvement begins between 12-24 hours after the event and Department of Defense (DOD) participation begins after the 24-48 hour mark.[58] Any attempt to assemble, plan and coordinate for, receive and integrate, and employ additional capabilities just adds additional response time. Again, this is not an issue, for instance, for a predictable flood in a single state; but it would be a major issue for a multi-state issue, such as an earthquake.

On 30 September 2010, FEMA's Assistant Administrator for Disaster Operations, Colonel (Retired) Bill Carwile, testified before the U.S.

Senate. His testimony emphasized the necessity for a unified effort across all of the tiers of government and non-governmental players, even within the first 72 hours. He stated that a major event such an earthquake "requires immediate, massive, and sustained support from not only the whole community and federal, state, and local governments, but also from our many private sector and volunteer agency partners."[59] FEMA seeks "the active participation of the whole community to heighten awareness, plan, train, and organize as a practiced team."[60] "We have identified the highest priority tasks necessary to save and sustain lives and stabilize a catastrophic incident during the crucial first 72 hours."[61]

The current policy is reactive and does not provide for immediate, effective response. It requires the federal government to wait until called and then respond, but the rapid and ad-hoc assembly of personnel and capability is not always effective. The President may declare a national state of emergency as another way to quickly marshal the resources of the federal government with less bureaucracy.[62] Even with an early declaration, precious hours are lost as teams assemble – hopefully with the right capabilities, resources, and people. Current threats demand that our federal, state, and local systems prepare to provide immediate, effective response to a regional or multi- state disaster or emergency.

**Requirements and Recommendations**

Katrina and subsequent assessments demonstrated significant shortfalls in providing for regional disaster response and identified the requirements for immediate, effective, unified effort in regional response. Solutions to strategic issues include the identification of the desired ends, the methods/ways to achieve those ends, and the means required by the methods. The desired capability is to provide immediate and effective, whole of community, unity of effort in responding to a multi-state or regional emergency or disaster. Given this broad strategic capability vision, we now must identify the ways and means.

To achieve the desired vision, a regional organization will have to identify essential tasks, develop systems, and gain proficiency in those essential tasks. Based on the GAO reports and FEMA testimony, it is clear that holistic planning, readiness reporting, and synchronization remain as areas requiring improvement. To improve overall performance, one

must identify the organizational characteristics and supporting tasks that a regional organization must perform.

According to the FEMA, there are fourteen "proven management characteristics that contribute to the strength of the overall [Incident Command] System." A few are listed as challenges in the 2010 annual update on the National Security Council and Interagency System, including incident action planning, timely unity of effort, and information and intelligence management.[63] Each of these three management characteristics is supported by three essential tasks which must be achieved to obtain effective regional response. A summary of each of the three tasks is outlined in subsequent paragraphs. It should be noted that these tasks are some of the most difficult things that military organizations struggle with and each of these tasks are currently included as some of USNORTHCOM's unique challenges in the October 2010 annual update titled *National Security Policy Process: the National Security Council and Interagency System*.[64]

The first essential task is to *manage information and maintain situational understanding and a Common Operating Picture (COP)*. The regional organization must receive, process, distribute, and store information. Information management is incredibly important and grows more challenged as information sharing is promoted between federal, state, local, and NGO partners.[65] Based on historical assessments, information management should include reception and review of Incident Action Plans (IAPs), preparedness reports, and the current status of personnel, systems, and equipments. Data concerning capabilities and synchronization efforts should be maintained on a COP and staff section running estimates and preferably posted to what could be referred to as a "Regional Portal." The COP should also contain the disaster assessments and identification of support needs. Responders "…require real time information about the magnitude and effects of natural and manmade disasters to properly, and promptly, tailor effective…support…"[66] Clearly, the COP must include a common view of organizations, capabilities, and the problem.

The second essential task is to *coordinate and synchronize*. With a clear understanding based on information sharing and a COP, the real work can begin "…[p]lanning for, integrating, and synchronizing the

activities of the DOD, DHS, Department of Justice, state and local entities, and NGOs to ensure mutual understanding and unity of effort."[67]

Specifically, a regional organization must be capable of rapidly and continuously coordinating with DHS, all levels of government, governmental departments and agencies, the military components, and the private sector. It must be able to prioritize competing efforts and employ multiple capabilities against a variety of issues, threats, and requirements.

The third essential task is to *manage resources*. The regional office must have precise, up-to-date, knowledge of the types, quantities, and readiness status of all available resources. With this situational understanding, the regional office should identify resource requirements and shortfalls and prioritize limited assets and capabilities. Finally, the regional office must be capable of immediately integrating other capabilities and organizations, at least for the first 72 hours or until a JFO is active. This integration of other units would include, but is not limited to three main tasks:

**Reception, Staging, and Integration**

Each of the three tasks contains many sub-tasks and associated skills. Given this set of essential tasks, one can identify requisite staff functions. Since the RRCC is designed to stand in as a JFO until a JFO is activated, it makes sense that a standing regional capability should mirror the capability in a functioning JFO – which mirrors the Incident Command System (ICS). The DHS JFO Activation and Operations Standard Operating Procedure outlines the JFO staff. It consists of a Chief of Staff; a support staff including a safety coordinator, legal affairs officer, equal rights officer, and a JFO Security Officer and several deputies; Liaison Officers; External Affairs Officers; a Public Affairs Information Center; and the DCO/E. The JFO staff is typically organized into four major sections including plans, operations, logistics, and finance/administration.[68] The ICS staff is identically organized. For continuity and interoperability, this paper recommends mirroring the ICS and JFO staffs.

Having identified the requisite characteristics, essential tasks, and a base structure, it is important to further describe some key points that will make a regional organization capable of obtaining the desired end state. First, a regional organization should include permanent representation from federal agencies and each state, in addition to on-call representation from non-governmental organizations as required by the incident. The requirement for state representation is non-negotiable. Agency representatives might be able to double-up or rotate, depending, for instance, on whether or not they are involved in an ESF. Structurally, the most effective coordinating organizations have a flat hierarchy and free flow of information. This type of organization facilitates collaboration, and ensures that all participants have equal prestige and autonomy.

The facility and information management design should be such that it facilitates continuous situational awareness and collaboration, rapid assessments and prioritization, and timely unified response across the region. Design of physical space and facilities must emphasize the equality of all players and facilitate collective focus on problem solving and synergistic response. Everything must be designed to facilitate collaborative and continuous coordination based on a central COP.

To this point, this paper has listed the characteristics, essential tasks, a base structure, and a few keys to success. Given these details, a team can assemble and begin to form. Any team, expected to perform at an acceptable level within a very short time, must develop systems and processes and train before they can be expected to execute.

In quantifying minimum team processes, the author draws heavily on experience as the Senior Command and Control Trainer at the Joint Readiness Training Center. The most essential tasks, and the biggest challenges, that headquarters have in managing on-going operations or executing pre-planned missions all revolve around the establishment and enforcement of base systems: Organizational and Section Battle Rhythms; Individual and Section Duties and Responsibilities; Planning, Synchronization, and Assessment Systems; and Knowledge Management.[69] Even in a standardized organization like the ICS, it would be virtually impossible for an ad-hoc team to gain any reasonable level of performance in a short period of time, especially when reacting

to a major regional disaster or emergency. It is possible for a cadre to develop, refine, and lead others if the base systems exist and have been previously exercised by the entire team. With those base systems in place, any organization attempting to gain unity of effort must address and collectively practice communication, sharing situational understanding, providing assessments and recommendations, and planning for and synchronizing future operations.[70]

As a regional organization establishes these key processes, their proficiency in the three essential tasks will improve. These improvements will not only show in daily situational understanding, but will show through improved planning, readiness reporting, and the ability to execute crisis and consequence management. It is feasible that the regional offices could take on the task of standardizing and articulating readiness reporting metrics and ensuring the subsequent reporting, tracking, and COP of a region's disaster readiness.

After building the regional capability, the regional teams should be incorporated into pre-planned and no-notice disaster response and military exercises. FEMA will host the National Level Exercise 2011 (NLE 11). NLE 11 is a series of congressionally mandated exercises culminating in May of 2011 with the capstone. It will test the whole of community catastrophic earthquake response, including focus on the interaction between state EOCs, FEMA RRCCs, and federal EOCs. Specifically, response capabilities will be measured in communications, logistics, mass care, medical surge, evacuation, sheltering, public information and warning, EOC management, and long-term recovery.[71] The capabilities that NLE 11 will evaluate should be the desired no-notice and continuous capabilities we intend to maintain.

Having identified the strategic vision and the methods required to reach that vision, means must be applied. Specifically, regional capability facilities and personnel requirements must be identified. Forecasted budgetary constraints will likely limit the means available. This paper has already enumerated the threat and response requirements for a regional capability. Budgetary constraints should not drive a shortsighted or narrow view when searching for means. As we look to raise homeland security capabilities and readiness, we must accept

that it will take time, remembering that it took decades to build our national security systems, arguably the best in the world.

Budgetary constraints require current organizations, capabilities, and facilities be maximized. This paper would suggest that the most effective approach is to integrate all requirements within the existing 10 FEMA Regional Offices and RRCCs. With the facilities identified, the next challenge becomes identifying the personnel to man them.

The optimal solution is to man every RRCC at 100% using new hires, but that is not likely to be considered feasible. Fiscal concerns at all levels of government require the most efficient use of resources. Maximizing current capacity and existing structure will provide the most feasible, acceptable, and suitable course of action.

How could DHS and FEMA obtain a regional capability? FEMA has already invited associations to nominate corporate candidates to serve three month rotations within the NRCC and recognizes that "success depends on the collective and collaborative efforts of the whole of community."[72] This approach also has the potential to work at the regional level, given FEMA's existing ties at local and state level. To minimize requirements, the best approach should be one of batching where a single expert or group of experts represents several grouped industries, businesses, vocations or organizations. For example, one person represents an entire state's first responder organizations. Individual proficiency, regional understanding, and overall preparedness would improve through shared information and lessons learned. FEMA could offset some of the financial burden through readiness grants, much as it did historically for the state disaster response planners.

With an already standing RRCC and some ESF augmentation, one significant manning issue remains – the military. All branches and components of the military may have a large part in regional response, especially within the first 72 hours. In fact, a briefing slide presented by the FEMA administrator in September 2010 reflected DOD as an ESF lead or supporter in all ESFs.[73] The challenge is to ensure an immediate regional military coordinating entity, capable of coordinating all branches of service and components.

Regional DCO/Es, if collocated inside the FEMA RRCC and augmented by a National Guard representative from each of the states within the region, can serve as immediate, temporary operations centers to facilitate military unity of effort until the appropriate Joint Task Force headquarters is established. The Guard representative would be directly responsible for the status of military within their state – Army and Air Guard and the reserves of all branches. Additionally, the state Guard representative would be the conduit for, partner in, if not a planner of, the states' holistic disaster response plans.

Several other options to improve regional capability are available for further study, including the realignment of U.S. Army Corps of Engineer Districts and of existing military reserve force structure. Regardless of the final solution, "Regional personnel must remember that they represent the interests of the federal government and must be cautioned against losing objectivity or becoming mere advocates of the State and local interests."[74] Rewards for regional cooperation and collaboration and for state participation will go a long way in reinforcing the importance of the regional capability.

This paper has captured the requirements for a regional capability. It also identified that the vision of the desired capability is to provide immediate and effective whole of community unity of effort in responding to a multi-state or regional emergency or disaster. This work then provided the requisite characteristics, three essential tasks, a base organizational structure, a few structural keys to success, and minimum team processes required to obtain base proficiency as a regional coordinating organization.

Finally, this study recommended a few means which could be applied to bring about the desired end state. Regional unity of effort is difficult, but it must be achieved. We cannot wait for another 9/11 or Katrina to reprove the existing requirement to immediately synchronize federal support should a catastrophic event simultaneously influence multiple states.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Military Police Mutual Aid and the Posse Comitatus Act

**Lieutenant Colonel Dennis M. Zink**
United States Army

RECENT INTEREST IN THIS TOPIC started with a news report in March, 2009, of Fort Rucker, Alabama, Military Police (MP) being accused of violating the Posse Comitatus Act of 1878. The article published in October of that year by the Dothan Eagle, was a report on the conclusion of an investigation by the U.S. Army Inspector General.[1]

In August, 2009, the U.S. Army Inspector General completed an investigation of an incident at Fort Rucker involving a possible violation of the Posse Comitatus Act (PCA). The results of that investigation concluded there was a violation of the PCA.

> *The first test was whether the actions of military personnel (MPs) were active or passive....By directing and diverting traffic and people, and by their uniformed and armed presence in the streets at TCPs [traffic control points], the MPs actively participated in law enforcement activities.*[2]

This incident presents a distinct case for research as to whether military law enforcement personnel (U.S. Army and U.S. Marine Corps Military Police, U.S. Navy Master at Arms, and U.S. Air Force Security Force Police) should be classified the same as "all" members of the Army and Air Force in relation to the PCA. While there are numerous historical vignettes of "regular" military forces used to conduct civilian law enforcement duties,[3] there are relatively few incidences where military police forces were used to conduct civilian law enforcement.[4] This research will explore these incidences to determine what, if any, benefits or perils there are associated with using military law enforcement personnel to assist civilian law enforcement in cases of mutual aid.

The history of the PCA section will include a review of the law associated with the PCA,[5] what other scholars have written about the

PCA[6] (noting that there are conflicting opinions about the reasons for the establishment of the PCA),[7] and a review of case law arising from use of military forces to conduct civilian law enforcement.[8] The analysis section will include various points of study regarding the history of mutual aid,[9] current emergency response requirements under the National Response Framework (NRF),[10] standardization of first responders under NIMS,[11] similarities in training and certification of military police forces compared to civilian police,[12] and similarities of enforcing state laws both on and off federal installations.[13] The recommendation section will help to establish both benefits and caveats associated with the use of military police forces to conduct civilian law enforcement off of federal installations.[14]

This research is limited to Military Police Mutual Aid and will not cover other Federal Forces, such as the United States Coast Guard, who may be used to conduct civilian law enforcement. For purposes of this research, Department of Defense Civilian Police, including the Departments of the Army, Navy and Air Force Civilian Police, are also included as military police forces since they fall under the restrictions of the PCA unless otherwise exempted.[15]

**History of the Posse Comitatus Act**

The Posse Comitatus Act is an act of Congress written into the code of U.S. law, referred to as the U.S. Code. This act can be found at the government publications website under Title 18, Part I, Chapter 67, Section 1385 (1878). A reading of the act is quick and easy. Section 1385 says:

> *Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a Posse Comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.*[16]

On its face, the PCA looks to be directed at local Sheriff's and U.S. Marshal's who were the main violators of conscripting Army Soldiers and pressing them into service as a posse.[17] However, the congressional records of 1878 show that the language contained in the Knott

Amendment to the Army Appropriations Bill, demonstrates the PCA was, "[c]learly enacted in response to military involvement in reconstruction south."[18]

Congressional members from the Southern States were becoming politically powerful. They used that political power to reverse the influence of the federal government by continued military intervention in the south.[19] In his book, *The Role of Federal Military Forces in Domestic Disorders, 1789-1878,* Robert W. Coakley asserts that the federal government was still involved in the south because of the problems with southern white supremacists and former confederates.[20] Stephen Young reports in his book, *The Posse Comitatus Act of 1878: A Documentary History*, evidence he found that support for enactment of the PCA was also related to Sheriffs' pulling military personnel away from their duty out west.[21]

County Sheriffs and U.S. Marshalls were using their authority to draft and deputize soldiers in their counties to be part of posses. Serving in these posses took the Soldiers away from their military duties. The War Department (and to a lesser extent Congress) wasn't happy that deployed soldiers in the south and out west were being drafted and pulled away from their duties.[22]

These historical accounts provide a detailed record of the War Department's actions, the U.S. Attorney General's actions, and General Ulysses Grant's actions during the timeframe in question. These primary and ancillary actors contributed to the climate that ultimately caused enough support to be garnered for the U.S. Congress to pass Section 1835 of the U.S. Code.[23]

With the passage of the act came restrictions; both intended and unintended. A legal department spokesperson for the Department of Homeland Security, David Brinkerhoff, says that: "In passing the act, the Congress voted to restrict the ability of U.S. Marshals and local sheriffs to conscript military personnel into their posses."[24] As a means to ending military control of the South, the PCA also restricted military commanders from volunteering to conduct civilian law enforcement without presidential approval.[25]

In addition to published historical accounts, there are a multitude of legal opinions and writings regarding the law. The U.S. Army employs several methods to opine on proper procedures and regulatory guidance. The chief method used is the U.S. Army Judge Advocate General (JAG) Corps, also known as Army Lawyers. To ensure military commanders are provided uniform legal advice by the JAG, the JAG Corps publishes several documents. One such document is the Domestic Operational Law Handbook published by the Center for Law and Military Operations.[26]

One section in the JAG handbook covers the history, provisions, applicability and exceptions of the Posse Comitatus Act.[27] Of note, the historical reasons provided by the handbook differ from the historical reasoning of Brinkerhoff.[28] While Brinkerhoff claims the Act was to reduce local sheriffs and U.S. Marshals use of military personnel located in their jurisdiction, the JAG handbook states the Hayes/Tilden election was contested because General Grant used federal troops at polling places in three southern states which possibly caused the electoral votes of those states to be given to Hayes.[29]

Possibly because of the differences in opinion as to the historical reasons and legal applications of the PCA, Congress and the Executive Branch granted exceptions to the act over the years. General Currier's U.S. Army War College strategic research thesis on the PCA being an impediment to transformation contains an appendix with a lengthy table of exceptions to the PCA.[30] Four notable exceptions that pertain to the use of military police in cases of mutual aid are: non-active support to civilian law enforcement off of federal installations; military personnel conducting law enforcement against civilians on federal installations; military personnel providing designated personnel security off of federal installations; and National Guard personnel conducting law enforcement against civilians off of federal installations when activated under state orders.[31]

Currier also discusses the three tests used by the courts in determining appropriate use of PCA. The three tests determine whether military forces regulated, proscribed, or compelled civilian law enforcement actions (U.S. v. McArthur), whether military forces provided active

or non-active support (U.S. v. Red Feather and U.S. v. Hartley), and whether the military forces constituted a pervasive amount of assistance or involvement (U.S. v. Jaramillo).[32]

A second Department of Homeland Security legal department opinion, proffered by C.T. Trebilcock, discusses at length current "erosions" of the act and gives possible areas where the military can become more involved in supporting law enforcement, including civil disturbances and the war on drugs.[33] The opinion continues by stating that military police have jurisdiction over military members subject to the uniform code of military justice (UCMJ) whether on or off federal installations. Trebilcock concludes by surmising that the history of the law was not intended to prevent federal police forces from enforcing the law.[34]

To clarify Trebilcock's point, military police forces only have limited jurisdiction over military members off of federal installations. Notwithstanding criminal behavior conducted on a federal installation, which follows the person regardless of geographic location, jurisdiction over military members off the installation is limited to purely military offenses such as Absent without Leave (AWOL), missing movement, or failure to obey an order. For crimes conducted off of a federal installation and covered under federal, state or local statute, the civilian authorities retain jurisdiction unless granted to the military.[35]

One area not covered in the legal opinions or exceptions to the Act is the possible use of trained and certified military police conducting active law enforcement activities in support of civilian law enforcement officials off of federal installations. Without an exception for this, the PCA will continue to restrict the use of military police forces to aid civilian law enforcement. When the case for mutual aid arose, such as during the Los Angeles riots and after Hurricane Katrina, presidential authority for military police forces to deploy and conduct civilian law enforcement activities was used to great benefit.[36] However, short of a presidential order, the PCA prevents military police mutual aid support.

**Mutual Aid**

Mutual Aid is a concept over 2,000 years old and over 330 years old in America.[37] The concept involves neighboring jurisdictions sending

support to assist other neighboring jurisdictions in putting out fires, rescuing people, and providing additional security.[38] This concept has such wide acclaim that even the National Response Framework, the document that outlines national activities in light of disasters or major terrorist attacks, calls for its use.[39]

From a law enforcement perspective, mutual aid began as historical policing efforts of the Night Watch, Constables, Sheriffs and Posses.[40] Modern policing adopted the concept of mutual aid as more departments became professionalized and similarly trained.[41] In 2003, The Department of Justice and Department of Homeland Security codified the notion of mutual aid between police forces in Homeland Security Presidential Directive (HSPD)-5 - Management of Domestic Issues.[42] Following on the heels of HSPD-5 was the establishment of the National Response Framework (NRF)[43] and the National Incident Management System (NIMS).[44] The NRF and NIMS were designed to better manage emergency response at the local through federal level with standardization of training, operating procedures, and preparedness goals.[45] Both of these landmark initiatives place mutual aid squarely at the forefront of response to crises.

In contrast to these two initiatives stands the PCA. The historical argument for creation of the act (Soldiers being conscripted into a posse) currently precludes federally constituted and certified law enforcement professionals, military police, from supporting local police departments in a crisis (without Presidential or Secretary of Defense [SECDEF] approval).[46] A Director of Emergency Services – formerly known as a Provost Marshal – cannot volunteer to respond to an adjacent local jurisdiction authorities' request for support to conduct active law enforcement operations. In other words, sending military police from Fort Rucker, Alabama to Samson, Alabama (under the authority of the County Sheriff)[47] would run afoul of the PCA despite the new federal desire to rely on mutual aid as a tenant of responding to disasters.

As mentioned in the introduction, the PCA precludes MPs from responding to mutual aid requests, even if they are the closest law enforcement agency. This was borne out in another case near Fort Leonard Wood, Missouri. On July 4, 2009, a shooting occurred at a

park adjacent to the military installation. Of particular note was the mutual aid call that went out. Police from five different jurisdictions responded to the shooting location, except for the closest one – the military police on Fort Leonard Wood.[48]

Only two of the departments had concurrent jurisdiction, the county and state police agencies. Under the structure of mutual aid, responding departments fall under the authority of the Sherriff. This allows mutual aid to work when police, who would ordinarily have no authority in another jurisdiction, gain authority under the Sheriff.

The Fort Rucker, Alabama, violation of the PCA was similar to this incident. The director sent military police to a town outside of the jurisdiction of the federal reservation to which they were assigned. The town was Samson Alabama, and the orders to go were in response to a call for mutual aid. Samson is a small town and was unable to deal with a mass shooting that had just occurred. The shooting caused eleven deaths (including the offender), covered a multitude of crime scenes, and rapidly depleted the local, county, and state police agencies ability to secure evidence and restore safety.[49]

Suffice to say the Inspector General (IG) of the U.S. Army determined the actions of the MPs were active in nature and as such in violation of the PCA.[50] The finding by the IG indicates a gap in availability of military law enforcement personnel (Army and Marine Military Police, Navy Master of Arms, and Air Force Security Police) to support local, county and state law enforcement authorities.

The JAG handbook previously mentioned, outlines the PCA and other elements of federal law relating to Defense Support of Civilian Authorities (DSCA).[51] In this publication is the U.S. Army's legal opinion on such matters as the Stafford Act, and its role in DSCA. The Stafford Act was written in response to several state requests for federal assistance, including federal troops, in the wake of natural disasters and unmanageable natural or man-made incidents.[52] The JAG handbook also outlines procedures for requesting federal assistance, including military personnel.

In addition to the NRF and NIMS, the Department of Defense published the *Strategy for Homeland Defense and Civil Support,*[53] and the National Homeland Security Council published the *National Strategy for Homeland Defense*.[54] These strategic documents set the stage for the "whole of government" approach to terrorism and natural disasters. While not binding, these documents are a baseline proclamation to inform all concerned elements of government and effected private enterprises of the intent should security operations become necessary.[55] The strategy in numerous sections discusses shared responsibilities of all levels of jurisdictions. It discusses the USA Patriot Act, intelligence sharing, intelligence led policing and using all aspects of the U.S. Government (USG) to effect security and manage future incidents. There are continual references throughout about federal, state, local, and tribal assets and efforts and even mentions private enterprises and non-profits. It also discusses emergency management and responses and representative jurisdictional responsibilities. Overall it stresses that we must leverage all assets within USG actions in extremis circumstances.[56]

A scholarly look at the framework of response capabilities includes Posner's assertions on the flexibility of the U.S. Constitution. He argues that the constitution is not a "suicide pact that requires the exclusion of actions to provide security in the face of suspending constitutional rights…"[57] Brinkerhoff's second essay on how the PCA relates to Homeland Security in the wake of 9/11 also allows for the suspension of previously prohibited practices.[58] Louden remarks on the expanded role of law enforcement officials to include service as the on-scene commander – a post traditionally held by a Fire Chief unless it was purely a crime scene.[59] He also argues those officials need to leverage the interdisciplinary community and mutual aid assets.[60] Currently, all manner of military support – fire trucks, helicopters, ambulances, and engineers – are available to assist local officials except for military police.

**Military Police**

It is important to make a distinction here. This position is not referring to all military personnel – it only refers to Military Police

(MP) who are already conducting active police operations – albeit on federal installations. MPs are professionally trained, and in many cases certified, law enforcement officers on federal installations. Their ability to conduct mutual aid is not in question. At issue is the prohibition that off-post jurisdictions have in requesting MPs to respond during mutual aid situations in a law enforcement capacity. MPs can go to an incident to provide advice and information, but cannot conduct any operations related to security, active law enforcement operations, or controlling the actions of the civilian populace without specific authorization by the President or SECDEF.[61] When a military policeman conducts duties on the federal installation, he is appointed by the Army to provide security, conduct active law enforcement operations, and control the actions of the military and civilian populace on federal property. Responding off of a military installation in support of a local police official would be commensurate with their police duties and training. Notwithstanding the PCA prohibition, military police have the capability to perform mutual aid duties in accordance with training and operational policies and procedures.

The training conducted by MPs when conducting law enforcement duties on the installation mirrors that of civilian police officers. Training such as rights of the accused, determining probable cause, the use of force, interpersonal communications, elements of state and federal statutes, and rules of evidence are just some of the many similarities in training.[62] It is a matter of Department of Defense (DOD) policy that MPs enforce many of the state statues on the installation for the state in which it is located.[63] To do that, MPs must be trained and certified.

The prohibitions of the PCA do not extend to exterritorial areas. As such, MPs are routinely deployed overseas and frequently tasked to provide training and supervision of indigenous police forces. Over the years, MPs have trained or partnered with civilian police forces in Germany, Japan, Vietnam, Korea, Grenada, Panama, Iraq, Afghanistan, Kuwait, Saudi Arabia, Egypt, Israel, Lebanon, Taiwan, Philippines, the United Kingdom, France, Belgium, The Netherlands, Columbia, and Honduras, just to name a few.[64]

Military Police also provide law enforcement services on military installations overseas in friendly host countries, such as Germany, Belgium, and Korea. Status of Forces Agreements (SOFAs) prescribe the interaction between the military and civilian authorities off of the military installation, but ordinary procedure is for MPs to work with host nation law enforcement officers in the supervision of military personnel off-post. It is commonplace for MPs to provide mutual aid to host-nation police.[65]

Additionally, the U.S. military relies heavily on MPs to conduct Customs Inspections. Upon return to the United States from deployments or overseas assignments, military members and equipment often pass through a Military Customs Port of Departure. Military Police serve as agents of U.S. Customs and Border Police enforcing federal law. This type of mutual aid is not prohibited by the PCA.

Military Police do have some restrictions on enforcing laws on the civilian populace inside of military installations, but in general, they enforce the same state laws.[66] The major difference is that when a civilian enters a federal installation, they waive many of their rights – including the protection of the PCA where Soldiers would otherwise be prohibited from controlling or detaining them.[67]

When dealing with the civilian populace on a military installation, MPs are required to attend to the exact same professional legal interaction with them as their civilian counterparts off-post. Reasonable suspicion, probable cause, interviewing, detention, search, seizure, and transfer to other competent authorities, all comes into consideration. MPs therefore are required to have policies, procedures and training in place to professionally and justly interact with the civilian populace.[68]

**Possibilities and Perils**

The possibilities and perils research covers current standing exceptions to the PCA, faulty historic incidents of military support to civilian law enforcement, and potential possibilities for Military Police Mutual Aid. Included in the exceptions discussion is an annotation of exclusions and exceptions.

As of 2010, there were 26 exceptions to the PCA.[69] These exceptions range from the use of the Army to protect Yellowstone National Park, to the use of land and naval forces to serve warrants in civil rights cases (at the request of the Magistrate).[70] Other high profile exceptions contained under Homeland Security support, include deterring terrorism (1996 Olympics in Atlanta), interdicting drugs and smuggling (1980s), and civil disturbance operations (LA riots).[71] The DOD currently allows its police, moving between federal installations in the National Capitol Region (NCR), to assist local law enforcement if needed.[72] DOD also allows federal forces, including MPs, to control civilians if the course of providing security for designated personnel.[73]

Protecting the Homeland and providing assistance to the interagency community accounts for several of the exceptions to the act. In the case of nuclear material, members of the military can work for the Department of Justice irrespective of the mission to be performed – including having active role in law enforcement operations. Support to combat terrorism and defense against weapons of mass destruction, specifically biological and chemical weapons is also excluded. Finally, routine support to civilian agencies is permissible, but must be passive, not active. Passive activities include providing intelligence and information, loaning equipment, fixing the equipment, training of personnel to operate the equipment, and personnel service support (cooks, medics, and drivers).[74]

Not all uses of federal military forces in support of civilian law enforcement were exemplary. High profile cases such as Wounded Knee, the Branch Davidian Compound, and the Pullman Riots, gave cause for re-evaluation of allowing for exceptions to the PCA. Anytime federal forces become involved, questions regarding government primacy and government nexus are raised.

Government primacy is the theory that if a government agency responds to or becomes involved in a domestic law enforcement operation, that the government automatically assumes control.[75] This false assumption may unduly cause hesitation for local authorities in requesting assistance, but also on the part of military leaders when providing support. Included in this theory from a litigation standpoint is the argument over government nexus. When federal forces provide

support, they operate under the jurisdiction of the local authority and mitigate the nexus.[76]

Operating under the control of the local authorities is crucial. The National Guard Joint Task Force Commander for response to Hurricane Katrina, Brigadier General Michael Richie, stated his force deployed to Louisiana and worked under the control of the Governor and County Sheriffs.[77] His initial concerns about jurisdiction were alleviated when his task force was ordered to report to, and work for, state and local authorities. They provided him the authority and legal protection while he provided support.[78]

When discussing mutual aid, General Richie did caution about habitually providing support to local authorities, lest they become too dependent on it. His concern stemmed from the State of Louisiana's inability to internally deal with the disaster because over 50% of the National Guard was deployed overseas. He indicated state and local jurisdictions were not self-supporting enough and if in the future, other localities became reliant on federal forces providing mutual aid, and those forces were not available, the municipalities would be unable to deal with a crisis.[79]

Compliance requirements were established under the NRF and NIMS programs to meet several goals. NIMS protocols ensure that local disasters and incidents start and end at the local level, but are supported from a host of authorities above and outside of the local jurisdiction.[80] Because it can be strenuous for local jurisdictions to meet the response and recovery mandates when an incident occurs, FEMA established various command systems, interoperability structures, and training venues to aid local and state jurisdictions. This system of systems ensures authorities are provided tools to successfully manage their disasters, and are not supplanted by federal authorities to do it for them.[81] FEMA also provides non-emergent grants for mitigation efforts, training, and equipping. This effort at improving prevention, preparedness and readiness is supported by NIMS compliance requirements and enables local jurisdictions to respond to crises.

Military Police support for mutual aid is manageable under the NIMS and NRF guidelines. However, in evaluating the relevancy of the PCA,

relating to cases of mutual aid by certified MPs, the PCA comes up short. The possibility exists for the MPs to support local jurisdictions through the rubric of mutual aid if allowed by an exception to the PCA.

The PCA is an outdated concept according to several authors including General Donald Currier. In effect, General Currier argues that while you can use a National Guard Soldier, who only knows how to drive a tank, to perform law enforcement duties, you can't use a military policeman from the local military base because they are a federal asset and not a state asset.[82] Colonel David Bolgiano writes that the military purpose doctrine allows federal forces to conduct law enforcement activities off of the federal installation provided there is a direct connection to the illegal activity and the security of the installation.[83] Jennifer Elsea, in her Congressional Research Report, entitled *The Posse Comitatus and Related Issues: A Sketch*, adds to this by saying that an activity solely for a military purpose – despite having incidental benefits to civilian government and/or civilian Law Enforcement – is permissible.[84]

There are three basic statutory exclusions concerning the military and the PCA.[85] The U.S. Coast Guard is designated as a law enforcement organization and excluded from the PCA.[86] The Insurrection and Sedition Act allows for the President to use federal troops to enforce civil law.[87] The Law Enforcement Support Amendment allows the military to provide information and equipment.[88]

DOD and army regulations play a large role in regulating the usage of MPs off of federal installations. The possibility of opening up an exception to the PCA for military police under the concept of mutual aid is in keeping with ability of DOD to regulate military forces. The benefits of allowing MPs to respond to off-post requests for mutual aid, even in cases of conducting active police operations, outweigh any historical concerns about local sheriff's drafting soldiers to be part of a posse. MPs performing law and order duties off of federal installations are consistent with military readiness and duty performance.

One of the benefits of working mutual aid activities with civilian law enforcement agencies includes providing MPs experience with other departments' procedures and techniques. Partnering with local

law enforcement professionals builds synergy and cohesion. This mutual understanding helps eliminate friction when responding to incidents of significant magnitude. In his article, *Troops Defending the Homeland*, William Banks posits that in the fight against terrorism and other threats to national security, the use of the military in domestic counterterrorism is a wise course to pursue.[89]

**Recommendations**

The spirit of the PCA has morphed from protecting Soldiers so they could perform military duties, to handcuffing military law enforcement personnel from being able to provide local law enforcement assistance in a time of emergency. MPs can be a great tool to enhance public safety and support local law enforcement, but that usage is not without concerns that must be mitigated. If MPs are to serve as that additional tool, another exception to the PCA would be required to allow this aid to occur. Implementation of an exception must cover training, supervision, temporary nature, liability, jurisdiction and local military command approval process.

Training and certification requirements for military law enforcement personnel must be uniform across the services. Variances between military forces and civilian departments must be identified and a strategy enacted at the local level to close those gaps. Local agencies requesting support must understand the limited ways support can be provided. Avenues for cooperation, such as joint training and observation of operations, can increase mutual understanding and foster improved relations. Scenario-based joint training with local law enforcement is a best practice approach.

Supervision of MPs must be limited to the military, not local authorities. A leadership hierarchy containing information on which leader at which level can make what decision is required. When responding to requests for support, tasks are provided by the local authorities, but guidance on the execution of those tasks is the obligation of the MPs in accordance with established procedures.

Memorandums of Agreement are a valuable tool for establishing in advance what type, how much, and for how long, support can be

provided in response to an emergency. Recognizing the temporary nature of mutual aid, agreements for relief must be included.

Assumed liability by the requesting agency must be stated in advance as a means to divest the support provided from the government nexus. When falling under the jurisdiction of local authorities, MPs must be given authority from the supported jurisdiction. Upon competent execution of the support, protection from liabilities associated with that support must also be provided by the local authorities.

Veto authority by the senior military commander or the senior MP is retained. Military missions that preclude the rendering of support take precedence to any prior agreements. Requests for support outside of the scope of capabilities must be reviewed carefully before rendering support. Senior leaders should have a working knowledge of the restrictions and allowances of support to be provided.

Requesting authorization from the President or SECDEF can be problematic at best. In most instances a situation is likely to be resolved before authorization would ever be given. To effect these recommendations for timely Mutual Aid support, a change in law is required. A mechanism is needed to request MPs be exempt from the provision of the PCA in cases of mutual aid.

"Things have changed a lot since 1878, and the Posse Comitatus Act is not only irrelevant but also downright dangerous to the proper and effective use of military forces for domestic duties."[90]


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Contingency Dual Status Commander: Balancing Title 10 and Title 32 Responsibilities

**Lieutenant Colonel William J. Prendergast IV**
Oregon Army National Guard

SINCE THE FORMATION OF THE UNITED STATES, the military has supported civilian authorities across a wide spectrum of events. As defined by the Federal Research Division, Library of Congress, Military Support to Civilian Authorities (MSCA), also now referred to as Defense Support of Civil Authorities (DSCA), occurs during a state emergency declaration supported by a presidential emergency declaration or during a National Special Security Event. Support is required due to a natural or man-made disaster or National Special Security Event, which requires assistance to civilian authorities at the local, state or federal level to help manage a crisis, attack, or calamity.[1] These events can be small in scale or very large, affecting several states; in most cases, the disaster has reached a size or level of destruction that requires additional support from the state or federal level and an emergency or major disaster declaration allows this support to occur. In some of these events, the military might have specialized capabilities or additional manpower not readily available to civilian authorities. This support can come in the form of National Guard or federal military forces. Problems may arise when concerns of state sovereignty conflict with the power of the U.S. President when a natural or man-made disaster occurs and federal military support is required.

In the United States, the governors are the Commanders in Chief of their state's National Guard and the President is the Commander in Chief of Title 10 forces. Both the governors and the President must preserve their legal authority to command and control their forces appropriate to their troops' status, depending on whether in a Title 10 or a Title 32 role. Due to the nature of their state and federal legal authorities, legal challenges may arise when the two forces co-mingle to perform domestic missions. Co-mingling forces may also break the

chain of command, for either the Title 10 or Title 32 force, from their civilian leader; that chain was a basic tenant held by the framers of the constitution when they were ensuring civilian control of the military. Placing either a National Guard or federal officer in command of their respective titled forces was their method of ensuring maintenance of the appropriate chain of command. The shared goal has not changed since the writing of the constitution; it is to place state and federal assistance at the right place at the right time. When conducting consequence management in a politically and environmentally complex situation, state and federal governments will not have time to determine the finer details of federal support. In order to minimize the loss of life and property, policies must ensure the right amount of support is available at the right place and at the right time. To achieve this goal all of the actors must agree, in advance of a disaster, on how to provide a wide spectrum of flexible support from the federal government during times of state need.

This backdrop created the challenges of command and control when considering the use of Title 10, active federal forces, and Title 32, members of the National Guard. This paper will examine how we currently coordinate execution of consequence management during a natural or manmade disaster. It will emphasize the importance of understanding the differing points of view between the federal and state governments, examine the current proposal to create a Contingency Dual Status Commander (CDSC) during the execution of consequence management, and identify the possible points of friction resulting from this solution. Finally, it will offer a longer-term solution to align the state and federal military response.

Joint Publication (JP) 5-0, Joint Operation Planning, discusses the challenge of understanding any operational environment and, in this case, how each set of actors view operational problems through a different lens; different perspectives have led to different definitions and points of view about the use of the CDSC. The current situation is extremely complex and interconnected among factions of political leadership, the military structure and historical precedence.[2]

Several legislative acts affect the military's response to a request for assistance. In addition to legislation, history offers several examples in which MSCA has worked well and others where it has not met expectations for success. The friction about command of the National Guard and federal forces, while executing consequence management, is rooted in Federalism and the conflict between states rights and the federal government. Unity of effort, for the military, during a no-notice or imminent disaster that requires responding to the needs of the people, is an end-state that the actors at all levels of government wish to achieve. It is important to discuss legal limitations when combining state and federal efforts to appreciate the complexity of the problem. Though laws direct and guide the governments in the United States, there are often minor changes in law or policy that makes it possible to reach goals that previously eluded us.

## Legislative Background

There are three major legislative limitations or constraints on MSCA. This legislation is the basis and guide for any military action within the United States. Two basic principals have evolved from the early history of the United States and continue to evolve to meet changing circumstances. The Posse Comitatus Act and the Insurrection Act were early tenets for the use of force by the United States Army; these acts were in response to experiences with the British Army prior to and during the Revolutionary War. The older of the two bills is the Posse Comitatus Act. Taken from Latin, Posse Comitatus is the "power of the country" or "the force of the country" which dates back to English law established in the 15th century.[3]

With the break from British rule and the creation of our nation, the use of the military against the civilian population was important to the framers of the Constitution. However, the framers did not specifically place limits on the Army from acting against the citizens of the new nation, but rather balanced its control between the President and the Congress. They established checks and balances between command of the Army, exercised by the President, and its' funding by the Congress.[4] Laws regulating the ability to use the militia and the army had only a few small changes in the period up to the Civil War. The use of

the Army during reconstruction led southern Democrats, during the Grant Administration, to propose more control over the Army's ability to conduct operations in the United States against citizens of the country. Matt Matthews, in his history of Posse Comitatus Act and the Army, states, "…there can be little doubt that the Posse Comitatus Act was a direct result of the Army's involvement in Reconstruction and the military's involvement in Grant's campaign against the (Ku Klux) Klan."[5] This rise against the aggressive policies of the North changed the definition of Posse Comitatus and created a law that continues to affect the employment of the military within the United States.

Modified through the mid-20th century to include its application to the Navy, Marine Corps and the Air Force, through policy not law, the law received its first major clarification in 1973, resulting from the siege and associated law enforcement activities at Wounded Knee where the Army and National Guard supplied assistance and equipment to federal law enforcement officials. Due to the Army's actions 83 years earlier against the Sioux at Wounded Knee, the federal government wanted to prevent similar events by limiting military involvement in law enforcement activities.[6] During their trial, the defense team for members of the American Indian Movement (AIM) contended, in one of the lines of defense, that the military's involvement violated the Posse Comitatus Act. It took years of litigation, but the courts did what Congress had been unable to do; it gave a legal description of what the Army could do in support to law enforcement. The courts placed military support into two types of activities, active or passive. The courts prevented the Army from conducting active support, but allowed the support in the form of guidance, material support and basic intelligence activities.[7] The courts were able to give the Army and, by this time, the military, clear guidance on the lawful types of support to law enforcement. The act had evolved from preventing federal forces from interfering in the governance of states in the south to clearly defined areas of support during law enforcement events and activities. As defined by Sean McGrane, the Posse Comitatus Act finds in its roots, "the idea that military personnel are trained to act in circumstances where defeat of the enemy, rather than the protection of constitutional freedoms, is the paramount concern; and that applying such a mindset to domestic law enforcement would be a significant

'danger' to the rights of Americans."[8] Posse Comitatus and the Posse Comitatus Act, along with the Insurrection Act of 1807, have guided military use in the nation for over 100 years.

Continuing the checks and balances found in the Constitution, the Congress has the power to call the militia to federal service, but the President is the Commander in Chief of the militia once called to service.[9] The Insurrection Act allows the President to call the military to service for domestic situations. The act has its roots in the 1792 Calling Forth Act and the Judiciary act of 1789; both pieces of legislation clarified the use of the militia, the power of the federal marshal and the ability to call the military in execution of the marshal's duties.[10] These acts also had very specific guidance for the President, working in conjunction with the courts, to call the militia. The Insurrection Act gave the President the ability to call the militia to service when the laws of the United States are not being followed or the application of the laws are being obstructed.[11] The act provides the President a clear path to follow in any situation where calling the militia is required. One of the key requirements of the act was the President must issue a dispersal order, giving time for the insurrection to end prior to calling the militia to enforce federal laws.[12] The first use of the law was during the Whiskey Rebellion in 1794 when President George Washington moved to disband a large number of insurrectionists in western Pennsylvania.[13] The call up of the militia ended with little bloodshed and a return to normalcy in the counties affected by the insurrection. This was the first use of the militia to support the laws of the federal government. President Washington's successful use of the Calling Forth Act and the dispersal order written by Alexander Hamilton, which gave extremely clear guidance and instructions, was an endorsement of the laws. Some of the more stringent parts of the act were removed to allow future Presidents more flexibility to apply the act.[14] Several Presidents invoked the act in the latter part of the 20th century to protect civil rights in the south, aid in hurricane recovery and respond to the Los Angeles riots in 1992.[15] During each of these cases, the President executed the act in a different manner and situation. In some cases the state governor requested assistance; in others the President acted without a governor's approval or request. For example, to enforce school desegregation in the south during the 1950s and 1960s, the

President invoked the Insurrection Act to use the National Guard to enforce federal law. The Posse Comitatus Act and the Insurrection Act work hand-in-hand when considering calling the military to operate within the United States.

The origin of the Stafford Act is in the expansion of the federal government's power to help end the depression in the 1930's. The New Deal and the creation of federal agencies to oversee its projects created a situation where the government was more involved in funding and assisting the response to major disasters.[16] This worked with President Roosevelt's policies for recovery of the United States from the depths of the Great Depression. However, until 1950, disaster recovery and federal funding had little structure and each disaster response was different from previous responses. It was the Civil Defense Act and the Disaster Relief Act of 1950 that established the current methodology behind disaster response and the bottoms-up approach for requesting assistance from the federal government.[17] The federal response continued to grow in scope through the middle 20th century and in 1979 the creation of the Federal Emergency Management Agency consolidated all of the federal programs that were involved with federal emergency response.[18] In 1988, the federal response to natural disasters received further clarification with the Robert T. Stafford Disaster Relief and Emergency Assistance Act. The Stafford Act provided a framework for federal response to natural disasters. It created the current process in which state governors declare a state emergency or major disaster area and, in turn, request federal assistance from the President.[19] The Stafford Act further strengthened the Federalism approach to disaster response and recovery. The state requesting assistance must first expend all options within their state emergency response plan before being eligible to receive federal assistance. Although there is no guarantee the President will issue a federal declaration for the emergency or major disaster, which invokes the Stafford Act, he is likely to do so when the requesting state has met federal minimum requirements.

Each of these acts defines and places constraints and limitations on the military's ability to operate within the United States. The acts give a framework to both state and federal levels of government during situations where military use may be required within the United States.

The acts are rooted in Federalism, balancing states' sovereignty with the federal government's authority. One of the key features of each act is its evolution over time to meet the needs of the government while responding to current events based on the failure or success of pervious federal responses.

**Post 9/11 Adjustments and Reorganization**

Legislation directing federal forces' response to disasters has been mostly a reactive process. In the case of the Stafford Act, the focus is the ability of the government to support the population or reduce suffering after a natural disaster. In the Posse Comitatus Act, the intent is to prevent the Army from conducting operations against United States citizens, and the Insurrection Act is to address situations where states are unable or unwilling to enforce federal law. Before the terrorist attacks of 9/11 these three acts did not align and changed independently of each other. Established in March of 2003 due to the attacks on 9/11,[20] the Department of Homeland Security (DHS) placed many small agencies and departments under one cabinet umbrella to improve the federal response to disasters. In response to the attacks, the federal government consolidated authorities to increase the government's ability to detect and respond to possible future attacks. The federal government's reorganization had unintended effects on support to civil authorities; in their rush to establish an organization that oversaw the safety of the homeland, they did not anticipate unintended effects of adding an additional layer of bureaucracy to agencies that had functioned for many years without a higher-level organization. The Federal Emergency Management Agency (FEMA) was one of the organizations that had operated very effectively without specific cabinet level oversight, but its placement under DHS helped streamline the coordinated response to terrorist acts and natural disasters.[21] At the time this consolidation made sense, especially with the 9/11 attacks and the difficulties encountered when organizing the federal response to a homeland emergency.

The first significant, post 9/11 test of DHS came in late summer of 2005, with the response to Hurricane Katrina. With the linkages and historical partnerships to FEMA broken, the agency struggled to achieve the expectations of the public and elected officials. Even after

removing political rhetoric and unfounded finger pointing, the response to the disaster did not meet the public's threshold for an acceptable response from any agency or level of government. This led to the Post Katrina Emergency Management Reform Act of 2006, which attempted to correct some of the gaps in the organization, structure and operation of DHS.[22] The corrections continued with the 2007 National Defense Authorization Act, which gave the President the authorization to mobilize the National Guard in response to a terrorist act or natural disaster.[23] These changes in the provisions of a current federal law increased the President's ability to respond to crisis within the United States. However, most of the state governors and their adjutants general did not agree with this increase of the President's power and reduction of state rights. The states responded with overwhelming pressure on the federal government, resulting in the striking of the natural disaster provisions of the law.[24] The removal of these provisions prevented the state governors from loosing authority over their National Guards. As discussed in the article *A Brief History of the Evolution of United States Disaster Policy*, the government has shown three stages in reacting to disasters:

> *The specific reactionary relationship of the government can be observed in three evolutionary policy stages from the mid-nineteenth century to the present. During stage one, there is a loose government initiative in respect to implementation and coordination of policies at all levels of government, with little attention given to future events. In stage two, the government takes on a more assertive role; however the state and local government units are predominantly responsible for mitigation and relief efforts. Entering into stage three, disaster policy begins to stray from the prior two stages in that the federal government attempts to meld national security and disaster policy together.*[25]

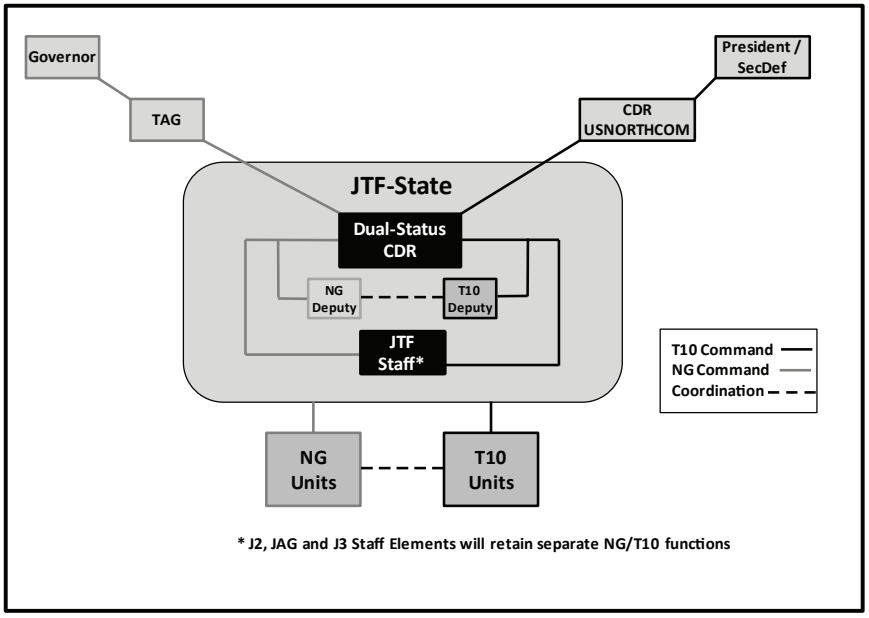
As the federal government attempted to consolidate the federal agencies conducting consequence management, there was also an attempt to streamline the President's ability to marshal all of the resources available to execute consequence management as quickly as possible. However, the governors' perception was that the act was a movement towards control of the National Guard without the approval of the governors, a move that was contrary to the principal of dual sovereignty and the balancing of state and federal power. Currently President Obama has

established a "Council of Governors" to provide the Executive Branch advice on homeland security and matters relating to the National Guard. This council is comprised of 10 state governors – five from each political party – representing states from across the nation.[26] The council gives the governors access to the President on matters relating to the National Guard and eliminates the impression that the states' opinions do not count, an impression given by the content of the 2007 National Defense Authorization Act. The National Guard Bureau (NGB), Department of Defense (DOD) and U.S. Northern Command (USNORTHCOM) are working in conjunction with the National Governors Association and the Adjutants General Association to solve coordination problems. At this point discussions have begun, but a resolution is not imminent. The removal of the original language of NDAA 2007 created a gap between the governors and President when requesting Title 10 personnel and assets to support state activities in response to an imminent or occurring natural or man-made disaster. This gap creates issues and concerns for military organizations due to the lack of unity of effort, which is a basic tenet of military leadership. This unity is extremely important to the disaster response; alignment ensures state and federal resources have the correct level of use and are available at all times.

**Dual Status Commander**

Under the dual status commander (DSC) concept, the commander would be able to respond to command and control needs of both the state governor and the President.[27] The issue of meeting the needs of the governor to protect and secure the citizens of his state, balanced with the needs of the President to maintain control of federal forces, is crucial to this success of this alternative. The current and agreed upon solution for National Special Security Events entails establishing a DSC to serves as the Joint Task Force Commander of both Title 10 and Title 32 forces. This solution allows military commanders to serve in both Title 10 and Title 32 capacities during the event. Key to the DSC concept is the separation of authorities to ensure Title 32 and Title 10 maintain their distinct lines of command and tasks while the concept is in operation.[28]

As seen in the diagram below, the DSC has two chains of command and the two chains operate separately from one another. It however, "provides a common operating picture to both sovereigns, thereby allowing for greater efficiency, less redundancy and greater unity of effort."[29]




**Dual Status Commander Wire Diagram**[30]

Unity of effort occurs when the same officer, the commander, is responsible for both constructs while conducting operations, has the ability to understand and see the concept of operation for both elements and can quickly see and assess the friction between the two. To clarify, dual status revolves around the commander, not the command. This ensures the separation between state and federal forces, a separation that would otherwise limit the possibility of commanding both forces simultaneously.[31]

This eliminates duplication and increases efficiency since the commander must understand the legal constraints for using Title 32 and Title 10 forces. The commander must manage each separately and the overall structure is set up to prevent Posse Comitatus issues or challenges seen at Wounded Knee in 1973.[32]

Executed successfully at several National Special Security Events (NSSE), discussions have begun about the DSC model and its use during consequence management situations. When applied to consequence management situations, the DSC model is referred to as the Contingency Dual Status Commander (CDSC) concept. During a NSSE, all of the actors are able to meet before the event, work through issues, and select a DSC who has approval from the Governor and the President. Considering the DSC model for consequence management will require detail conversations between the states' military departments and the DOD. Unlike a NSSE, an imminent or no notice disaster requires the military to move quickly.

As seen during Hurricane Katrina, public opinion forced political action after the response was well underway. National Guard and aviation assets were in the disaster area within days. The National Guard responded with 40,000 Guardsmen in 96 hours; the Air National Guard provided most of the airframes used to move them.[33] Coordinated with a conference call, the National Guard was able to respond quickly to the disaster, however the media and public from outside of the disaster zone held the opinion that the federal government was not moving quickly enough to minimize suffering. Elements of the 82nd Airborne Division and the 23rd MAGTAF provided the federal military response.[34] Due to the lack of a unified effort, federal military and National Guard forces had overlaps and duplications in their efforts to clear the city.[35] If a CDSC had been in place, the commander would have been able to prevent duplication of efforts and conserve resources during the response.

The main difference between an NSSE and consequence management is time available to respond. Time is required to ensure the necessary agreements are in place, the commanders have met with their Title 32 and Title 10 staffs, and there is a basic understanding of the requirements for consequence management. As with any plan or operation, the enemy, or in this case the disaster, has a say as to where the disaster is located and when it occurs. The plan may not be developed and personnel may not be available or ready.

A key to the entire process is to conduct all of the leadership and much of the personnel selection and education prior to a disaster.[36]

It is essential that states select officers who have the ability to make it through a federal vetting process, by USNORTHCOM and the President, which allows the selected officer to take command of Title 10 forces during a disaster response. In concept, the officer would be in the Title 32, National Guard and the Title 10 chains of command.

**Friction**

During a consequence management event there is usually friction among at least some of the actors involved. Key actors include the media, the population, elected officials at several layers of government, non-governmental organizations and the commanders of the military organizations participating in the response. Clausewitz discussed how friction causes one to fall short of the intended goal, in part due to the human nature of the individuals involved in the action.[37] Some of this friction starts with the limitations and constraints placed on the military by current laws, as discussed above, as well as public opinion and political guidance due to that opinion. Military leaders must work to reduce this friction prior to an event occurring. One of the ways to reduce friction is to create doctrine that aligns all elements within the DOD. For example, the draft version of FM 3-28, Civil Support Operations, does not fully align with concepts from USNORTHCOM.[38] The current challenge with the CDSC is that legalities and common understanding of the mission are still undefined, which is creating a situation where a solution is in the process of being implemented but the outlying actors are creating doctrine and policy without understanding the current relationships among USNORTHCOM, NGB and the State Adjutants General. Having a common picture and understanding of the process will minimize the friction prior to an event occurring and while managing the consequences of the event. Once the CDSC is in place and responding to a crisis, friction will develop around the CDSC and his reporting to both the Title 32 and Title 10 chains of command. The ability to forecast tensions would be extremely difficult, but developing relationships between the selected CDSC and likely Title 10 deputy commanders and staff would minimize operational friction during an event. As with all military actions, friction will develop; however, it is the mitigating steps prior to developing the CDSC that will reduce friction to manageable levels.

**Long Term Solution**

To develop a long-term, sustainable solution, a change is needed to allow the National Incident Management System (NIMS) and Incident Command System (ICS) to function as designed: to facilitate and assist state and local agencies in any crisis.

> *(NIMS) provides a systematic, proactive approach to guide departments and agencies at all levels of government, non-governmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment.*[39]

Within the NIMS framework, the ICS is the management methodology that incident leadership follows when responding to any type of event that falls within the purview of NIMS. The ICS is a collaborative team process that allows participation from any organization that is a stakeholder in the event the ICS is managing. The National Response Framework (NRF), which is the structure that gives national-level policy for incident management, would require restructuring to place the military under the NRF and ICS during times of implementation.[40] A change to NIMS and the ICS will allow the military to be a more active member of the incident command structure and would allow the military to become fully integrated and participating member in the disaster response. Currently, as discussed in FM 3-28, the military does not abandon its mission command and operational methods to conform to NIMS. However, they adapt their operating procedures to interface with the other governmental agencies.[41]

This change for the military would have two consequences: the civilian heads of the military would remain in charge of their responding forces through the CDSC and would remain participating members of the ICS, much like a coalition framework or our participation in the North Atlantic Treaty Organization. The ICS provides resources and a framework for the requested federal support and its strength is that it provides a framework for operating as a collective rather than using a federal or state agency in the lead.[42] NIMS and the ICS provide a

very well-rounded and tailored response to any emergency. In addition, municipalities who receive federal funds under NIMS must agree to follow and participate in the ICS when required. This option places the resources from both the federal and state levels on equal footing and would place the command structure for the military in the ICS and the NRF.

In addition to creating a CDSC, finding a long-term solution is necessary before response to a future disaster provokes public opinion and politics to force externally driven change. The states did not accept the legislation contained in the 2007 NDAA, largely due to a lack of consensus building with the governors prior to the laws approval. The federal government could build consensus with the states about calling the National Guard to service, but discussions would have to be open and include a select group of governors that represented the National Governors Association. This mechanism is already in place with the President's Council of Governors. The proposed law that would have given the President authority to call the National Guard without approval of the state governors is an excellent example of how difficult it is for all interested parties to read and understand an entire bill prior to making it law. A small section of the bill slipped into the law with little or no review. However, with the participation of the state governors in an open and frank discussion about how to improve response to disasters, the actors could agree on changes that would approve the call up of the National Guard while ensuring state sovereignty.

The concept of a CDSC during disaster response is a highly charged political issue. One should not downplay the perceived threat to the authority of the governors or the President. However, many elected officials want to avoid the political fallout similar to that seen after the Hurricane Katrina response. Anticipating political considerations in the discussion would allow the CDSC option to be successful and elected officials, in conjunction with their respective military organizations, should see this option as a means to minimize the loss of life, property and resources.

The stakeholders in this issue approach the problem with widely different points of view. They all have the common interest of coming to a resolution, but each approaches the issue with differing

perspectives. It is only a matter of time until a disaster forces the federal and state governments to consider unity of command and effort while in a complex environment. Understanding the differing points of view between the federal and state governments is extremely important to determine a feasible and long-term solution before a disaster forces the actors to make rushed and possibly less than optimal decisions.

**Recommendation**

The CDSC concept is the correct process to manage and create unity of effort during a consequence management operation. USNORTHCOM, in conjunction with NGB and the adjutants general, must create a vetting process that meets the needs of Title 10 organizations, but recognizes the requirements of the National Guard. The vetting process must allow adjutants general to submit qualified officers from within their commands. In turn, USNORTHCOM must create a series of courses that develop the skills of the selected officers, while maintaining their traditional National Guard status. These courses should include training exercises with possible Title 10 staffs who may respond as the federal portion of the CDSC's force during a consequence management event.

During the current series of mobilizations, many senior National Guard officers have operated at battalion or above organizations in support of contingency operations and have operated with Title 10 staffs and senior level commanders. Tabletop exercises or other staff training would develop effective working relationship between the selected CDSC and Title 10 staff. The National Guard must also select alternate CDSC officers for their plan, in case the primary selectee has civilian business or other conflicts and cannot serve. The alternate could be a deputy commander or another brigade commander from the same state. To ensure that USNORTHCOM training occurs and builds necessary long-term relationships, the assignment of federal forces must be by FEMA region. In some situations, the Title 10 staff may be from another service due to location and regional availability of Title 10 forces. Developing long-term relationships is paramount to the success of the CDSC. If the commander has worked with the Title 10 and Title 32 staffs, success will be easier to attain.

Each state must develop officers who are qualified to become DSCs. Selecting a Title 10 officer for the DSC position fails to take advantage of the strength of having an officer from the state who knows the environmental and political landscapes; this would give some of the rights of the National Guard to federal forces if a state cannot fill the DSC position.

## Conclusion

The most feasible solution to the problem of effective command and control of combined state and federal forces is the Contingency Dual Status Commander concept. This decision is feasible due to the lack of legislation needed for implementation. One key to the DSC concept's feasibility is that it is a policy change rather than a legislative change, which allows for quick implementation and closes the gap created by the 2008 NDAA. The CDSC concept is also sustainable by requiring officers to be approved prior to a disaster occurring. The number of Dual Status qualified officers is a metric that is measurable for each state, and can be used as an indicator of that state's level of preparedness for a no-notice or imminent disaster. The CDSC option also allows for a legislative long-term solution by establishing a program consistent with a legislative solution that changes the Stafford Act to allow CDSCs when a state governor declares a state emergency or major disaster. A change in the Stafford Act would be consistent with current legal uses of CDSC for responses using combined state and federal forces. It would also allow the CDSC to serve as a member and, when appropriate, lead in the ICS. A legislative change should be a long-term goal to take advantage of the systems that are already in place, but is unlikely until a failure in disaster response forces the system to change. The CDSC allows the National Guard and the DOD to become partners in the solution. However, there are several pitfalls with the CDSC concept. The largest of these is the approval process for Title 32 soldiers chosen as the possible National Guard DSC. As much as the National Guard has participated in operations overseas, there is a lingering doubt among many in DOD that a National Guard officer has the ability or skill to lead federal soldiers. A solution requires the active component to acknowledge that there are qualified National Guard officers who are capable of serving as CDSCs. The most important problem to address

is the effective response to natural disasters to minimize the loss of lives and property while conserving the resources of both the state and federal governments. The response to Hurricane Katrina had successes, but the initial response from state and federal governments was not effectively coordinated and lacked unity of effort. Elected officials must focus on the task of approving legislation designed to avoid repeating these failings. They must also ensure that a discussion about the Contingency Dual Status Commander concept occurs at all levels to address concerns and friction points prior to a disaster occurring. The state and federal governments must make the hard decisions sooner rather than later. These decisions will help Americans recover from disasters and strengthen positive public opinion about the effectiveness of our military and civilian leadership.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Section Three

## Border Security


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Introduction

**Colonel Steven P. Carney**
Homeland Defense and Security Issues Group
Center for Strategic Leadership
U.S. Army War College

THE ILLEGAL DRUG TRADE across the U.S.-Mexican border, and the loosely estimated billions of dollars that change hands each year, has enabled, if not empowered, human smuggling, human trafficking and the gun trade to flourish in northern Mexico. This section offers three papers addressing these issues: one focusing on the increased power of drug trafficking in the region; one focusing on the rise of narco-terrorist organizations in northern Mexico; and one recommending a new "whole of government" approach to addressing these and similar threats.

Lieutenant Colonel John P. Maier's article, "The Mexican Cartels and Jihadist Terrorism: The Nightmare Next Door," posits the metamorphosis of Mexican Drug-Trafficking Organizations, into asymmetrical narco-terrorist groups. Lieutenant Colonel Maier argues the current deteriorating conditions of local government services in northern Mexico are favorable for an increase in transnational threats. Maier examines not only the deleterious effect of drugs flowing north from Mexico into the United States, but also the estimated annual rate of 10,000 illegal guns and billions of dollars flowing from the United States into Mexico, as manifestations of the emerging problem. Maier suggests the synergy between the narco-terrorist drug cartels and Jihadist terrorist organizations exposes the blurred line between terrorist and criminal organizations seeking to destabilize the Mexican government and fund activities via the drug trade. If left unchecked, Lieutenant Colonel Maier warns Jihadist organizations will later seek to target and destabilize U.S. cities and communities on the southwestern border.

Special Agent Michael D. Kennedy's article, "Securing the U.S. Southern Land Border: Enhancing the Interagency Effort," makes a

sound case for the establishment of a Border Interagency Operations Center in order to fuse command responsibilities within the Department of Homeland Security (DHS), Department of Justice and the Department of Defense. Kennedy convincingly argues each of the three Departments have their own intelligence fusion cells, but require a collaborative operations center to achieve unity of effort in a multi-agency, multijurisdictional environment. The author posits the establishment of Border Interagency Operations Centers will allow for all agencies to legally maintain their statutory authority, responsibility and authority, and to effectively manage task forces on the southwestern border.

The U.S. National Drug Threat Assessment 2010 report estimates that heroin production in Mexico jumped from 17 metric tons in 2007 to 38 metric tons in 2008. Colonel John Stewart's article, "U.S.-Mexico Security Cooperation: The Time to Act is Now," suggests that the illegal drug production center of gravity is no longer in Colombia, but closer to the source of U.S. demand in northern Mexico. Colonel Stewart opines that drug trafficking organizations continue to terrify the populace and local governments in northern Mexico through the use of intimidation, murder, and corruption; and increases the security threat to states along the sizeable, if not porous, U.S. southern border.

Colonel Stewart's discussion includes the history of long standing traditional views and mistrust between the United States and Mexico in order to frame the current problem. Stewart contends that a whole of government approach must be maintained and funded to address the two-sided drug dilemma of illegal supply and illicit demand. Colonel Stewart concludes with the observation that the momentum for improved relations between both governments is present, and warns the program must continue to be funded beyond the U.S. national elections in 2012 in order to achieve positive results.

# The Mexican Cartels and Jihadist Terrorism: The Nightmare Next Door

**Lieutenant Colonel John P. Maier**
United States Army

THE RECENT NETWORKING between the Los Zetas Drug Cartel and The Iranian Revolutionary Guard (Quds Force) is the opening volley in what is likely to be a long, painful and violent coupling of international criminalization and Jihadists terrorist ideologies.[1] Mexican Drug-Trafficking Organizations (DTOs) have morphed into asymmetrical narco-terrorist groups that now control the Mexican side of the border. These Transnational Criminal Organizations (TCOs) represent the greatest security threat facing the Mexican government and present a significant threat to the national security interest of the United States.[2] Understandably preoccupied with their repetitive assignments to Southwest Asia, most military professionals are unaware of the dire situation in Mexico.[3] Given the proximity of U.S. military bases to the southwest border, the recruitment of U.S. military personnel into these TCOs, and Mexico's need for U.S. assistance, must be addressed. Senior defense professionals must become aware of the situation and insure that their intelligence personnel monitor the TCO threat.

Since the spring of 2006, 40,000 thousand people have been killed in the Mexican drug wars, an overwhelming majority within an hour's drive of the border.[4] The U.S. Customs and Border Patrol (CBP) is inundated with a yearly flow of illegal crossings exceeding 400,000.[5] The volume of narcotics moved northward is measured in the hundreds of tons.[6] The volume of cash and weapons moving south-bound is incalculable, but is estimated at billions in cash and well over 10,000 military-grade weapons per year.[7]

Alarm over this border area is not limited to the TCOs alone.[8] The emerging synergy between the TCOs and terrorist (Jihadist[9]) ideologies currently at war with America is grounds for grave concern.[10] Both organizations would make tremendous gains if they could increase the

safe havens within the southwest border, push Mexico into a failed state,[11] and bring terrorism into the southwestern United States.[12] To those in a stable and secure America this threat may seem farfetched and distant.[13] Many experienced security professionals reading this will be immediately inclined to draw comparisons between the current Mexican Cartels and the Colombian Cartels that wreaked havoc in that country throughout the 1990s. It is encouraging that the Colombian situation has stabilized, but this favorable outcome should not be used as an excuse to dismiss the severity of the current Mexican security situation.

Security theorists have long feared that the differences between criminals and terrorists are rapidly fading to such an extent that the future may only identify "irregular attackers."[14] For example, terrorist organizations such as the Taliban and Revolutionary Armed Forces of Colombia, or FARC, deal in narcotics on a massive scale to fund their movements. Conversely, the Mexican Cartels employ terrorism to insure a permissive operational environment and the survival of their narco-trafficking.

The existence of autonomous regions, i.e. "safe-havens," where TCOs can conduct illegal activity unfettered by the government has become the "center of gravity" in the fight against narco-terrorism. A "safe-haven" constitutes a place where "illicit actors can operate with impunity…and…can organize, train and operate in relative security."[15] They are created when state institutions in the area are ineffective, non-state armed groups are superior in the use of force, and the State has lost control of its borders. To achieve such conditions, insurgents must create their own infrastructure, their own economy, enable favorable populations, and maintain invisibility from security forces.[16]

The Mexican Cartels are achieving these benchmarks by a three-step process.[17] Firstly, they use ultra-violence to undermine the State. This is done along the border by the daily infliction of kidnappings, murders, torture, and mutilations, coupled with bribery and corruption of state security mechanisms.[18] The end result is that the populace has no place to turn, thus the TCOs achieve popular support through capitulation.[19] Those elements of the State that resist the TCOs are subjected to direct murder and violent intimidation of themselves or those they hold dear,

resulting in either their deaths or submission. This further deepens the leadership vacuum which is then filled by the TCOs or those bureaucrats loyal to them. The end result is the creation of a pro-narco governmental structure – the second step in the process. The recurring murder of police chiefs within numerous Mexican cities is evidence that the TCOs have achieved this step.[20] Lastly, these shadow states are geographically created and eventually linked. An example of this achievement is found within the Sinaloa State of Mexico.[21] Within Sinaloa, government agencies cannot enter major (hundred square mile) TCO enclaves. This autonomy is replicated within the slums of Mexico City, and along the southwest border region.

The populace within these areas is controlled not only by violence, but also by a disturbing economic reliance on TCO activities.[22] With the decline of normal economic activities, the narco-economy supplants the marketplace.[23] This economic reliance is coupled with a conditioning that creates a pro-drug culture, culminating in acceptance and identification with the TCOs as the principal, social group. The TCO becomes the community and government, thus achieving complete anonymity among the populace. To the Mexican Cartels, invisibility does not so much mean secrecy as it does creating a so-called "blind-eye" through intimidation and corruption. Freed from outside interference, the TCOs replace the institutions of legitimate government enabling them to pursue unlimited drug trade and enjoy the fruits of their labor. Once this status is achieved, the State is no longer a factor and the battle for the populace is lost.[24] Within Mexico this process has not only begun, but is well along. If achieved to fruition, these TCO safe havens will be of great use to al Qaeda and other Jihadists,[25] providing access to a failed U.S. border, as well as to advanced asymmetrical criminal networks, both in Mexico and the United States.

The relationship between Jihadists and the Mexican Cartels is already established, it possesses the potential to expand rapidly and catastrophically. Other-than-Mexican (OTM) smuggling across the border has exploded. By mid-decade OTMs accounted for roughly one in eight apprehensions.[26] The majority are Central American, but significant percentages are also from the Middle East.[27] Based on money, physical similarities, and mutual supporting relationships,

Jihadists cross the border into the United States unknown to the U.S. security apparatus.[28] (Human smuggling in itself is a valuable criminal enterprise, which has long-been practiced by terrorist organizations as a fund raising activity.[29])

The Jihadist affiliation, coupled with their own mature operating methods places the Mexican Cartels squarely within 3rd generation gang status.[30] Possessing immeasurable cash reserves, advanced military skills,[31] safe havens, and now terrorist connections, a new era of TCO operational capacity is emerging. An example of this is the car bomb, a technique perfected by Jihadists now being used along the border region.[32] U.S. personnel have been subjected to "rocking," a tactic made famous by the Palestinians.[33] Another technique, borrowed from Chechen terrorists, is the intentional wounding of police officers in order to set ambushes upon the security forces attempting their rescue. Such techniques demonstrate a relationship between Jihadists and the TCOs. Trained Mexican terrorists pose a threat as uncountable numbers could easily infiltrate the United States through illegal immigrant networks. Terrorist techniques do not have to be taught directly from other asymmetrical organizations, but can be garnered through message traffic, open sources, or paid mercenary advisors. This lethality is supported with Information Operations campaigns. In the case of La Familiar (The Family), we see the TCOs emerge as a Maoist-type movement attempting to use narco-trafficking to improve the lives of the populace, an empty promise that results only in greater violence and terror.[34] A more sinister synergy emerges with the Cult of Saint Muerto, a pro-narco death cult, based on Catholic ritual and, grotesquely, Satanism. The Cult serves as a stabilizing religious force by using traditional cultural norms to justify the new narco-culture.[35] Barbaric violence and the death cult create a "no fear" synergy that twists TCO behavior beyond the rational.

These socializations and attitudes are coupled with a significant TCO military capability. This capability was garnered when the Los Zetas Cartel entered the drug-trade after deserting, en masse, from the Mexican Special Forces.[36] Their military techniques have been honed by continuous combat experience. They have been maintained by a recruitment and training process that indoctrinates TCO irregulars into an advanced, well organized paramilitary force.[37] Combat action,

including raids, assassinations and kidnappings, utilizing advanced weaponry, battlefield communications, and fluid tactics occurs daily along the border.[38] Greater levels of violence are sought as the Los Zetas reach out to other Latin American special operations forces in an attempt to increase their lethality and power.[39] Military weaponry, advanced tactics, and illicit money serve as force multipliers.[40] Like any asymmetrical organization, the TCOs continue to adapt their methods. Gang alliances fold and shift, operating methods emerge and develop, key leadership is removed and yet, throughout the years the TCOs have flourished.[41] In fact, the TCOs don't even have to smuggle operatives across the border, they are already here.

The linkage between the TCOs and U.S. gangs is circular in nature. Gang personnel and illicit goods flow north and south. TCOs possess sophisticated special operations actors. Such irregulars coming under scrutiny within Mexico can easily escape justice by crossing the porous border. Once inside the United States their leadership and expertise enhance gang capabilities and establish a line of communication back to the Mexican Cartels, in essence closing the loop between 3rd generation TCOs and 1st generation U.S. street gangs.[42] In a disturbing trend, TCOs have recruited active U.S. military personnel for crimes such as murder and smuggling.[43] The participation of U.S. service members offers the TCOs access to increased lethality, advanced techniques, and improved intelligence.

If the TCOs continue unabated a new wave of terror along the southwest border will emerge. The Mexican government possesses little counterterrorism capability. Overwhelmed, under-resourced, corrupt, and ignorant in advanced counterinsurgency techniques, there is little hope that it can conduct a successful counter-narco campaign on its own. Eventually, participatory U.S. assistance will become necessary. The U.S. Army should continue with preparations to provide advisory and intelligence support (to include tactical UAV support), as well as training and logistics packages. Conventional threat assessment is based upon the thought that one's adversary is a rational actor with a rational goal in mind. Evidence of the TCOs counters this belief. Though some may say that attacks upon the United States would be bad for the drug business and therefore America is safe, this belief fails to account for the

emergent narco-terrorist, anti-American synergy. As TCO criminality morphs from drugs to terrorism, and as a new breed of hate is coupled with the Jihadists,[44] the likelihood of cross-border terrorism throughout the southwestern United States becomes a major security concern. Such violence is no longer a faint worry, but is quickly becoming a reality.

# Securing the U.S. Southern Land Border: Enhancing the Interagency Effort

**Special Agent Michael D. Kennedy**
United States Immigration and Customs Enforcement

HISTORICALLY THE BORDER between the United States and Mexico has been a dangerous place. It is no different today. In the 1800's, bandits and criminals used Mexico as a safe haven from U.S. law enforcement officers after committing crimes in the United States. This situation continued into the 20th century, highlighted by General John Pershing's "punitive expedition" into Mexico in pursuit of Pancho Villa in 1916.[1]

The remainder of the 20th century was relatively calm with only sporadic outbreaks of cross-border violence. So far, the 21st century has seen a disturbing trend. The violence in Mexico just south of the U.S. border has escalated dramatically over the past several years and now threatens to expand into the United States. Traditional U.S. border control and law enforcement strategies may not be enough to prevent this violence from spreading north. A new interagency approach may be needed. This paper will explore strategies that could provide a greater unity of effort in the Federal government's approach to border security in order to counter this emerging threat. A basic understanding of the various Federal departments and agencies that have a role in border security is needed before these strategies can be analyzed.

## The Department of Homeland Security

Prior to the tragedy of September 11, 2001, border security was primarily divided between four cabinet departments: the Department of Justice (DOJ) (Immigration and Naturalization Service), the Department of the Treasury (U.S. Customs Service), the Department of Agriculture (USDA) (Animal and Plant Health Inspection Service), and the Department of Transportation (DOT) (the U.S. Coast Guard).[2] The Homeland Security Act of 2002 (Public Law 107-296) consolidated most federal agencies that operate along U.S. borders

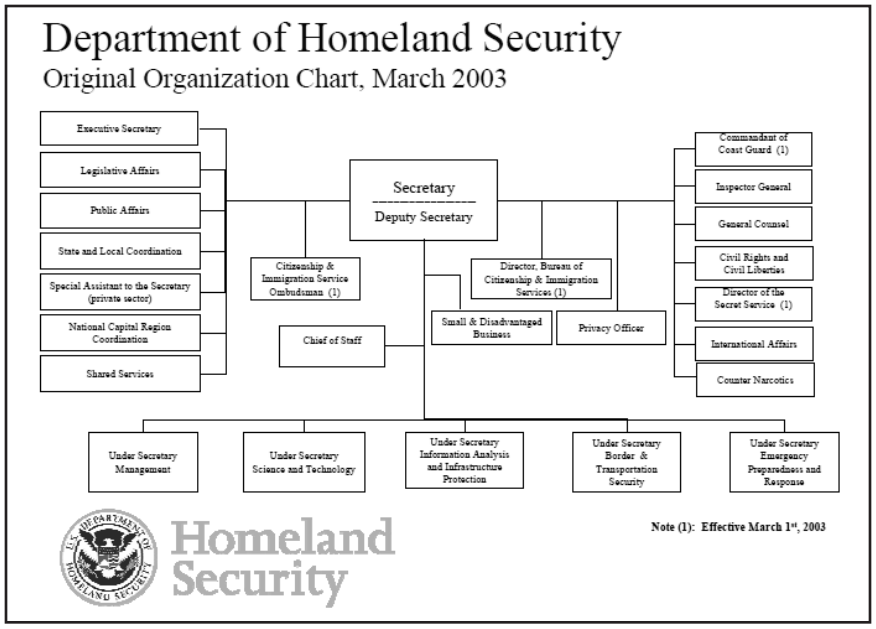



**Figure 1. This chart depicts the original organization of DHS. CBP, ICE and TSA were components of the Under Secretary of Border and Transportation Security (BTS). Some of the operational components are not listed but are under BTS, and some are listed separately on the right side of the chart (U.S. Coast Guard and U.S. Secret Service).**

into the Directorate of Border and Transportation Security (BTS), a subordinate element of the Department of Homeland Security (DHS).[3] The exception was the U.S. Coast Guard which remained a separate organization under DHS. BTS consisted of three main agencies:

1. Customs and Border Protection (CBP), responsible for commercial operations, inspections, and land border patrol functions
2. Immigration and Customs Enforcement (ICE), responsible for customs and immigration investigations, alien detention and removals, air/marine interdiction, and federal protective services
3. Transportation Security Administration (TSA), responsible for protecting the nation's air, land, and rail transportation systems from all forms of attack[4]

In 2005, DHS Secretary Chertoff, with Congressional approval, eliminated the BTS Directorate as part of the DHS Second Stage Review, placing the main border control agencies (CBP, ICE, and

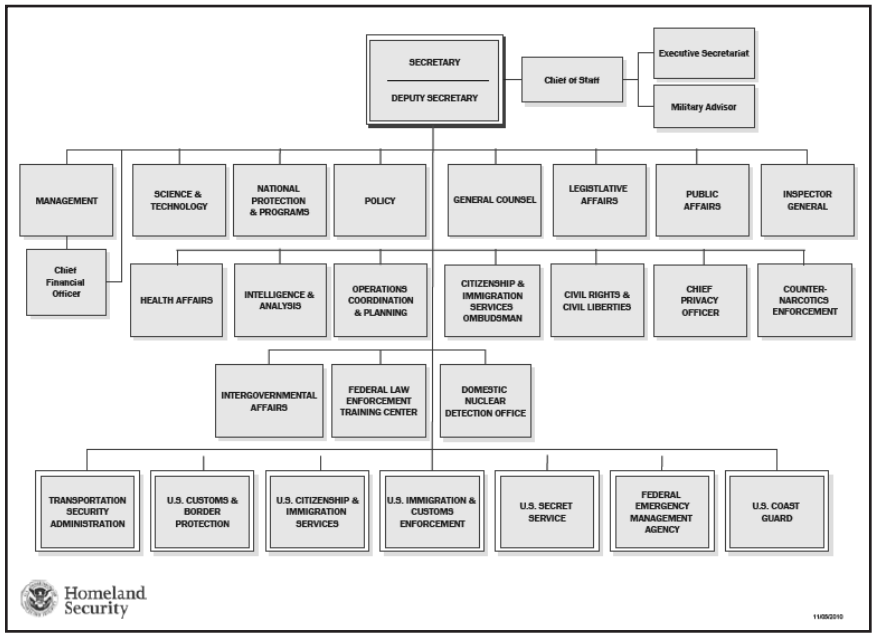



**Figure 2. This is the current organizational chart for DHS. Note the operational components are functionally aligned, but protecting the border requires a multifunction effort.**

TSA) directly under the Secretary and Deputy Secretary of DHS. The Federal Air Marshal Service (FAMS) was moved back to TSA from ICE (FAMS was placed under ICE for an interim period between 2003 and 2005), and in addition, the Air and Marine Office was transferred to CBP from ICE.[5] No reason was given for this change and it added three additional direct report agencies to the span of control of the Secretary of DHS. DHS currently has 25 entities that directly report to the Secretary/Deputy Secretary. This creates a span of control problem. DHS should analyze its current structure and consider some logical subdivisions such as undersecretaries for operations, management, and technology. This structure would be a hybrid between the original DHS organization (Figure 1) and its current form (Figure 2).

Each border security component of DHS has unique capabilities and specialties. They are also organized differently for their unique missions and have cultural differences which can lead to friction when they interact with each other. A look at each component's organization is needed to fully appreciate this point.

## U.S. Customs and Border Protection (CBP)

CBP combined portions of several different border law enforcement agencies under one new agency. CBP is a large agency with over 58,000 personnel.[8] It has three major border enforcement entities: Field Operations, Border Patrol, and Air/Marine Operations (AMO). Field Operations consists of the inspectors from the former Immigration and Naturalization Service (INS), U.S. Customs Service (USCS) and USDA. Field Operations is responsible for conducting immigration, customs, and agricultural inspections of persons and merchandise coming into the United States through official ports of entry.[9] Primary inspectors are cross-trained and do the initial screening for violations of law. Secondary inspectors are more specialized and conduct more in depth inspections into possible violations of immigration, customs or agricultural law.[10]

The U.S. Border Patrol (USBP) is another component of CBP and enforces primarily immigration law between the ports of entry and transportation facilities with a nexus to the border (i.e. airports, bus,

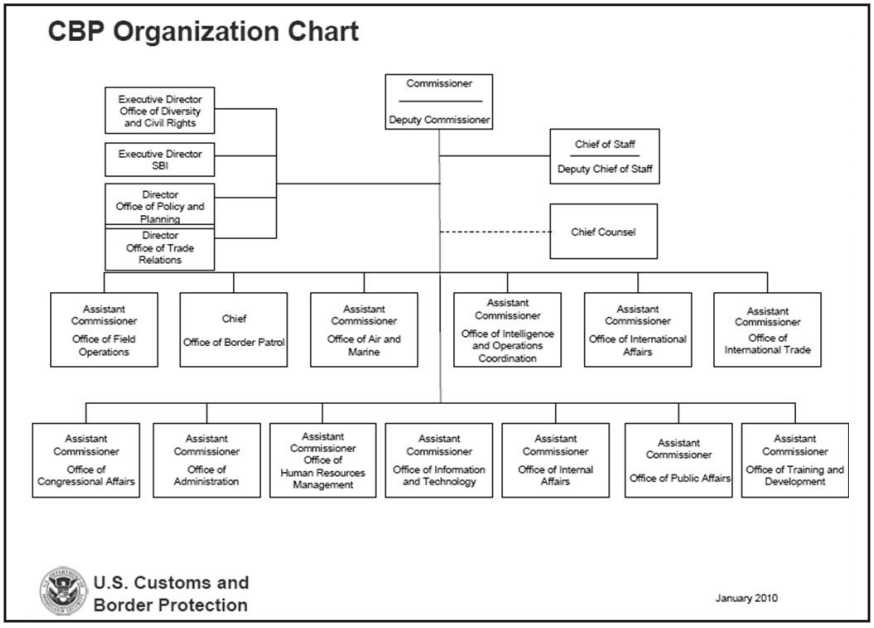



**Figure 3. This is the current CBP Organizational Chart. Note Border Patrol Chief (traditional title) is equivalent to the other Assistant Commissioners.**[11]

and train stations). Unlike field operations, USBP was transferred from the DOJ mostly intact. In contrast to field operations, USBP kept their traditional green uniforms and paramilitary type structure. Subsequent to the merger, USBP agents have been cross-trained to detect and enforce customs violations in addition to their traditional alien apprehension role.

AMO is the third border enforcement component of CBP. When DHS was initially created, AMO resided in ICE. The primary mission of AMO is interdiction and patrol oriented so it was transferred from ICE to CBP shortly after DHS was formed. In addition to its patrol and interdiction mission, AMO provides air support to ICE in the form of air surveillance, tracking, and transportation of tactical and response teams. Currently, CBP operates over 290 aircraft of 26 types and 251 vessels.[12]

### U.S. Immigration and Customs Enforcement

ICE is the largest and principal investigative arm for DHS with approximately 20,000 personnel. ICE's mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks.[13] ICE merged the investigative functions of the former INS and Customs Service, INS detention and removal functions, some intelligence functions from both INS and USCS, and the General Services Administration's Federal Protective Service (FPS). ICE investigates customs and immigration violations along the border as well as in the interior of the United States. ICE's mandate includes investigating national security threats such as proliferation of weapons of mass destruction and potential terrorists, identifying criminal aliens for removal, investigating immigration-related document and benefit fraud, investigating work-site immigration violations, alien and contraband (including narcotics) smuggling, customs commercial fraud, and dual-use and munitions export violations.[14]

### U.S. Coast Guard

The Coast Guard was incorporated into DHS by the Homeland Security Act of 2002 as a standalone agency. The Coast Guard is the

nation's principal maritime law enforcement authority and the lead federal agency for the maritime component of homeland security. Some of the law enforcement related missions of the Coast Guard include, evaluating, boarding and inspecting commercial ships approaching U.S. waters, countering terrorist threats in U.S. ports, protecting U.S. Navy and other high threat ships in U.S. ports, and narcotics interdiction. The Coast Guard has almost 50,000 military and civilian personnel.[15] The Coast Guard gains its authority from several U.S. statutes. Title 14, United States Code (USC), Section 89, gives the Coast Guard its primary law enforcement powers. In addition, under Title 19, USC, all commissioned and petty officers of the Coast Guard are also Customs Officers. This authority gives the Coast Guard the same border search authority as CBP and ICE.

**Federal Air Marshal Service**

After the attacks of 9/11, the FAA had less than 100 FAMS and requested other federal agencies augment the program. Special agents from many U.S. law enforcement agencies were attached to the FAA until the newly formed TSA was able to hire and train an adequate force. In 2002, TSA was transferred from DOT to DHS and the current FAMS program was established. The FAMS are the primary in-flight law enforcement arm of TSA. In addition to these flying duties, FAMS are used to assist other elements of TSA in their maritime and surface transportation security role as they are one of the few armed elements of TSA. Although not a border security agency per se, TSA's implementation of the Transportation Worker Identification Credential (TWIC) and its maritime and surface transportation security mission bring TSA into the border security arena.[16]

**Other U.S. Government Entities**

Even though DHS is the primary U.S. Government (USG) department responsible for border security, many other USG agencies have important supporting roles. The Department of State (DOS) is responsible for the overseas issuance of visas to foreign visitors to the United States (ICE has visa security officers posted in embassies overseas to assist DOS consular officers in this function). The three DOJ law enforcement

agencies (Federal Bureau of Investigation [FBI], Drug Enforcement Administration [DEA], and Alcohol, Tobacco, Firearms and Explosives [ATF]) all coordinate with CBP and ICE when their investigations involve the border area. Other entities include, the Department of Health and Human Services through the Food and Drug Administration and Centers for Disease Control, the FAA under the DOT, the Central Intelligence Agency (CIA) and various Department of Defense (DOD) activities. All of the above to include other state and local agencies make important contributions to border security.[17] However, the largest federal contribution outside of DHS is from the DOD.

**Department of Defense**

The Department of Defense's primary player in border security is United States Northern Command (USNORTHCOM) which was established in 2002. "USNORTHCOM conducts homeland defense, civil support and security cooperation to defend and secure the United States and its interests."[18] "In providing civil support, USNORTHCOM generally operates through established joint task forces (JTF)."[19] The command provides a full range of domestic support when tasked by DOD but are restricted by the Posse Comitatus Act.[20]

Joint Task Force-North (JTF-North) is the primary USNORTHCOM entity for law enforcement support. Originally established in 1989 as Joint Task Force Six to support the "War on Drugs," it was renamed JTF-North in 2004 and given an expanded mission. JTF-North's mission is to support federal law enforcement agencies in the interdiction of suspected transnational threats along the approaches to the continental United States. These threats involve international terrorism, narco-trafficking, alien smuggling, and weapons of mass destruction.[21]

Another DOD resource are the ten Defense Coordinating Officers (DCOs) assigned to each Federal Emergency Management Agency (FEMA) region. If requested and approved, the DCO serves as DOD's single point of contact at the Joint Field Office (JFO). With few exceptions, requests for Defense Support of Civil Authorities originating at the JFO are coordinated with and processed through the DCO. The DCO has a Defense Coordinating Element consisting of a staff and military liaison officers to facilitate coordination and support to

activated Emergency Support Functions (ESFs). Specific responsibilities of the DCO (subject to modification based on the situation) include processing requirements for military support, forwarding mission assignments to the appropriate military organizations through DOD-designated channels, and assigning military liaisons, as appropriate, to activated ESFs.[22]

Using the military in a law enforcement support role is not a new concept. The Posse Comitatus Act restricts the military from a direct law enforcement role unless expressly authorized by the Constitution or Congress. Title 10, USC, Section 375 further directs the Secretary of Defense to promulgate regulations forbidding the direct participation of U.S. military members (minus Coast Guard) in a search, seizure, arrest or other similar activity during support activities to civilian law enforcement agencies.[23]

The Posse Comitatus Act does not apply if Congress specifically authorizes the use of the military to execute domestic law enforcement. In addition, the courts have not answered the Constitutional question of presidential authority in the cases of sudden emergency and protection of federal property. Congress has enacted several laws that authorize the military to conduct specific law enforcement support activities. In summary, reconnaissance and detection activities, loan of equipment, and movement of law enforcement personnel by the U.S. military have been specifically authorized by Congress. In addition, two broad exceptions to the tenants of the Posse Comitatus Act have been granted by Congress. In accordance with Title 14, USC, the U.S. Coast Guard is granted specific law enforcement authorities while operating under DHS control. The National Guard is also able to have a more direct law enforcement role when they are operating under the authority of a State Governor under Title 32, USC. [24]

## The Challenge of Border Security

Border security presents unique and significant challenges for the United States. The National Strategy for Homeland Security states, "Our first and most solemn obligation is to protect the American people."[25] The next sentence advocates that this strategy be implemented to sustain "our way of life as a free, prosperous, and welcoming America."[26]

The hard balance is how to protect the Nation's borders in a way that embraces individual freedom as well as being a welcoming nation to legal immigrants. We must also balance governmental authority which is grounded in our Constitutional framework. State, local and tribal governments provide the first response capability in law enforcement, fire, public health and emergency medical services.[27] The Federal government provides military, disaster response, and federal law enforcement capabilities to protect the Nation as a whole. Many of these capabilities overlap. The question "who is in charge?" is not always easy to answer due to the multiple jurisdictions of our three levels of government. The Federal government was criticized by state leaders for a slow disaster relief response to Hurricane Katrina when Federal law requires the state to request the assistance, which was slow in coming from the State of Louisiana. Contrast that with the Federal government's criticism of Arizona's immigration law, which is seen by the Federal government as a state's encroachment into a Federal responsibility.[28]

The current National Strategy for Homeland Security addresses three areas:

1. The prevention and disruption of terrorist attacks
2. Protection of the American people, critical infrastructure and key resources
3. Respond to and recover from incidents.[29]

This strategy does not specifically address trans-national crime, only terrorist acts. The current "drug war" in Mexico may change that. Several estimates put the drug related death toll in Mexico between 18,000 and 23,000 in the past four years.[30] In comparison, these figures greatly outnumber the total deaths in Afghanistan. During the past three years, almost 7,000 Afghans (including soldiers, insurgents, and civilians) and approximately 550 coalition military were killed.[31]

So far, the violence has not spread significantly into the United States. In spite of political rhetoric, U.S. border cities such as El Paso, Nogales, Yuma, and Tucson have actually seen a decrease in violent crime over the past decade.[32] The question that comes to mind, however, is what

can the USG do to keep the drug violence in Mexico from spreading into the United States?

**Agency Organization and Task Forces**

One of the issues that affect the response options is the organization of U.S. border and law enforcement agencies and how they interact with one another. Within CBP there are 20 Field Operations Offices and 20 Border Patrol Sector Offices. Due to the differences in their missions, the areas of responsibility of these offices do not coincide with one another even they are part of the same agency. To complicate this further, there are 26 ICE Homeland Security Investigations Field Offices whose special agents conduct investigations on their own and in support of CBP. The effect of this organizational structure is that in many areas, the senior field managers of three agencies of DHS have multiple counterparts in which to coordinate and de-conflict activities.

Within the DOJ, there are three agencies that have major roles in border security (FBI, DEA, and ATF). Their situation with areas of responsibility is no better. The FBI has 56 Field Divisions, DEA has 21, and ATF has 25. As disjointed as this all appears, each agency is organized to best address their specific jurisdictional crime threat with the resources available.

The mechanism that has been used for many years to address multi-jurisdictional crime is task forces. The Federal government has two task force models that have been used to address large-scale drug related crime problems and one that addresses border crime. The oldest is the Organized Crime Drug Enforcement Task Force (OCDETF) that was established in 1982,

> *…to combine and leverage Federal law enforcement assets into a comprehensive attack against significant drug trafficking problems. OCDETF is comprised of special agents from Customs, DEA, FBI, INS, ATF, IRS, the Marshals Service, and the Coast Guard and implemented in nine regions throughout the United States…its innovative approach to solving the problems facing law enforcement serves as the model for cooperative investigative efforts.*[33]

OCDETF under the authority of the Attorney General was originally managed by the United States Attorneys. It is now managed by DEA and "…combines the resources and expertise of its member federal agencies which include: the Drug Enforcement Administration, the Federal Bureau of Investigation, the Bureau of Immigration and Customs Enforcement, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Marshals Service, the Internal Revenue Service, and the U.S. Coast Guard – in cooperation with the Department of Justice Criminal Division, the Tax Division, and the 93 U.S. Attorney's Offices, as well as with state and local law enforcement."[34] "The principal mission of the OCDETF program is to identify, disrupt, and dismantle the most serious drug trafficking and money laundering organizations and those primarily responsible for the nation's drug supply."[35] OCDETF assisted the development of the Attorney General's Consolidated Priority Target List, which is a list of international drug traffickers and money launderers who exert large-scale "command and control" over major drug trafficking organizations (DTOs) at the strategic level.[36] OCDETF "Strike Forces" have been extremely successful in dismantling major DTO's and seizing millions of dollars in illicit assets and drugs over the last 28 years.

The High Intensity Drug Trafficking Task Force (HIDTA) program was authorized by the Anti-Drug Abuse Act of 1988 and the Office of National Drug Control Policy (ONDCP) Reauthorization Act of 1998. This legislation authorized the ONDCP to designate areas of the United States as HIDTA areas. The HIDTA program could then provide additional federal resources to those areas to eliminate or reduce drug trafficking.

HIDTA as opposed to OCDETF is geographic in nature. The first five HIDTA areas were designated in 1990 (including the Southwest Border HIDTA that covers California, Arizona, New Mexico and Texas). Currently there are a total of 28 HIDTA's. Each HIDTA has an Executive Board composed of an equal number of Federal and non-Federal law enforcement leaders. This design was created to ensure the needs of the state, local and tribal law enforcement agencies were addressed. The key priorities of the program are: assess regional drug threats; design strategies to focus efforts that combat drug trafficking; develop and

fund initiatives to implement the strategies; facilitate coordination between federal, state, and local efforts; to improve the effectiveness and efficiency of drug control efforts to reduce or eliminate the harmful impact of drug trafficking.[37] HIDTA funds 670 initiatives throughout the United States. Most of these are local and regionally focused, to include five state Native American projects. There are three initiatives that provide support to other initiatives throughout the Nation. They are the Domestic Marijuana Eradication and Investigation Project, the National Methamphetamine and Pharmaceuticals Initiative and the Domestic Highway Enforcement Program.[38]

The most recent large-scale federal law enforcement task force is the Border Enforcement Security Task Force (BEST). Created in 2006, BEST task forces have expanded from a single task force to 12 of which eight are along the southwest border. Each of these 12 BEST task forces was formed to counter a variety of border threats along the U.S./Canada (Northern) and U.S./Mexico (Southern) border areas. The current situation along the border between the United States and Mexico was a large factor in the initial formation of BEST. These task forces are different than OCDETF or HIDTA which focus primarily on drug trafficking/smuggling. While BEST task forces also address drug crime, they are much broader in scope to address other criminal activity in the border region. For example, BEST task forces target inbound drugs, other contraband, and criminal immigrants from Mexico but also target weapons, ammunition, explosives and technology leaving the United States that assist the DTO's operating in Mexico. BEST task forces include the participation of CBP, U.S. Coast Guard, DHS Office of Intelligence and Analysis, DEA, FBI, ATF, multiple state, local and tribal agencies, as well as several Mexican agencies. The efforts of BEST task forces have resulted in the seizure of over 8,000 pounds cocaine, 173,000 pounds of marijuana, 1,000 weapons and explosives and $25 million in U.S. currency.[39]

**Current Southwest Border Strategy**

The current strategy for dealing with the myriad of issues along the Southwest border is a combination of additional resources and the task force approach. DHS Secretary Napolitano outlined this strategy in

recent Congressional testimony. She stated that DHS will strengthen its "…efforts at the border through additional manpower, equipment, and technology; prevent the southbound flow of weapons and cash into Mexico; and increase support and collaboration with our Mexican counterparts."[40] She additionally stated that "…we are also deepening and expanding our engagement with federal partners such as the Departments of State, Justice and Defense, as well as state, local, and tribal governments and border communities…,"[41] OCDETF, HIDTA, and BEST task forces have already been addressed above. In addition to these task forces, CBP has developed and implemented Border Violence Protocols to better coordinate activities with local U.S. agencies as well as Mexican government officials. DHS has allocated $59 million under Operation Stonegarden to enhance state, local, and tribal law enforcement activities along the border. This funding is used for additional law enforcement personnel, overtime expenses and deployment travel.[42]

Secretary Napolitano also addressed the importance of international cooperation by stating, "The cornerstone of U.S.-Mexico security cooperation is the Mérida Initiative, led by U.S. State Department."[43] DHS uses Mérida as the basis for regional security partnerships with Mexican authorities. ICE's Border Liaison Officer Program provides streamlined information and intelligence sharing mechanism. The ICE Attaché office in Mexico City has established vetted Special Investigative Units of Mexican officers who work with ICE special agents in Mexico to investigate and prosecute border crimes. The ICE attaché office has also assigned native Spanish speaking special agents to small posts of duty at key border cities inside Mexico to better coordinate with Mexican law enforcement officials. Since 2005, CBP has also worked closely with Mexican officials on Operation Against Smugglers Initiative on Safety and Security, a bilateral alien smuggler prosecution program that enables both governments to share information in order to prosecute smugglers for crimes committed in the border region.[44]

A large number of weapons linked to drug violence and recovered in Mexico are smuggled illegally from the United States into Mexico. Stopping this outbound flow of weapons is a DHS priority. ICE established Operation Armas Cruzadas, a partnership with the

government of Mexico, to fight outbound arms smuggling. Operation Armas Cruzadas uses an intelligence-driven, systematic approach to arms smuggling investigations. ICE created a vetted Arms Trafficking Group of Mexican law enforcement officers to better share information and intelligence between the two countries. Operation Armas Cruzadas has resulted in 112 criminal arrests and seizure of over 116,000 rounds of ammunition, 1,417 weapons, and over $3.3 million in monetary instruments.[45] In addition to Operation Armas Cruzadas, several other arms smuggling enforcement initiatives are ongoing. ICE and CBP have partnered with ATF in the eTrace initiative that aids Mexican officials in the forensic tracking of weapons used in drug cartel violence. CBP partners with DEA and HIDTA centers to increase the deployment of License Plate Readers, to gather intelligence on trafficking organizations. CBP, ICE, DEA, and ATF have joined forces to develop the Southwest Border Trafficking Initiative to identify and disrupt weapons and ammunition smuggling.[46]

In addition to the inter-agency and task force efforts, CBP is now screening 100 percent of southbound traffic at the eight southwest border rail crossings. CBP is using existing non-intrusive inspection equipment to screen all outbound rail cars for anomalies that may indicate arms smuggling. Previously, this equipment was dedicated to inbound inspections. Mobile x-ray equipment is also being directed against outbound traffic at ports of entry as well and inbound traffic. CBP is using Mobile Response Teams from Field Operations and Border Patrol agents to augment current staffs at ports of entry along the southwest border.[47]

DHS is also combating the illegal movement of currency across the southwest border. Operation Firewall, led by ICE, is addressing the bulk cash smuggling threat. ICE and CBP have conducted numerous operations under Operation Firewall with their Mexican counterparts. ICE has recently established a Trade Transparency Unit with Mexico to identify cross-border trade anomalies, which often indicate some kind of trade-based money laundering. This is accomplished by the analysis of import and export data and financial information. ICE's efforts have led to more the $50 million is cash in FY 2008.[48]

This international cooperation and collaboration has resulted in significant success. According to ONDCP statistics, in fiscal years (FY) 2009 and 2010, CBP seized more than $104 million in southbound illegal currency – an increase of more than $28 million over FY 2007-2008. Also in FY 2009/2010, CBP and ICE seized more than $282 million in illegal currency, more than 7 million pounds of illegal drugs and more than 6,800 weapons along the Southwest border. These seizures represent increases of more than $73 million in currency, more than 1 million pounds in drugs, and more than 1,500 weapons over FY 2009/2010. The increase in seizures can be linked to an increase in cooperation and information sharing between U.S. Federal, state, local and tribal law enforcement agencies and Mexican law enforcement authorities.[49] The Mérida Initiative allocated $700 million to enhance Mexican law enforcement and judicial capacity in FY 2009. These funds will help improve the government of Mexico's efforts in crime prevention, rule of law, and law enforcement. Equipment such as five helicopters, a maritime patrol aircraft, and non-intrusive inspection technology will be purchased with these funds. Training and other support will also be provided to help Mexico implement its new legal system and establish an effective witness and victim protection program, crucial to successful prosecution of drug offenders.[50] These efforts are showing signs of success. "On November 18, 2010, Antonio Cardenas Guillen, the leader of Mexico's Gulf Drug Cartel was killed in a gun battle with Mexican marines."[51] It is too early to tell what effect Guillen's death may have on inter-cartel violence.

**Border Security Options**

Even a brief study of international drug cartels, money laundering, narco-terrorism, and border violence in Mexico will reveal that border security is a wicked problem without a simple solution. The term wicked problem is used for two reasons. First as a definition of a complex problem that has no definitive formulation, without a well-described set of potential solutions, with a set of interlocking issues and constraints that change over time, embedded in a dynamic social context.[52] The second reason is the violence in Mexico along the border with the United States is so extreme (as many as 23,000 deaths in the past four years), that it rivals that of the most violent terrorist

organizations. Assassinations of government officials and journalists, running gun battles without concern for innocent civilians, bombings, torture and beheadings by the drug cartels are truly wicked from a more traditional definition of the word evil.

Several U.S. administrations have struggled with border security issues and challenges. The strategy so far has been to allocate more resources and create more programs and task forces. These efforts are portrayed as comprehensive in nature and do address many different facets of a complex problem. However, comprehensive does not necessarily equate to coordination. A more unified approach to border security should be considered. There have been several concepts proposed to provide more unity of effort in the Federal government's approach to border security.

One of the original options after 9/11 when DHS was formed was to bring together the FBI, DEA, ATF, and Customs under DHS. This would have brought most Federal law enforcement and investigative personnel under one Secretary. This option would have also separated the entities responsible for the investigation of Federal crimes from the prosecution function, which would remain under the Attorney General and DOJ. The Secretary of DHS would be able to re-structure the Department as needed to address border security as well as any other organized criminal or terrorist threat to the U.S. There were many functional advantages to this option. This option would have matched approximately 25,000 criminal investigators with a roughly equivalent number of uniformed law enforcement officers (Border Patrol and Customs Field Operations). This option would have also merged the air assets of CBP, DEA and FBI into a more capable interdiction and investigative support arm. This option would also have created strong unity of command and effort as the Secretary of DHS would have command and control over all of the enforcement and investigative agencies involved in border security.

Politics played a large role in why this option was not implemented. The Attorney General did not want to lose his investigative agencies (FBI and DEA). The FBI and DEA also have strong support in Congress. The primary Congressional authorizing committees for DOJ are the powerful House and Senate Committees on the Judiciary. These committees provide advocacy as well as oversight for DOJ. Another

issue with this option was the inherent mistrust of large, powerful government departments by the American people and the fear of the abuse of power.

There has been a move within DHS to subdivide and consolidate many of its functional agencies under a regional concept mimicking FEMA. Regional Commissioners would exercise command and control over a multi-functional sub-department. This organizational structure was used by INS and USCS for many years. In INS and Customs, the Regional Commissioner had Assistant Regional Commissioners (ARCs) who managed regional functional elements. For example, Customs had ARCs for Inspections, import specialists, and investigations. The advantage of this system is that it gives the regional executives a robust capability to deal with regional problems. It also established a clear chain of command for unity of effort.

As positive as this system sounds in theory, it was not successful in the two historic instances that specifically relate to border security. The regional system employed by INS led to Congress eliminating it as an agency during the creation of DHS in the original Homeland Security Act. The U.S. Customs Service converted from a regional system to a functional system in the early 1990's with positive results. The basic problem that arose out of the INS and Customs regional systems was the unintended creation of regional fiefdoms. The INS and Customs Regional Commissioners became very powerful and each ran their regions differently. This was not totally negative as they had the flexibility to address regional problems quickly.

However, problems arose when it came to the allocation resources and consistent procedures nationally. The regional commissioners lobbied against each other and headquarters for personnel and financial resources. Strong regional commissioners had more than enough resources and resisted giving them up to weaker ones who struggled to get adequate resources to address their threats. Another problem that arose was an inconsistency in procedures. For example, each region had different procedures on how to conduct immigration and customs inspections. Personnel policies also differed. Employees were moved to different job series for either promotion or for disciplinary reasons. These employees were often not trained or qualified to perform in these

new job series. These personnel practices led to a dilution of job skills and lack of professionalism.

## A Unity of Effort Approach

"Homeland Security Presidential Directive-5 (HSPD-5), called for a single, comprehensive system to enhance the ability of the United States to manage domestic incidents."[53] The National Response Framework established response structures based on the National Incident Management System (NIMS).[54] If one considers the border security situation along the southwest border as a "domestic incident," albeit more long term than most events traditionally labeled as domestic incidents such as hurricanes, flooding, and earthquakes, then this approach makes sense. Three concepts of NIMS are the Incident Command System (ICS), Multiagency Coordination System (MACS), and Unified Command. ICS was developed by the Federal, state and local wild land fire agencies during the 1970s in order to have a common base of key principles. ICS normally consists of the functional areas of command, operations, planning, logistics, and finance/administration and sometimes intelligence/investigations.[55] The MACS system is used to coordinate activities above the field level by numerous agencies and to prioritize resources. Some examples of the MACS concept are the DHS National Operations Center, the FBI Strategic Information and Operations Center, the National Counterterrorism Center, and numerous intelligence fusion centers. Unified Command is a key element in multijurisdictional or multiagency incident management. Unified Command is a team effort that brings agencies with different authorities and functional responsibilities to jointly provide management direction through the use of a single Incident Action Plan. The effort is unified while each participating agency maintains its own statutory authority, responsibility, and accountability.[56] The result would closely resemble a coalition military organization, where each military is under its own national command authority while working together for a common purpose. Unified Command could be used to effectively manage consolidated task forces on the southwest border.

DHS and DOJ are the two primary departments that are responsible for border security and the enforcement of Federal criminal statutes.

DOD is a vital part of the overall Federal effort as they provide critical support to the civilian law enforcement agencies under DHS and DOJ. The key concepts of NIMS could be brought into a new strategy that consolidates the numerous border task forces (OCDETF, HIDTA, and BEST) under two regional Border Interagency Operations Centers (BIOC). These centers would be located in the existing DOJ led El Paso Intelligence Center[57] in El Paso, Texas and the DHS-led Intelligence and Operations Coordination Center in Tucson, Arizona. The Tucson BIOC would consist of California and Arizona and the El Paso BIOC would consist of New Mexico and Texas. The El Paso BIOC would continue to be led by a DOJ senior executive with a DHS deputy and the Tucson BIOC would be led by a DHS senior executive with a DOJ deputy. Both BIOC's would have "joint staffs" consisting of personnel from all of the Federal agencies involved as well as state, local, and tribal officers. USNORTHCOM, through JTF-North would continue to coordinate DOD support to both BIOC's.

The advantage of this strategy is that it does not alter the existing structure of any department or agency of the Federal government. It does leverage the strengths of the various Federal, state, local, and tribal

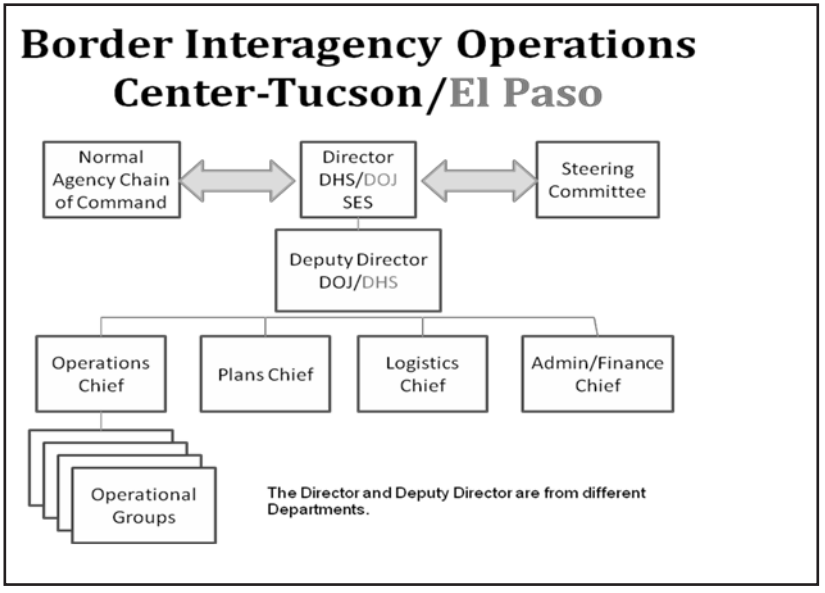



**Figure 4. Notional chart of the Border Interagency Operations Centers (BIOC's) based on the ICS model. El Paso is in gray to denote director's position from DOJ.**

law enforcement agencies into a coordinated and united effort using existing principles. The geographic areas are broad enough to contain significant resources and limited enough to be able to focus these resources. This strategy would require minimal additional financial resources as the appropriated funds to HIDTA, OCDETF, and BEST would continue to be used. Congress would need to be consulted to implement this change as the appropriations committees would need to approve some of the changes in structure. A disadvantage of any new strategy is that it creates a period of disruption and possible paralyses as new procedures are put into place. However, it consolidates significant resources and reduces the duplication of effort that currently exists.

This strategy has many advantages but it would face some significant hurdles. The current HIDTA, OCDETF and BEST task forces would be transitioned to the new BIOC structure. They by default become the bill payers. This includes much more than just funding. HIDTA's have staff paid normally through a state or local agency. OCDETF is based more on reimbursement but there are OCDETF paid positions in some Federal agencies and in some U.S. Attorney's offices (USAOs). There will be resistance to these personnel changes as well as legislative remedies that would need to be completed to ensure the funding streams from appropriated funds as well as from the Federal forfeiture funds are not interrupted. OCDETF and HIDTA are long-standing Federal programs with political advocates. The benefits of converting the southwest OCDETF and HIDTA's to BIOC's would need to be explained in a clear and convincing manner to the stakeholders. These stakeholders include CBP, ICE, FBI, DEA, USAOs, state, local and tribal law enforcement agencies as well as several Congressional committees. A key point to Congress and the Federal agencies is that the HIDTA and OCDETF programs themselves are not being eliminated as OCDETF and HIDTA task forces in other geographical areas would not be affected by the creation of the BIOCs.

There are other actions that can take place to ensure the BIOC's are successful. A steering committee could be formed with representatives from the various U.S. Attorneys, state, local and tribal law enforcement executives in each BIOC area. These steering committees would give the BIOCs strategic guidance and be a forum to resolve issues.

The concept of some kind of steering or oversight committee is common to HIDTA and other current task forces. There should also be an international provision to allow input by vetted Mexican law enforcement authorities into the overall strategy. The ultimate success or failure of any current or new strategy is largely based on the buy-in and support of the stakeholders.

On February 7, 2011, CBP announced the creation of the Arizona Joint Field Command (JFC). The JFC is described as "an organizational realignment to integrate CBP's border security, commercial enforcement, and trade facilitation missions to more effectively meet the unique challenges faced in the Arizona area of operations."[58] A Chief Patrol Officer was appointed as the commander of the Arizona JFC. The JFC consists of U.S. Border Patrol's Tucson and Yuma Sectors, the Office of Field Operation's Tucson Field Office, and the Office of Air and Marine's Yuma and Tucson Air Branches.[59] This new structure may be an indication of DHS' intent to move to a more joint operating environment. Arizona has been the test bed for other imaginative efforts to counter border threats. The original BEST and the Southwest Border Initiative both began as pilot programs in Arizona. Even though the Arizona JFC currently only affects CBP, other agencies have to wonder if this will be the path that DHS will take as a model. One striking element of the announcement was that the JFC was not characterized as a pilot or temporary organization.

The BIOC strategy could be very successful in providing a unity of effort in the Federal government's response to the violence along the border between the United States and Mexico. It will need broad support and commitment by not only the Federal agencies involved but state, local, tribal and Mexican law enforcement agencies. A peaceful, secure border promotes legal immigration, trade and other economic efforts and is in the best interests of citizens of the United States and Mexico.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# U.S. – Mexico Security Cooperation: The Time To Act Is Now

**Colonel Vance F. Stewart III**
United States Army

SENSATIONAL HEADLINES GREET NEWSPAPER and Internet readers daily on both sides of the U.S.-Mexican border announcing the latest crimes committed by the self-styled drug cartels: murder, kidnapping, arson and other forms of intimidation calculated to create and maintain their freedom of activity and shipping of illegal drugs to the United States. The Drug Trafficking Organizations (DTOs) power and control have paralyzed the populace and local governments within the northern Mexican states and to a lesser degree, the country as a whole, disrupting everyday life. If left unchecked, the DTOs threaten the stability of the Mexican federal government.

The emboldened increase and severity of DTO violence within Mexico has created the impetus for the United States and Mexican governments to set aside traditional views and mistrust to work in partnership – making both countries safer and improving the quality of life of their citizens. In 2006, Mexican President Felipe Calderón made weakening the DTOs one of his top priorities and, beginning with U.S. President George W. Bush, created a positive and reciprocal atmosphere towards improving U.S.-Mexican relations.[1] President Barack Obama has seamlessly embraced these efforts and has also made it a priority of his administration.

While inroads have been made over the past three years, this cooperation is at a crossroads. Both countries will enter their respective presidential election cycles in 2011. While President Calderón is unable to run for reelection, he will devote significant time and effort to ensure his political party, the National Action Party (PAN), will continue in power. In all likelihood, President Obama will run for reelection. This crucial juncture is the optimal moment to create irreversible momentum and enact, emplace, and execute a whole-of-government approach to

suppress both the demand and supply of illegal drugs in the U.S. and Mexico in order to defeat the DTOs. This paper will examine why the DTOs threaten U.S. security; why U.S.–Mexico relations have historically been strained; the initial Mérida Initiative; and how the revised Mérida Initiative goals provide a roadmap to successfully solve this complex situation.

**Importance of U.S. – Mexico Security**

The power and influence of DTOs operating within Mexico has reached a crescendo – threatening not only the people and government of Mexico – but also the security and safety of the American public primarily in Arizona, New Mexico, and Texas. The terror, anguish, and violence created is not contained within rival DTOs. In only one recent incident in the northern Mexican border town of Nuevo Laredo it was reported in the U.S. press:

> *[M]exican soldiers clashed here with drug cartel gangsters in running gun battles that lasted five hours. The outlaws hijacked vehicles, including a bus, for use as barricades and battering rams. Terrified residents scrambled for safety. At least a dozen people were killed, including bystanders. Children were wounded in the crossfire.*[2]

Shannon O'Neil, a Latin American scholar at the U.S. Council on Foreign Relations, attributes this crisis to three conditions. First, the scale of illegal drug activity has increased. While Mexico has long been an operating base of illegal activity into the United States, the sheer volume of illegal drugs crossing U.S. borders in terms of quantity and dollar value is increasing. The U.S. National Drug Threat Assessment 2010 report estimates that heroin production in Mexico jumped from 17 metric tons in 2007 to 38 metric tons in 2008.[3] In order to guarantee freedom of action and movement, intra-DTO violence and crime in and around the border towns of Tijuana, Cuidad Juarez, and Nuevo Laredo is spreading over into the United States and, in increasing frequency, affecting U.S. citizens.

Second, the success of Plan Colombia[4] and other U.S. efforts in the Caribbean has shifted the illegal drug trade center of gravity to

Mexico. Plan Colombia was launched in 1999 as a joint effort between Colombia and the United States to fight drug trafficking, promote economic growth, encourage social development, and strengthen democratic institutions.[5] Proponents tout the success of disarming the leftist Revolutionary Armed Forces of Colombia (FARC) rebels, restoring government control over the entire country, and dismantling the illegal drug manufacturing and transport.[6]

However, the unintended consequence of these efforts is the Mexican DTOs filled the vacuum created by the reduced influence of the Colombian cartels. They exerted their influence over control of the entire illegal drug market; no longer only serving as a transit zone but now managing the entire supply chain from manufacturing to sales.

Finally, the rise of the PAN party with the election of Vicente Fox in 2000 and affirmed with Felipe Calderón's election in 2006 caused the demise of the Institutional Revolutionary Party (PRI) 70 years of one-party rule. Interrupting this political control unraveled long established corruption between DTOs and government officials at the local, state and national levels. It also opened opportunities for other non-state actors to enter or expand their illegal activities within Mexico.[7]

The frequency, proximity, and intensity of DTO-fueled violence along the U.S. southern border raises this issue to the forefront – one that U.S. elected officials can no longer ignore or simply paint as a Mexican internal issue. It is a vital U.S. national security interest that must be directly confronted and solved in concert with the Mexican federal government.

**Why U.S. – Mexican Relations are so Difficult**

At best, the United States has struggled to maintain effective foreign relations with Mexico. Mexicans carry a long memory of U.S. interventions, beginning with the conquest of nearly 40% of their territory in 1847 and reinforced by what they perceive as U.S. meddling in internal affairs with the influence of the presidential election in 1914 and the "invasion" of Mexican territory in 1916 to pursue a national hero, Francisco "Pancho" Villa. Jeffrey Davidow, the U.S. Ambassador to Mexico from 1998-2002, opines the worst label for a Mexican

politician is to be branded "Pro-American."[8] Mexicans do not want to be marked by their peer Latin and Southern American states as merely a minion of the United States. They value their independence, often taking an anti-U.S. position on world issues to reinforce this autonomy, as seen by their non-support of the invasion of Iraq in 2003.[9] Due to the longstanding mistrust of U.S. intentions, there has been very limited military interaction between U.S. and Mexican armed forces; merely token efforts to exchange defense attachés and have officers attending professional military schools.

However, Mexican cultural sensitivities toward direct U.S. military involvement in Mexico also appear to be thawing. The director of the Mexican Armed Forces University (La Universidad del Ejército y Fuerza Aérea Mexicanos), Brigadier General Benito Medina, recently remarked it was time for Mexico to accept international assistance to increase the fight against the DTOs.[10] Mexico has reinforced this notion with action – by assigning military officers to both U.S. Northern Command in Colorado and the Western Hemisphere Institute for Security Cooperation at Fort Benning, Georgia.[11]

Mexican cooperation with the United States, especially in regard to crime and corruption within Mexico, its peoples and institutions will require a delicate and sensitive approach to ensure U.S. efforts are not seen as overbearing and domineering.

**A New Beginning: The Mérida Initiative**

In 2007, Presidents Bush and Calderón, along with other Latin American leaders met in Mérida, Mexico to discuss rekindling security cooperation to address the threats of DTOs and other organized crime in Mexico and Central America. The stated goals were to:

> *[B]reak the power and impunity of criminal organizations; assist the Mexican and Central American government(s) in strengthening border, air, and maritime controls; improve the capacity of justice systems in the region; and curtail gang activity in Mexico and Central America while diminishing the demand for drugs in the region.*[12]

This initial effort centered primarily on a material solution to reduce the supply of illegal drugs by providing Mexico with specialized equipment for its police and military, along with automated information systems to assist intelligence gathering and law enforcement.

Providing specialized equipment and technical assistance to the Mexican Government enhanced their capabilities to reduce the supply of illegal drugs and restrict operations of Mexican-based DTOs. Between 2007 and 2010 over $1.4 billon has been pledged by the U.S. government: highlighted by the purchase and delivery of rotary and fixed-wing aircraft, non-intrusive inspection equipment, ion scanners, and canine units for Mexican customs, armed forces and federal police. Additionally, secure communications and data systems, as well as technical advice and training, are being purchased and provided to Mexican judicial institutions at the federal and state levels.[13]

The strengths of this effort are its ease of development, funding, and execution. First, U.S. military and law enforcement officials can easily develop an exhaustive list of capabilities to be purchased for the Mexican government that it either does not have or have in sufficient quantity. Second, the purchasing of goods and services with U.S. funding will be applied to U.S. businesses, maintaining or creating jobs in congressional districts across the nation – always an inviting proposition to elected officials. Congressional backing will ease the passage of funding requests in both the Department of Defense (DoD) and Department of State (DoS) appropriations, without drawing undue scrutiny from those parties overseeing federal spending. Finally, measurable progress can be demonstrated by equipment deliveries and systems fielding – providing citizens of both countries concrete proof that each government is fulfilling its pledge.

However, there are a number of drawbacks and limitations to this approach. First, it only solves a portion of the problem – reducing the supply of illegal drugs by combating DTOs – not the contributing causes of pervasive corruption within Mexican law and order institutions and illegal drug demand (addiction). In reviewing the DoD's FY 2009 budget request for the Mérida Initiative, the Senate Appropriations Committee "…remains concerned that the Mérida Initiative represents a one-dimensional approach to drug-trafficking and gang violence and

that a more comprehensive strategy is needed that also addresses the underlying causes."[14] Second, by only providing material and U.S. expertise, critics charge the United States is not fully committed, only making a token effort to solve the problem, and at worst creating ill will between the governments. Previous U.S. efforts have been less than successful. In 1995, U.S. officials offered Mexico 72 UH-1 series helicopters to support drug interdiction efforts. These were surplus helicopters being phased out of U.S. service. When transferred, they were not fully operational, had limited repair parts, and were not to be used in offensive operations against the separatists in the southern state of Chiapas. After the United States agreed to cannibalize parts and create 20 operational helicopters, the Mexicans demurred and declined to accept any of them – working with the U.S. government was in Ambassador Davidow's words, "just too much trouble for too little reward."[15] Next, procurement of equipment, especially aircraft and other specialized equipment is slow and not responsive to Mexican needs. Purchases made with U.S. appropriations must go through the Federal Acquisition Regulations procurement process, a plodding and unyielding system. Equipment is needed now, not months or sometimes years in the future as has often been the situation in previous cases.[16] For example, the three new UH-60M Black Hawk helicopters authorized and funded in June 2008 were finally delivered in November 2010 to the Mexican Federal Police.[17]

Finally, this approach is one dimensional; it ignores the demand side of the equation, the consumption of illegal drugs in the United States; as well as a fast-rising addiction rate among Mexican citizens. The number of Mexicans who said they had tried illegal drugs rose by more than 25% since the last survey in 2002, while addicts number almost half a million – a 51% increase. Mexican Attorney General Eduardo Medina Mora remarked in 2008, "[I]t is clear to everyone that our nation has stopped being a transit country for drugs going to the United States and become an important market as well."[18] Laura Carlsen, a former Fulbright Scholar and currently Director of the Americas Program of the Center for International Policy, based in Mexico City, is a vociferous opponent of the original Mérida Initiative. She believes this option,

> *…departs from the mistaken logic that interdiction, enforcement, and prosecution will eventually stem illegal cross border drug-trafficking…[P]roviding equipment and resources to Mexican security forces in the current context of corruption and impunity will deepen the problems, reduce civil society's role in reform, and inhibit construction of democratic institutions.*[19]

In summary, this approach, while a necessary and concrete first step, is easily continued by the Obama Administration and U.S. Congress but only provides superficial window dressing. The press releases and photo opportunities with U.S. officials presiding over equipment deliveries may be sufficient to convince the average voter; but will not adequately reduce the flow of illegal drugs into the United States. If continued, it will continue to be pilloried by critics and viewed by Mexicans as merely the United State's latest, insincere and impotent attempt to solve an important security problem affecting both peoples.

**The Next Level: Beyond Mérida**

In March 2010, U.S. Secretary of State Clinton and Mexican Foreign Minister Espinosa announced a second phase of the Mérida Initiative. The four goals referred to as "Beyond Mérida" or as the "4 Pillars" are to:

> *Disrupt organized criminal groups; institutionalize reforms to sustain the rule of law and respect for human rights; create a 21st century border; and build strong and resilient communities representing a conscious advance to tackle the root causes of this problem.*[20]

The goals were revised to emphasize the critical issue of not only reducing the supply of illegal drugs, but the demand as well – both in the United States and Mexico. This reorientation goes beyond providing U.S. equipment and expertise; it aims to strengthen individuals, groups, and institutions in a holistic, whole-of-government approach that is consistent with the current National Security Strategy (NSS). The strengths of this second phase are its whole-of-government emphasis, which is consistent with the current NSS: "[T]o succeed, we must update, balance, and integrate all the tools of American power and work with our allies and partners to do the same."[21]

**First Pillar: Disrupt Organized Criminal Groups**

This first goal continues the fight against the DTOs, with both material and non-material solutions. As mentioned earlier, the DTOs have evolved from merely providing transit services for illegal drugs flowing through Mexico to the United States into viable, enduring, profitable (albeit illegal) enterprises. By murdering public officials and targeting violence against a region, the DTOs demonstrate to the citizenry their ability to undermine civil control and the rule of law to fortify their freedom of action. John Sullivan, an officer with the Los Angeles Sheriff's Department and an expert on gang warfare, refers to this evolution as a third-generation gang, capable of protecting their lucrative economic activities by undermining the authority and legitimacy of the state.[22] Under this revised goal, the United States must assist the Mexican government with a combination of technical capabilities, training, and partnership opportunities to combat the DTOs on both sides of the border. However, this integration must and can only be successful if it proceeds at the pace comfortable and agreeable to the Mexican government and its society. As previously described, the introduction of U.S. government officials and military forces into Mexican territory has a checkered past and must be implemented skillfully. All efforts in Mexico must be Mexican-led activities, with the United States in a supporting role.

Equally important is the acknowledgement that U.S. consumption of illegal drugs must be addressed in this comprehensive solution. It was noteworthy that during her first official visit to Mexico as U.S. Secretary of State, Mrs. Clinton confronted this reality by stating, "[T]he U.S. recognizes that drug trafficking is not only Mexico's problem. It is also an American problem. And we, in the U.S., have a responsibility to help you address it."[23] Laura Carlsen feels this is the primary deficiency of the original (2007 Mérida Initiative) goals, "[S]tudies have shown that treatment and rehabilitation are 20 times more effective in decreasing the illegal drug trade."[24] By increasing U.S. funding of rehabilitation and treatment programs, the demand side of this economic equation is actively pursued. Richard Nixon, who coined the term, "War on Drugs" in 1971, was the first U.S. President to recognize and aggressively fund drug treatment and rehabilitation programs.[25] The Reagan presidency

saw the creation of some of the most visible prevention programs in the "Just Say No" campaign spearheaded by the then-First Lady Nancy Reagan, the growth of the Drug Abuse Resistance Education (D.A.R.E.) school lecture program, and the Partnership for a Drug-Free America public service announcements featuring the catch phrase, "This is your brain on drugs." Although memorable, these programs failed to significantly curtail the demand for illegal drugs.[26]

President Obama has continued emphasizing the importance of reducing illegal drug use. In the 2010 National Drug Control Strategy, the number one goal to be attained by 2015 is: Curtail illicit drug consumption in America. There is however, a disconnect between linking this number one goal with funding distribution: 64% of the FY 2010 funding request is directed towards supply reduction and only 36% for demand reduction programs.[27] To correct this disconnect, funding from sources involved in supply reduction must be reallocated to demand reduction, specifically towards the drug rehabilitation programs being administered by the Substance Abuse and Mental Health Services Administration within the Department of Health and Human Services.

In parallel, the significant flow of illegal small-arms weapons from the United States into Mexico must be stopped. In 2007-2008, over 5,000 weapons seized by Mexican law enforcement officials were positively traced to U.S. origins. Critics deride that the individual weapons seized are semi-automatic hunting rifles and handguns; while the DTOs purchase of vast quantities of automatic machine guns, rocket-propelled grenade launchers and other high-tech weapons goes unchecked. The U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) began Project Gunrunner as a pilot program in 2005 and expanded it into a national initiative in 2006. This program installed eTrace technology in U.S. consulates in Mexico, as well as assigning additional ATF agents in New Mexico and Arizona to stem the flow of weapons into Mexico.[28] However, according to the U.S. Justice Department's Inspector General, this program has been insufficient for reducing the continual flow of illegal weapons from the United States to Mexico.[29]

Notwithstanding the quantity and types of weapons in use, this source can be immediately stopped by ratifying the Inter-American Convention Against Illicit Manufacturing of and Trafficking in Firearms (CIFTA), which has been languishing in the U.S. Senate since 1998.[30]

Success in achieving the aims within this first pillar rest on the United States providing material and expertise, when asked, to support Mexican law enforcement and military institutions, taking significant steps to decrease the demand for illegal drugs in the United States, and strengthen laws to prohibit the illegal transfer of firearms.

**Second Pillar: Institutionalize Reforms to Sustain the Rule of Law and Respect for Human Rights**

This goal reflects one of the shortcomings in the 2007 initial effort. Through the establishment of programs in Mexico to educate and assist in maintaining sound governance and observe human rights, the vicious life cycle of corruption can be broken. Shannon O'Neil underscores the significance of this dimension at his recent congressional testimony: "[W]ithout capable and clean courts and cops, this battle cannot be won."[31] Laura Carlsen echoes this notion and further believes that merely providing U.S. tax dollars towards advanced information technology systems for Mexican law enforcement agencies is not a lasting solution. She views a three-pronged effort to effectively reform the Mexican judicial systems. The first and most important is recognition that improving the Mexican rule of law requires the will of its people to succeed. Corruption at all levels has been a fabric tightly woven into Mexican society. Comprehensive rule of law reform must involve a public outreach campaign, led by President Calderón, to instill a sense of commitment between the Mexican government and the people to ensure these reforms are palatable, achievable and lasting. Second, there must be acknowledgment that Mexican laws and legal system are not the same as in the United States. As is the case with U.S. military assistance, training and partnership within the Mexican legal community must have a Mexican face in order to be accepted, implemented and have a chance at enduring. An alternative to counter perceptions of the United States forcibly installing "North American" reforms would be to invite a member nation within the

Organization of American States, one with recent positive changes to its own legal institutions, such as the Republic of Colombia, to act as the mentor to the Mexicans. This would not only demonstrate that the reforms were not solely U.S. demands, but more importantly, that a peer nation faced a similar situation and found a working and lasting solution. Finally, in her third prong, Carlsen recommends that the U.S. government should address its own legal system. She favors reducing the demand for illegal drugs by prosecuting dealers and DTOs leaders as opposed to current laws that are drug user-centric. She asserts that the focus on arresting and prosecuting drug users drains critical law enforcement resources away from the drug providers, the DTOs and their representatives within the United States.[32]

Another initiative to improve the Mexican rule of law is to create protected justice complexes – a "legal green zone" – similar to what is being built in Iraq. Under this concept, a fortified base is constructed housing law enforcement offices, court facilities and a prison. In this environment, law enforcement personnel, judges and their families are able to safely live and work without fearing for their personal safety.[33] It also serves as a barrier to restrict corruption or other illegal influences upon the officials. This initiative could easily be replicated and placed into operation in Mexico as a tangible measure, demonstrating the Mexican government's commitment to its people to install genuine and lasting reform. The Iraqi government could be asked to provide its lessons learned in implementing this concept, again to put not only a non-U.S. face on it, but allow the Iraqi government to proudly display their efforts to rebuild their country and institutions.

Sustaining an effective rule of law within Mexico and changing the emphasis of U.S. drug laws will take considerable time and effort to achieve. It is worth the resources invested as it will provide the most benefit to all citizens if reforms are enacted appropriately and allowed to mature at a reasonable pace.

**Third Pillar: Create a 21st Century Border**

This goal, representing the economic component of this issue, has the most potential but also the most baggage. The creation of a high-tech border between the United States and Mexico presents an

opportunity to improve the two-way transit of legitimate commerce while allowing customs and border officials in both countries to devote more resources toward disrupting the flow of illegal drugs and other criminal activity.[34] Under this concept, transportation hubs would be established in cities in both countries where freight would be inspected and certified for cross-border travel, alleviating bottlenecks at the current, limited number of border crossing checkpoints. Additional benefits of this construct would be to reduce the costs of goods, as transportation times and the manpower required to prepare, submit, and track paperwork would be reduced. This concept of streamlining the movement of legitimate travel of goods and people was revived in 2005 under the Security and Prosperity Partnership of North America (SPP) agreement between Canada, Mexico and the United States.[35] One of over 300 areas in the SPP, this concept creates a transportation zone to move goods safely and efficiently across borders. Detractors almost immediately decried this proposal as a "NAFTA superhighway" and it became the lightning rod for groups and individuals convinced the three governments were conspiring to create a "North American Union," with an ultimate goal of breaking down sovereignty.[36] While the SPP was effectively abandoned in 2009, the U.S. Customs and Border Protection agency is aggressively implementing several programs such as the Container Security Initiative, Secure Freight Initiative, Customs-Trade Partnership Against Terrorism and the Automated Commercial Environment to modernize trade policies while accommodating the increasing volume and complexities of international trade and ensuring illicit goods do not enter the United States.[37]

To achieve an operational and effective 21st century border, the U.S. and Mexican governments, in conjunction with the respective transportation industries, should establish a public-private sector working group to examine how these programs and other technology-based initiatives can be modified, thoroughly tested, and implemented to improve the flow of legitimate goods between the two countries.

**Fourth Pillar: Build Strong and Resilient Communities**

This goal, as introduced by Secretaries Clinton and Espinosa, seeks to: address the root causes of crime and violence, promote the culture of

legality, reduce illicit drug use, promote a broader perception of the links between drug use and crime and violence, and stem the flow of potential recruits for the cartels by promoting constructive, legal alternatives for young people.[38]

Carlos Reyna, a sociologist and journalist, reinforces the criticality of this when he observed in his home country of Peru that "[A]ny antidrug policy that forsakes or underestimates the decisive importance of democratic institutions or economic and social issues will always be counterproductive and play into the hands of drug traffickers."[39] The U.S. Agency for International Development (USAID) should leverage its on-going best practices, for rapid implementation in Mexico, to assist in achieving the aims of this goal. As examples, two on-going programs in Colombia whose efforts are in concert with the needs of the Mexican people could be easily replicated. The first program is operated by "Actuar por Bolívar" (Acting for Bolivar), a USAID-supported non-governmental organization (NGO) that provides psychological counseling, business skills training, and access to small loans for individuals displaced and adversely impacted by illegal drug-fueled violence in Colombia.[40] The second program, "Familias en Accion" (Families in Action) is a USAID-sponsored crop eradication program under Plan Colombia.[41] It is noteworthy that USAID partners with the NGO and U.S. Corporation, Land O'Lakes, to achieve success. If adopted in Mexico, these programs could adapt to provide alternative opportunities for people forced to work in illegal drug processing activities. In both examples, the programs combine the best attributes of government's will to assist their people and the money, time, and effort invested by public corporations to improve the lives of innocent civilians adversely impacted by the violence wrought by the manufacture and flow of illegal drugs, as well as the accompanying crime and degradation of a functioning society.

**Implementation Challenges**

There are several drawbacks to fully implement the goals within the 4 Pillars. First, to execute the full range of programs and operations, funding must be authorized and appropriated from the U.S. Congress. While the original Mérida Initiative goals had programs concentrated

in two executive branch agencies (Defense and State), this option would encompass programs in as many as 11 agencies.[42] Program expansion requires additional funding to each participating agency. If all 11 agencies are involved, it would require oversight and legislation from upwards of 18 congressional committees and be promulgated in 8 of the 12 appropriations bills.[43] A further complication is the President's three-year budget freeze for non-defense agencies, starting with the FY 2011 budget.[44] Unfreezing portions of discretionary spending would require detailed justification from the President to the Congress and the American people.

It would create a precedent and opportunity for members of Congress to exploit this exemption and attempt to fund their unrelated earmarks, thus circumventing the basic intent. Finally, in order to create irreversible momentum, in terms of affecting funding legislation, it may already be too late. The first quarter of FY 2011 is complete; seed or bridge funds to begin specific actions within each of the 4 Pillars will have to be funded from within an Agency's remaining, current budget requiring a bill payer from one or more existing programs. Program managers are loath to give up funding from programs within their purview. It will take extraordinary leadership at the agency level to make this happen. Additionally, the Office of Management and Budget is reviewing and packaging the President's Budget Request for FY 2012 and will submit it to Congress on February 7, 2011. As it is with the current budget year, once a budget request is submitted, it is difficult to make program funding changes. Any changes will raise the scrutiny within the respective congressional oversight committees. It is possible for President Obama to direct year-of-execution funding changes in FYs 2011 and 2012, but it will take his personal political capital and follow through to ensure they are adjusted by each agency and approved by Congress. More realistically, significant initiatives will have to be included in the FY 2013 President's Budget Request in February 2012; however, this is too late for the administration to show its full commitment to implementing the 4 Pillars. Both the U.S. and Mexican presidential election cycles will be in full motion and detractors will have an opportunity to publicly criticize and charge the incumbents with not acting in a timely manner.

Next, the proliferation of participating agencies creates a span of control issue for the President. Within the Executive Office of the President, there is no statutory or appointed position to synchronize and execute a multi-agency program such as this. Currently the Secretary of State is designated as the government's lead for the Mérida Initiative. With the current good relations and nature of foreign military sales between Defense and State, this is a manageable and working solution. However, with multiple agency involvement, it is imperative that a single leader be appointed to execute this vital mission. To succeed, this leader must have the ability to control budget decisions and authority to represent the administration before Congress to obtain the appropriate legislation and funding. One recent proposal calls for the creation of a "Chief Operating Officer" position as outlined by former Senator Bob Kerrey. This concept recognizes that the President requires a senior official empowered to synchronize and follow-through on important national priorities – with the statutory powers beyond the currently appointed "czars."[45] However, in lieu of creating larger government, this role could be duplicated from the Administration's existing framework and execution of the American Recovery and Investment Act (ARRA), using the vice president as the lead official. As the President's chair for implementation of the ARRA, Vice President Joseph Biden, with support from the Office of Management and Budget, established the Recovery Implementation Office to monitor the implementation. Each agency is required to submit weekly progress updates, participate in biweekly meetings and attend periodic cabinet meetings chaired by the vice president.[46] The personal involvement of the vice president directly contributes to the successful execution of the ARRA and this construct can be replicated to fulfill the goals and programs under the 4 Pillars.

There is however, a high profile challenge facing both governments that could distract attention from the 4 Pillars efforts. Two former Mexican presidents, former leaders of Colombia and Brazil along with U.S. based groups, such as the National Organization for the Reform of Marijuana Laws, have called for legalization of illegal drugs as a solution.[47] However, legalization is simply not a viable option to reducing the demand for illegal drugs. The United States has greatly decreased the rate of cigarette and alcohol use while driving over the

past 30 years due to focused programs involving time, money and effort. The legalization of illegal drugs flies in the face of Mothers Against Drunk Driving (MADD) and the anti-tobacco smoking grassroots efforts. MADD estimates its efforts have saved 300,000 lives and the Foundation for a Smoke-Free America estimates the tobacco smoking effects on the U.S. society: "[T]he costs…include over 400,000 lives lost every year in the U.S. – over 1,200 each day – and $50 billion annually in lost productivity and increased health care costs."[48] Legalization proponents tout that decriminalization will provide numerous benefits to society: billions of dollars in increased tax revenue, relief for overworked law enforcement, courts and prisons, and increased safety through product quality regulation and oversight. These alleged benefits are tantalizing at face value; however, it distracts from the central issue – illegal drugs are addicting, harmful to users, and create long-term health care liabilities.[49]

Employers are already strained with current drug-testing requirements that ensure their employees are able to conduct their duties in a sober and safe manner. Lance Winslow, a small business owner and a retired founder of a nationwide franchise chain trade association comments on the legalization of illegal drugs:

> *[I]f more workers do come to work high, well, this might cause more incidents and accidents in the workplace, and thus, could potentially send workers comp skyrocketing. It also leaves the business owner, and the corporations with severe liability risks, which could also drive up other types of insurance.*[50]

Finally, this comprehensive approach will draw resistance from all quarters of U.S. society. Private organizations, such as the National Rifle Association could mount an effort within Congress to delay or disrupt critical legislation such as CIFTA. Additionally, despite the best of U.S. intentions, resistance could emanate from any number or combination of Mexican institutions, government or private organizations.

A significant risk lies in the resulting myriad of programs spread across the federal government. Each may not receive the highest priority from its congressional oversight committees and be funded at the requested levels. Unfunded programs will create gaps in the 4 Pillars, sub-optimize

the capabilities and dilute the results. If only a portion of the programs get funded and executed, the American (and Mexican) public will view partial, piecemeal results as yet another demonstration of the inability of their government(s) to solve vital, national security problems.

## Conclusion

It is time for bold action. For the next 18 months, there is sufficient continuity within both governments to create irreversible momentum to implement the programs contained in the 4 Pillars and demonstrate to citizens of both nations that it is possible to reduce both the demand and supply of illegal drugs on both sides of the U.S.-Mexico border. It will also break the destructive cycle of violence associated with the manufacture, transport, and distribution of illegal drugs. On the U.S. side, the comprehensive program of reducing not only supply but demand for illegal drugs and the appointment of the vice president to coordinate federal government efforts will ensure empowered synchronization. Strengthening Mexican governmental institutions by reducing corruption and instilling an emphasis on human rights will make enduring, positive changes to Mexican society. Secondary and tertiary effects such as a revitalized Mexican domestic economy and reduced illegal immigration to the United States may be realized. Tangible results will encourage citizens of both countries to demand a continuation of these programs under subsequent presidential administrations on both sides of the border in 2012 and beyond.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Endnotes

## Section One:
## Threats Facing Our Nation

### A New Mindset for Countering Terrorism


1. Ronald W. Reagan, *National Security Decision Directive 179* (Washington, DC: The White House, July 17, 1985), http://www.fas.org/irp/offdocs/nsdd/23-2628a.gif (accessed November 3, 2010).
2. Terrorism Project. *Chronology of Major Terrorist Attacks Against U.S. Targets* (Center for Defense Information, n.d.) http://www.cdi.org/terrorism/chronology.html (accessed November 1, 2010).
3. William J. Clinton, *Presidential Decision Directive 39* (Washington, DC: The White House, June 21, 1995) http://www.fas.org/irp/offdocs/pdd/pdd-39.pdf (accessed November 3, 2010).
4. Executive Order 13228 of October 8, 2001, Establishing the Office of Homeland Security and the Homeland Security Council (The Federal Register, Vol. 66, No. 196, Washington, DC, October 10, 2001), http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?Dbname=2001_register &docid=fr10oc01-144.pdf (accessed November 2, 2010).
5. Glenn Kessler and Peter Baker, "Bush's 'Axis of Evil' Comes Back to Haunt United States," *Washington Post*, October 10, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/10/09/AR2006100901130.html (accessed November 3, 2010).
6. Thomas Donnelly, *The Underpinnings of the Bush Doctrine* (American Enterprise Institute for Public Policy Research Series, February 2003), http://www.aei.org/outlook/15845 (accessed February 15, 2011).
7. Barrack H. Obama, "Remarks to the Nation on the Way Forward in Afghanistan and Pakistan" (U.S. Military Academy at West Point, December 1, 2009), http://www.whitehouse.gov/the-press-office/remarks-president-address-nation-way-forward-afghanistan-and-pakistan# (accessed November 5, 2010).
8. Sarah E. Zabel, *The Military Strategy of Global Jihad* (Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, October 2007) 18pp. (U413 .C2Z11 2007) http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=809 (accessed November 5, 2010).
9. Title 22 United States Code, section 2656f(d), *Annual Country Reports on Terrorism.* http://www.law.cornell.edu/uscode/422/usc_sec_22_00002656---f000-.html (accessed November 5, 2010).

10. Joint Publication 1-02, *DOD Dictionary of Military and Associated Term*s, 12 April 2001 (as amended through 30 September 2010): 468.

11. Straight UN Facts, Eye on the UN, a project of the Hudson Institute, New York. http://www.eyeontheun.org/facts.asp?1=1&p=61 (accessed December 17, 2010).

12. "UN Reform." United Nations. 2005-03-21. Archived from the original on 2007-04-27. http://web.archive.org/web/20070427012107/http://ww.un.org/unifeed/script.asp?scriptId=73. Retrieved 2008-07-11. "The second part of the report, entitled "Freedom from Fear backs the definition of terrorism–an issue so divisive agreement on it has long eluded the world community–as any action "intended to cause death or serious bodily harm to civilians or non- combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act."

13. Free Online Encyclopedia, http://encyclopedia2.thefreedictionary.com/War, (accessed December 17, 2010).

14. Gilles Andreani, "The 'War on Terror': Good Cause, Wrong Concept," *Survival*, vol 46, no. 4, Winter 2004-05 pp. 31-50: 31.

15. Ruba Ali, "The Bush Administration and the Problem of Torture," n.p., August 2005, http://www.osgoode.yorku.ca/glsa/2007conference/documents/Ruba%20Ali%20-%20The%20Bush%20Administration%20and%20the%20Problem%20of%20Torture.pdf (accessed December 21, 2010).

16. Paul Rogers, "Why We're Losing the War on Terror." *Polity* (Malden, MA, 2008): 119.

17. Davis Allsop, *The Viability of Deterring Terrorism*, June 11, 2010. http://www.e-ir.info/?p=4330#_ftn2 (accessed December 28, 2010).

18. N.I. Klonis, *Guerrilla Warfare: Analysis and Projections* (New York: Robert Speller, 1972): 5-6.

19. M.L.R. Smith, "Guerrillas in the Mist: Reassessing Strategy and Low Intensity Warfare," *Review of International Studies*, Vol. 29, No. 1 (2003), 20.

20. Andreani, "The 'War on Terror,'" 39.

21. Steven R. Watt, "Can the United States "Defeat" Al Qaeda?," Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, March 19, 2010): 18.

22. Harry R. Yarger, "Strategic Theory for the 21st Century: The Little Big Book on Big Strategy," *The Letort Papers*, U.S. Army War College, February 2006.

23. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1976): 88.

24. Scott Wilson and Al Kamen, "'Global War on Terror' is Given a New Name," *Washington Post*, March 25, 2009.

25. Ibid.

26. For definitions based on terrorism as a form of violence against the "innocent" see Christopher C. Harmon, *Terrorism Today* (London: Frank Cass, 2000): 21; Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999): 11.

27. Peter R. Neuman and M.L.R. Smith, "The Strategy of Terrorism, How it Works and Why it Fails," *Contemporary Terrorism Studies* (Routledge, New York, N.Y., 2008): 8.

28. Joshua Sinai, "A Conceptual Framework for Resolving Terrorism's Root Causes," in *Root Causes of Terrorism: Myths, Reality and the Ways Forward*, ed. By Tore Bjorgo (Routledge, New York, NY): 215.

29. Ibid, 21.

30. John L. Esposito and Dalia Mogahed, "Battle for Muslims' Hearts and Minds: The Road Not (Yet) Taken," *Middle East Policy*, Vol. 14, Iss. 1 (Washington: Spring 2007): 27.

31. Jacquelyn K. Davis, and Charles M. Perry. "Rethinking the War on Terror: Developing a Strategy to Counter Extremist Ideologies: A Workshop Report" *Institute for Foreign Policy Analysis* (Washington DC, March 2007): I. http://www.ifpa.org/pdf/Rethink_WOT.pdf (accessed December 17, 2010).

32. Brachman, Jarret M., and William F. McCants. *Stealing Al-Qa'ida's Playbook*. (Combating Terrorism Center, U.S. Military Academy, West Point NY, February 2006): 18. http://ctc.usma.edu/pdf/Stealing%20Al-Qai'da's%20Playbook%20--%20CTC.pdf (accessed December 17, 2010).

33. Esposito and Mogahed, "Battle for Muslims' Hearts and Minds," 27.

34. Davis and Perry, "Rethinking the War on Terror," I.

35. Michael G. Knapp, "The Concept and Practice of Jihad in Islam," *Parameters*, (Spring 2003), 82. http://www.carlisle.army.mil/USAWC/parameters/Articles/03spring/knapp.pdf (accessed January 16, 2011).

36. Sarah E. Zabel, The Military Strategy of Global Jihad. (Strategic Studies Institute, U.S. Army War College, Carlisle Barracks PA, October 2007): 1. http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=809 (accessed December 17, 2010).

37. Paul Rogers,"Reconsidering the War on Terror," *RUSI Journal,* vol.152, no. 4 (August2007): 33.

38. The caliphate is a single Muslim state operated as the Prophet did the first Muslim state. "Caliph" means "successor" in Arabic; the caliph is the successor to the Prophet in that he guides the people of Earth to live in accordance with God's laws in all respects: politically, economically, and socially, as well as religiously. The caliphate is the physical and political form of government over the lands and peoples the caliph guides.

39. Zabel, "The Military Strategy of Global Jihad," 4.

40. Ibid, 3.

41. In mid-2005 and early 2006, the Gallup Organization surveyed 10 predominantly Muslim countries (Morocco, Egypt, Turkey, Lebanon, Jordan, Saudi Arabia, Iran, Pakistan, Indonesia and Bangladesh) as part of its new World Poll, which by the end of 2006 will survey about 130 countries, including more than 35 that are predominantly Muslim. There were 1,000 in-home, face-to-face surveys per country, with sampling in urban and rural areas that is the statistical equivalent of surveying the nation's adult population, with a statistical-sampling error rate of plus or minus 3 percentage points. The findings of the Gallup World Poll provide a critical foundation and context for understanding the nature and origins of radical views, as well as perceptions about Western attempts to foster democratic governments. To determine who might be accurately categorized as "politically radicalized" and (moderate," Gallup looked at how respondents answered a question about the moral justification of the 9/11 attacks and their favorability ratings of the United States. Those who said the 9/11 attacks were completely morally justified and who also have an unfavorable or very unfavorable opinion of the United States were termed politically radicalized and thus potential supporters of terrorism. Those who did not say the attacks were completely justified were termed moderates. This group of "moderates" can be further broken down into "skeptical moderates," those with unfavorable opinions of the United States (51 percent), and "pro-U.S. moderates," those with neutral to favorable opinions of the United States (38 percent).

42. Esposito and Mogahed, "Battle for Muslims' Hearts and Minds," 27.

43. Rogers,"Reconsidering the War on Terror," 33.

44. Brachman and McCants. "Stealing Al-Qa'ida's Playbook," 9.

45. Ibid, 17.

46. Andreani, "The 'War on Terror,'" 36.

47. Charles Pena, *Winning the Un-War: A New Strategy for the War on Terrorism* (Potomac Books, Inc. Washington, D.C., 2006): 97-118.

48. Abdullah Yousef Sahar Mohammad, *Roots of Terrorism in the Middle East, in Root Causes of Terrorism: Myths, Reality and the Ways Forward*, ed. By Tore Bjorgo (Routledge, New York, NY, 2005): 116.

49. Davis and Perry, "Rethinking the War on Terror," III.

50. Allsop, "The Viability of Deterring Terrorism."

51. Norman M. Worthen, *Retooling Deterrence for the Long War*, Strategy Research Project (U.S. Army War College, Carlisle Barracks, PA, March 15, 2008): 17.

52. Ibid.

53. Brachman and McCants. "Stealing Al-Qa'ida's Playbook," 17.

## Systems Analysis, Centers of Gravity and Homeland Security

1. Jena Baker McNeil, James Jay Carafano, and Jessica Zuckerman, *30 Terrorist Plots Foiled: How the System Worked,* Background Paper (Washington D.C.: The Heritage Foundation, 2010): 1. http://thf_media.s3.amazonaws.com/2010/pdf/bg_2405.pdf (accessed November 6, 2010).
2. Barry Meier and Eric Lipton, "In Air Cargo Business, It's Speed vs. Screening, Creating a Weak Link in Security," *New York Times*, November 2, 2010.
3. Germain Difo, *Ordinary Measures, Extrordinary Results: An Assessment of Foiled Plots Since 9/11,* Security Policy Paper (Washington D.C.: American Security Project, 2010): 12-25. http://americansecurityproject.org/wp-content/uploads/2010/09/Foiled-Plots.pdf (accessed November 6, 2010).
4. John A. Warden, III, "The Enemy as a System," *Airpower Journal*, 515, no. 1 (Spring1995) http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (accessed November 6, 2010).
5. Difo, *Ordinary Measures,* 1.
6. Dennis C. Blair, *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence* (Washington D.C.: Office of the Director of National Intelligence, February 2, 2010): 8. http://intelligence.senate.gov/090212/blair.pdf (accessed November 6, 2010).
7. Brian M. Drinkwine, *The Serpent In Our Garden: Al-Qa'ida and the Long War,* Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, January 2009): 1.
8. Warren S. Eller and Brian J. Gerber, "Contemplating the Role of Precision and Range in Homeland Security Policy Analysis: A Response to Mueller," *Policy Studies Journal*, 38, no. 1 (February, 2010): 33; Department of Homeland Security, *Right Wing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment,* (Washington D.C.: Department of Homeland Security, 2009): 7-8. http://www.fas.org/irp/eprint/rightwing.pdf (accessed January 8, 2011).
9. Difo, *Ordinary Measures,* 27.
10. Brian Michael Jenkins, *Basic Principles for Homeland Security*, Testimony before the House Appropriation Committee, Santa Monica: RAND Corporation, (2007): 2. http://www.rand.org/pubs/testimonies/2007/RAND_CT270.pdf (accessed November 6, 2010).
11. Brain A. Jackson and David R. Frelinger, *Emerging Threats and Security Planning,* Occasional Paper (Santa Monica: RAND Corporation, 2009): 1. http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf (accessed November 6, 2010).
12. Joint Chiefs of Staff, *Joint Operations Planning, JP 5.0* (Washington D.C.: Department of Defense, 2010): III-21.

13. Ibid.
14. Ibid.
15. Ibid., III-22.
16. Rudolph M. Janiczek, "A Concept at the Crossroads: Rethinking the Center of Gravity," Strategic Research Paper (Carlisle Barracks, PA: U.S. Army War College, 2007): 5-10. http://www.strategicstudiesinstitute.army.mil/pdffiles/pub805.pdf (accessed November 6, 2010).
17. Antulio J. Echevarria II, *Clausewitz's Center of Gravity: Changing Our Warfighting Doctrine-Again!* (Carlisle Barracks, PA: U.S. Army War College, 2002): 10. http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=363 (accessed November 6, 2010).
18. Ibid., vii.
19. Warden, "The Enemy as a System," 2.
20. John A. Warden, III, "Air Theory for the Twenty-first Century," in *Battlefield of the Future,* ed. Barry R. Schneider and Lawrence E. Grinter (Maxwell AFB, AL: Air University Press, 1995): 6. http://www.airpower.maxwell.af.mil/airchronicles/battle/chp4.html (accessed October 17, 2010)
21. Ibid.
22. Ibid., 4.
23. Ibid., 8.
24. Ibid., 7.
25. Ibid.
26. Ibid., 9.
27. David A. Deptula, *Effects-Based Operations: Change in the Nature of Warfare,* (Arlington: Aerospace Education Foundation, 2001): 1-6. http://www.aef.org/pub/psbook.pdf (accessed October 17, 2010).
28. Warden, "The Enemy as a System," 12.
29. Ibid., 7.
30. Deptula, *Effects-Based Operations*, 6.
31. Ibid., 6.
32. Ibid., 5.
33. Ibid., 25.
34. Henry H. Willis, *Risk Informed Resource Allocation at the Department of Homeland Security,* (Santa Monica: RAND Corporation, 2007): 2. http://www.rand.org/content/dam/rand/pubs/testimonies/2007/RAND_CT272.pdf (accessed October 17, 2010).
35. Ibid., 2.

36. Jackson and Frelinger, *Emerging Threats and Security Planning,* 10.
37. Willis, *Risk Informed Resource Allocation at the Department of Homeland Security*, 1.
38. Ibid., 3.
39. John Mueller, "Assessing Measures Designed to Protect the Homeland," *Policy Studies Journal*, 38, no. 1 (February, 2010): 2. http://psweb.sbs.ohio-state.edu/faculty/jmueller/isa9psjx.pdf (accessed November 6, 2010).
40. Ibid., 11.
41. Ibid.
42. George W. Bush, *Homeland Security Presidential Directive, HSPD-7*, (Washington D.C.: U.S. Government, 2003) http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1 (accessed January 8, 2011).
43. Department of Homeland Security, *The Physical Protection of Critical Infrastructures and Key Assets,* (Washington D.C.: Department of Homeland Security, February, 2003): 2. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (accessed October 17, 2010).
44. John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation,* Report for Congress (Washington D.C.: Congressional Research Service, 2010): 10. http://www.fas.org/sgp/crs/homesec/RL30153.pdf (accessed October 17, 2010).
45. Ibid., 27.
46. Eller and Gerber, "Contemplating the Role of Precision," 42.
47. Mueller, "Assessing Measures Designed to Protect the Homeland," 4.
48. Ibid., 1.
49. Ibid., 3.
50. Eller and Gerber, "Contemplating the Role of Precision," 43.
51. Ibid.
52. Department of Homeland Security, *National Infrastructure Protection Plan,* (Washington D.C.: Department of Homeland Security, 2009), 1, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed November 6, 2010).
53. Ibid., 27-48.
54. Ibid., 28.
55. Ibid.
56. Ibid., 32.
57. Ibid., 34.
58. Department of Homeland Security, *National Planning Scenarios: Executive Summaries* (Washington D.C.: Department of Homeland Security, July,

2004) http://www.scd.hawaii.gov/grant_docs/National_Planning_Scenarios_ExecSummaries_ver2.pdf (accessed November 6, 2010).

59. Department of Homeland Security, *National Infrastructure Protection Plan*, 35.
60. Ibid.
61. Moteff, *Critical Infrastructures: Background, Policy, and Implementation,* 26.
62. Department of Homeland Security, *The Physical Protection of Critical Infrastructures and Key Assets,* 7.
63. Eller and Gerber, "Contemplating the Role of Precision," 32.
64. Ibid., 33.
65. Counterterrorism Coordinator Richard Clarke, "Strategy for Eliminating the Threat from Jihadist Networks of Al Qaida: Status and Prospects, "Memorandum for National Security Advisor Condoleeza Rice," Washington D.C., declassified December 2000, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB147/clarke%20attachment.pdf (accessed October 12, 2010).
66. Randy Borum et al., "Threat Assessment: Defining an Approach for Evaluating Risk of Targeted Violence," *Behavioral Sciences and the Law*, 17, no. 3, (1999), 329, http://www. secretservice.gov/ntac/ntac_bsl99.pdf (accessed October 17, 2010).
67. Ibid., 330.
68. McNeil, Carafano, and Zuckerman, *30 Terrorist Plots Foiled,* 1-16.
69. Borum et al., "Threat Assessment," 332.
70. Jenkins, *Basic Principles for Homeland Security,* 3.
71. Drinkwine, *The Serpent In Our Garden,* 17-19.
72. Sarah E. Zabel, *The Military Strategy of Global Jihad,* Strategic Research Paper (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 2007): 6. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB809.pdf (accessed October 17, 2010).
73. Drinkwine, *The Serpent In Our Garden,* 17.
74. This information regarding systems analysis and center of gravity determination is available via the Joint Publication 5.0 and can be found at this website: http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf (accessed 15 Jan 2011).
75. Nick Bloom, *The Economic Impact of 9/11,* Policy Brief (Stanford: Stanford Institute for Economic Policy Research, 2007): 1. http://www.stanford.edu/~nbloom/uncertaintyshocks_SIEPR.pdf (accessed November 6, 2010).
76. Gail Makinen, *The Economic Effects of 9/11: A Retrospective Assessment,* (Washington D.C.: Congressional Research Service, 2002): CRS-9. http://www.fas.org/irp/crs/RL31617.pdf (accessed November 6, 2010).

77. Bryan W. Roberts, *The Macroeconomic Impacts of the 9/11 Attack: Evidence from Real-Time Forecasting,* Policy Paper (Washington D.C.: Department of Homeland Security, Office of Immigration Statistics, August, 2009): 4. http://www.dhs.gov/xlibrary/assets/statistics/publications/ois_wp_impacts_911.pdf (accessed November 6, 2010).

78. Makinen, *The Economic Effects of 9/11,* CRS 3-12.

79. Ibid., CRS-3.

80. Ibid., CRS-10.

81. Ibid.

82. Difo, *Ordinary Measures,* 23.

83. McNeil, Carafano, and Zuckerman, *30 Terrorist Plots Foiled:,* 11.

84. Marisa Reddy Randazzo, Michelle Keeney, and Dawn Cappelli, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* Assessment (Washington D.C.: U.S. Secret Service and CERT Coordination Center, 2004): 7. http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec4extra/certreport.pdf (accessed October 17, 2010).

85. Paul Nyhan, "Longshoremen strike or lockout could stagger nation's economy." *Seattle-Post Intelligencer,* June 10, 2002. http://www.seattlepi.com/business/73906_longshore10.shtml (accessed October 31, 2010).

86. Difo, *Ordinary Measures, Extrordinary Results,* 12, 16.

87. Brian,Cashell and Marc Labonte, *The Macroeconomic Effects of Hurricane Katrina,* (Washington D.C.: Congressional Research Service, 2005): 4. http://fpc.state.gov/documents/organization/53572.pdf (accessed January 8, 2011).

88. Department of Homeland Security, *National Infrastructure Protection Plan*, 32.

## Electromagnetic Pulse: A Catastrophic Threat to the Homeland

1. U.S. Congress, Senate, Judiciary Committee Subcommittee on Terrorism and Homeland Security. *Government Preparedness and Response to a Terrorist Attack Using Weapons of Mass Destruction,* 111th Cong., 2nd sess., August 4, 2010.

2. Peter V. Pry, "What American Needs to Know About EMPs," *Foreign Policy*, March 17. 2010.

3. Peter V. Pry, "Provocatively Weak," *The Journal of International Security Affairs*, no. 19 (Fall/Winter 2010): 67.

4. A Jointly Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, (Washington, DC, June 2010), 2.

5. International Electrotechnical Commission 61000-2-9, *Electromagnetic Compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP Environment – Radiated Disturbance* (Geneva, Switzerland, February 1996).

6. EMP Commission, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack Volume 1: Executive Report*, (Washington DC, 2004), 5.

7. Ibid, 6.

8. Ibid.

9. *EMP Commission, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, (Washington DC 2008), 57.

10. Ibid, 4.

11. Charles N. Vittitoe, "Did High-Altitude EMP Cause the Hawaiian Streetlight Incident?" June 1989, http://www.ece.unm.edu/summa/notes/SDAN/0031.pdf (accessed February 4, 2011).

12. Jerry Emanuelson, "Test 184," www.futurescience.com/emp/test184.html (accessedFebruary 4, 2011).

13. National Research Council of the National Academics, "*Severe Space Weather Events – Understanding Societal and Economic Impacts,"* (The National Academies Press, Washington D.C., 2008), 1.

14. Stuart Clark, *"The Sun Kings: The Unexpected Tragedy of Richard Carrington and the Tale of How Modern Astronomy Began,"* (Princeton, NJ: Princeton University Press, 2007), 17.

15. Ibid, 22.

16. "Nuclear Weapons: Who Has What at a Glance," http://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat (accessed February 7, 2011).

17. Choe Sang-Hun, "North Korea Claims to Conduct 2nd Nuclear Test," *New York Times*, May 25, 2009.

18. "Rumsfeld Warns of Iran, N. Korea Electromagnetic Pulse Attack," http://www.newsmax.com/Headline/Donald-Rumsfeld-book-Iran/2011/02/13/id/385889 (accessed February 14, 2011).

19. Peter V. Pry, "What American Needs to Know About EMPs," *Foreign Policy*, March 17. 2010.

20. "North Korea's Missile Programme," http://news.bbc.co.uk/2/hi/2564241.stm (accessed February 14, 2011).

21. "Iran Test Fires Long Range Missiles – Then Warns Israel," *UK Guardian*, September 28, 2011.

22. U.S. Congress, House of Representatives, House Armed Service Committee, *Chairman Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack Testimony,* 110th Cong., 2nd sess., July 10, 2008.
23. "As the Sun Awakens; NASA Keeps a Wary Eye on Space Weather," http://science.nasa.gov/science-news/science-at-nasa/2010/04jun_swef/ (accessed February 10, 2011).
24. National Research Council of the National Academics, *"Severe Space Weather Events – Understanding Societal and Economic Impacts"* (The National Academies Press, Washington D.C., 2008), 77.
25. Ibid.
26. Ibid.
27. "Electric Power Industry 2009: Year in Review," http://www.eia.doe.gov/cneaf/electricity/epa/epa_sum.html (accessed February 23, 2011).
28. EMP Commission, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack* (Washington DC 2008), 27.
29. "Why Trucks are Essential," http://www.truckline.com/Newsroom/Pages/TrucksareEssential.aspx (accessed February 23, 2011).
30. Ibid.
31. U.S. Congress, House of Representatives, Subcommittee on Emerging threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security. *Securing the Modern Electric Grid from Physical and Cyber Attacks*, 111th Cong., 1st sess., July 21, 2009.
32. Ibid.
33. Ibid.
34. "*Grid Reliability and Infrastructure Defense Act,"* http://www.cbo.gov/ftpdocs/115xx/doc11517/hr5026.pdf (accessed February 25, 2011).
35 "H.R. 668 SHEILD Act," http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.+668 (assessed March 16, 2011).

## DIME Elements of Jihad

1. P. David Gaubatz and Paul Sperry, *Muslim Mafia: Inside the Secret Underworld that'sConspiring to Islamize America* (Los Angeles, CA: World Net Daily. 2009), 265.
2. Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II* (Washington, DC: The Center for Security Policy. 2010), 66. Stealth Jihad is a term coined by Robert Spencer.
3. Gaubatz and Sperry, *Muslim Mafia: Inside the Secret Underworld that's Conspiring to Islamize America*, 228-229.

4. Ibid, 230.
5. Ibid.
6. Ibid, v.
7. Ibid, 259.
8. Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II*, 51.
9. Gaubatz and Sperry, *Muslim Mafia: Inside the Secret Underworld that's Conspiring to Islamize America*, 259.
10. Ibid.
11. Ibid, 260.
12. Michael Hirsh, "A Politically Correct War: Nine years after 9/11 we still don't know how to deal with radical Islam," Newsweek, June 17, 2010, http://www.newsweek.com/2010/06/17/a-politically-correct-war.html.
13. Ibid.
14. Ibid.
15. Gaubatz and Sperry, *Muslim Mafia: Inside the Secret Underworld that's Conspiring to Islamize America*, ii.
16. Bill Warner, *Sharia Law for the Non-Muslim* (Center for the Study of Political Islam, CSPI, LLC, 2010, www.CSPIpublishing.com), 6
17. Ibid.
18. Ibid.
19. Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II*, 37.
20. Ibid.
21. Warner, *Sharia Law for the Non-Muslim*, 8.
22. Gaubatz and Sperry, *Muslim Mafia: Inside the Secret Underworld that's Conspiring to Islamize America*, ii.
23. Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II*, 58.
24. ibn naqib al-Misri, *Reliance of the Traveller: A Classic Manual of Islamic Sacred Law* (Beltsville, Maryland, Amana Publications, 1991): vii.
25. Walid Phares, "Jihadism's War on Democracies," American Thinker, November 01, 2010, http://www.americanthinker.com/2010/04/jihadisms_war_on_democracies.html.
26. Ibid.
27. Ibid.

28. Ibid.
29. Ibid.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid.
34. Brigitte Gabriel, *They Must be Stopped: Why We Must Defeat Radical Islam and How We Can Do It* (New York, New York: St. Martin's Press, 2008), 90.
35. Ibid.
36. Ibid, 96.
37. Ibid, 91.
38. Ibid.
39. Ibid.
40. Ibid.
41. Ibid.
42. Ibid.
43. Ibid.
44. Ibid, 92.
45. Ibid.
46. Ibid.
47. Ibid.
48. Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II*, 82.
49. Ibid.
50. Ibid.
51. Team B, *Shariah: The Threat to America An exercise in Competitive Analysis – Report of Team 'B' II*, 73.
52. Brigadier S.K. Malik, The *Quranic Concept of War* (Shandar Market, Chiti Qatar: Adam Publishers & Distributors, 1992),19.
53. Ibid, 33.
54. Ibid.
55. Ibid, 38.
56. Ibid.
57. Ibid, 42.

58. Ibid, 44-45.
59. Ibid, 45.
60. Ibid, 47-48.
61. Ibid, 48.
62. Ibid.
63. Ahmad ibn naqib al-Misri, *Reliance of the Traveller: A Classic Manual of Islamic Sacred Law* (Beltsville, Maryland, Amana Publications, 1991) 599.
64. Malik, The *Quranic Concept of War*, 48.
65. Ibid, 54.
66. Ibid.
67. Ibid.
68. Ibid.
69. Ibid, 59.
70. Ibid.
71. Ibid.
72. Ibid, 60.
73. Patrick Sookhdeo, *Understanding Sharia Finance: The Muslim Challenge to Western Economics* (McLean, VA: Issac Publishing, 2008), 7.
74. Ibid.
75. Ibid.
76. Ibid, 9.
77. Ibid.
78. Ibid, 8.
79. Ibid, 13.
80. Ibid, 8.
81. Ibid.
82. Ibid, 9.
83. Ibid, 17.
84. Ibid.
85. Ibid, 18.
86. Ibid, 19.
87. Ibid.
88. Ibid, 20.

89. Ibid, 24.
90. Ibid, 25.
91. bid.
92. Ibid.
93. Ibid.
94. Ibid.
95. Ibid.
96. Ibid, 37.
97. Ibid, 33.
98. al-Misri, *Reliance of the Traveller: A Classic Manual of Islamic Sacred Law,* 272.
99. Sookhdeo, *Understanding Sharia Finance: The Muslim Challenge to Western Economics*, 43.
100. Ibid, 44.
101. Ibid.
102. Ibid.
103. Ibid, 45.
104. Ibid, 49.
105. Ibid.
106. Ibid, 50.
107. Ibid, 54.
108. Dr. Tawfik Hamid, *Inside Jihad: Understanding and Confronting Radical Islam* (self-published book, 2007), 187.
109. Ibid.
110. Ibid, 188.
111. Andy Barr, "Oklahoma Bans Sharia Law," *Politico*, November 03, 2010, http://www.politico.com/news/stories/1110/44630.html.
112. Robert Spencer, *The Truth About Muhammad: Founder of the World's Most Intolerant Religion* (Washington, DC: Regnery Publishing, INC, 2006), 192.
113. Ibid.
114. Ibid, 183.
115. Ibid.
116. Ibid.
117. Brigitte Gabriel, *They Must Be Stopped: Why We Must Defeat Radical Islam and How We can Do It,* 233.

118. Ibid.
119. Hamid, *Inside Jihad: Understanding and Confronting Radical Islam*, 189.
120. Ibid, 190.
121. Ibid.
122. Ali A. Mazrui, "Islam and the United States: Streams of Convergence, Strands of Divergence," *Third World Quarterly,* Volume XXV, Issue 5 (July 2004): 811
123. Ibid, 812.
124. Ibid.
125. Spencer, The *Truth About Muhammad: Founder of the World's Most Intolerant Religion*, 192.
126. Gabriel, *They Must Be Stopped: Why We Must Defeat Radical Islam and How We can Do It,* 55.

## Cyber Attack! Crime or Act of War?

1. John Rollins and Anna Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations" (Washington, DC: Congressional Research Service, March 10, 2009), 8-15.
2. U.S. Government Accountability Office, *CYBERCRIME: Report to Congressional Requesters* (Washington, DC: U.S. Government Accountability Office, June 2007), 12.
3. Jeffrey F. Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition* (Tucson, AZ: Lawyers and Judges Publishing Inc., 2009) 311.
4. Ibid., 318
5. Ibid. Addicott is quoting the United Nations Secretary General, Kofi Annan, in 2005 defining terrorism.
6. Merriam-Webster Dictionary
7. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Arlington, VA: RAND Corporation, 2009), 23
8. Ibid.
9. Ibid., 43-46.
10. Ibid., 117.
11. U.S. Department of the Air Force, *Air Force Basic Doctrine*, Air Force Doctrine Document 1 (Washington, DC: U.S. Department of the Air Force, November 17, 2003), 36-37.
12. Peter Pace, *The National Military Strategy for Cyberspace Operations (Redacted)* (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006), 3.
13. Ibid., ix.

14. Ibid., 3-5.
15. U.S. Department of the Air Force, *Cyberspace Operations*, Air Force Doctrine Document 3-12 (Washington, DC: U.S. Department of the Air Force, July 15, 2010), 7.
16. IHS Jane's, "Jane's Defense Equipment and Solutions," http://www.janes.com/products/janes/defence/index.aspx (accessed January 9. 2011)
17. U.S. Government Accountability Office, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance* (Washington, DC: U.S. Government Accountability Office, July 2010), 5.
18. Richard B. Porterfield, "Naval Intelligence: Transforming to Meet the Threat," *United States Naval Institute Proceedings*, (September 1, 2005): 13-14
19. U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01 (Washington, DC: U.S. Joint Chiefs of Staff, October 7, 2004), I3-I7.
20. Mark M. Lowenthal, *Intelligence: From Secrets to Policy,* 4th ed. (Washington, DC: CQ Press, 2009), 2-3.
21. Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyberattacks* (Washington, DC: The National Academies Press, 2010): 168.
22. George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), viii.
23. House Permanent Select Committee on Intelligence, *Cyber Security: Hearing on the Nation's Cyber Security Risks*, 110th Cong. (September 18, 2008) (Statement of Paul Kurtz, Former Senior Director, Critical Infrastructure Protection, White House Homeland Security Council).
24. Senators Sheldon Whitehouse, Barbara Mikulski, and Olympia Snowe, "Cyber Self-Defense Can Help U.S. Security," September 3, 2010, http://www.cnn.com/2010/OPINION/09/03/senators.cyber.security/index.html?hpt=C2 (accessed September 3, 2010). The senators are members of the Senate Intelligence Committee and were making comments on an unclassified key finding from a classified study on cybersecurity.
25. Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence,* (Washington, DC: Director of National Intelligence, February 25, 2009).
26. William Lynn, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September/October 2010): 99.
27. "2009 Report to Congress of the US-China Economic and Security Review Commission," (Washington, DC: U.S. Government Printing Office, November 2009), 167-180, quoted in U.S. Army War College, *Information Operations Primer,* FY11 ed. (Carlisle Barracks, PA: U.S. Army War College, November 2010), 21.

28. U.S. Government Accountability Office, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, 5.
29. Shirley Kan, "China's Anti-Satellite Weapon Test," (Washington, DC: Congressional Research Service, April 23, 2007), 1-3.
30. IHS Jane's, "Seoul Reacts to North Korean Cheonan Attack," http://www.janes.com/products/janes/defence-security-report.aspx?ID=1065927927 (accessed January 9, 2011)
31. Lynn, "Defending a New Domain," 99.
32. Whitehouse, "Cyber Self-Defense Can Help U.S. Security"
33. David M. Hollis, "USCYBERCOM, The Need for a Combatant Command versus a Subunified Command," *Joint Force Quarterly* 58 (3rd Quarter 2010): 50.
34. Libecki, *Cyberdetterence and Cyberwar*, xiii.
35. Brian M. Mazanec, "The Art of (Cyber) War," *Journal of International Security Affairs* no.16 (Spring 2009): 81-90.
36. Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 340.
37. Hollis, "USCYBERCOM, The Need for a Combatant Command versus a Subunified Command," 50.
38. Rollins and Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," 12-13.
39. Rollins and Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, 11.
40. Pace, *The National Military Strategy for Cyberspace Operations (Redacted)*, A1.
41. U.S Secretary of Defense Robert Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," Memorandum for Secretaries of the Military Departments, Washington DC, June 23, 2009.
42. Barrack Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 27
43. Leisheng Peng, University of Malaga, Spain, Duminda Wijesekera, University of Malaga, Spain, Thomas C. Wingfield, University of Malaga, Spain, and James B. Michael, University of Malaga, Spain. 2006. An ontology-based distributed whiteboard to determine legal responses to online cyber attacks. Internet Research 16, no. 5, (October 20): 475-490. http://www.proquest.com.ezproxy.usawcpubs.org/ (accessed December 8, 2010).
44. Ibid.
45. Oklahoma Assistant District Attorney Michelle Bodine-Keely, interview by author, Tulsa, OK, January 2, 2011.

46. A. LeRoy Bennett, *International Organizations*, 2nd ed. (Englewood Cliffs, NJ: Prentice-Hall, 1980): 54-60.
47. Ibid., 5-9.
48. George C. Herring, *America's Longest War*, 4th ed. (New York: McGraw-Hill, 2002): 142-145.
49. Ibid., xi.
50. Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 341.
51. United Nations Charter, Article 1.
52. United Nations Charter, Article 2(4).
53. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *The Columbia Journal of Transnational Law* 37 (1999): 900.
54. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 900-908.
55. Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 340-342.
56. United Nations Charter, Article 41.
57. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 913.
58. Addicott, *Terrorism Law; Materials, Cases, Comments Fifth Edition,* 312-314.
59. Thomas C. Reed, *At the Abyss, An Insider's History of the Cold War*, (New York: Ballantine Books, 2004), 268.
60. United Nations Charter, Article 51.
61. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156.
62. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 912-914.
63. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156-157.
64. United States Army War College, *Information Operations Primer – AY 11 Edition*, (Carlisle Barracks, PA: U.S. Army War College, November, 2010): 24.
65. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156-157.
66. Ibid.
67. Ibid.
68. Ibid.

69. Ibid.
70. Ibid.
71. Ibid.
72. Ibid.
73. Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, April 4, 2009, 1-5. http://www.iar-gwu.org/node/65 (accessed August 10, 2010)
74. Ibid.
75. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156-157.
76. Ibid.
77. Ibid.
78. Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," 3.
79. Ibid., 4.
80. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," 156.
81. Ibid.
82. Kenneth Geers, *Cyberspace and the Changing Nature of Warfare*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2008): 7.
83. Pascal Mallet, "Emergence of Stuxnet Worm Highlights Cyber Warfare," *Defense News*, October 1, 2010, http://www.defensenews.com/story.php?i=4824625 (accessed October 20, 2010)
84. Paul A. Matus, *Strategic Impact of Cyber Warfare Rules for the United States*, Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, 25 March 2010), 18-22.
85. Joseph Menn, "Rules of Engagement for Cyberwars See Slow Progress," *Financial Times*, December 29, 2010, http://ebird.osd.mil/ebfiles/e20101229797273.html (accessed December 29, 2010)

## Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy

1. Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 51-52.
2. Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May, 2010): 27.

3. Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February, 2010): 37.
4. Obama, *National Security Strategy,* 27.
5. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 24. Dr. Kuehl cites the William Gibson science fiction novel, *Neuromancer*.
6. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010, amended through January 31, 2011): 92.
7. Kuehl, "From Cyberspace to Cyberpower," 28. A similar definition is found in U.S. Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, September 17, 2006, incorporating Change 2, March 22, 2010): II-22.
8. Ibid., 38.
9. William Oliver Stevens and Allan Westcott, *A History of Sea* Power (New York: Doubleday, 1920), 443, quoted in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 38.
10. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009), 10-11.
11. Ibid., 80-81.
12. CBS News/Associated Press, "Lights Back On In Brazil After Blackout," November 11, 2009, http://www.cbsnews.com/stories/2009/11/10/world/main5607148.shtml?tag=mncol;lst;1 (accessed February 27, 2011).
13. Jeffrey Carr, *Inside Cyber* Warfare (Sebastopol, CA: O'Reilly Media, 2010), 3.
14. Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 475-476.
15. Clay Wilson, "Cyber Crime," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 420.
16. U.S. Congress, House of Representatives, Committee on Armed Services, *U.S. Cyber Command: Organizing for Cyberspace Operations*, 111th Congress, hearing held September 23, 2010 (Washington, DC: U.S. Government Printing Office, 2010), 37.
17. Carr, *Inside Cyber Warfare,* 12-13.
18. Ibid., 11.
19. Ibid., 4.
20. Kuehl, "From Cyberspace to Cyberpower," 39.

21. Harold Kwalwasser, "Internet Governance," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 498.
22. Starr, "Toward a Preliminary Theory of Cyberpower," 67.
23. Ibid.
24. Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 7.
25. U.S. Air Force, "Cyber Command Achieves Full Operational Capability," release number 031110, November 3, 2010, http://www.afspc.af.mil/pressreleasearchive/story.asp?id=123229293 (accessed April 21, 2011).
26. U.S. Strategic Command, "Factsheet: U.S. Cyber Command," http://www.stratcom.mil/factsheets/Cyber_Command (accessed April 18, 2011).
27. William J. Lynn, III, "Remarks at Stratcom Cyber Symposium," May 26, 2010, http://www.defense.gov/Speeches/Speech.aspx?Speechid=1477 (accessed April 18, 2011).
28. Ibid.
29. Cheryl Pellerin, "Lynn: Cyberspace is the New Domain of Warfare," (Washington, DC: American Forces Press Services, October 18, 2010), http://www.defense.gov/news/newsarticle.aspx?ID=61310 (accessed November 20, 2010).
30. U.S. Congress, *U.S. Cyber Command*, 40.
31. National Security Council, *The Comprehensive National Cybersecurity Initiative*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed April 18, 2011).
32. Lynn, "Remarks at Stratcom Cyber Symposium."
33. Ibid.
34. Department of Homeland Security, "Privacy Impact Assessment for the Initiative Three Exercise," March 18, 2010, (Washington DC: Department of Homeland Security, 2010): 3.
35. The White House, "National Cybersecurity Center Policy Capture," http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf (accessed April 21, 2011).
36. Shaun Waterman, "U.S. Cybersecurity Head Quits, Citing Growing Role of Spy Agencies," (Washington DC: UPI, March 11, 2009), http://www.upi.com/Top_News/Special/2009/03/11/US-cybersecurity-head-quits-citing-growing-role-of-spy-agencies/UPI-64411236692969/ (accessed April 21, 2011).
37. Director Beckstrom argued that improved checks and balances would result by keeping the operational agencies separate, a policy contrary to the principle of unity of effort. Though he could have, he did not advocate for legislative

or judicial oversight, similar to Congressional oversight of the military or of the intelligence community. Legislative or Judicial oversight would provide effective checks and balances while maintaining the benefits of interagency collaboration and cooperation.

38. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* 67.
39. Ibid.
40. Carr, *Inside Cyber Warfare,* 34-35.
41. International Criminal Police Organization, "About INTERPOL," http://www.interpol.int/public/icpo/default.asp (accessed April 25, 2011).
42. Carr, *Inside Cyber Warfare,* 35.
43. Ibid., 15-17.
44. Kwalwasser, "Internet Governance," 517.
45. Council of Europe, *Convention on Cybercrime*, European Treaty Series No. 185 (Budapest: November 23, 2001).
46. Carr, *Inside Cyber Warfare,* 67.
47. Obama, *National Security Strategy,* 27.
48. U.S. Joint Chiefs of Staff, *Deterrence Operations Joint Operations Concept* (Washginton, DC: U.S. Joint Chiefs of Staff, December 2006), 20.
49. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 303.
50. Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security,* Kramer, Starr, and Wentz, 314.
51. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 141.
52. U.S. Congress, *U.S. Cyber Command*, 40.
53. Kramer, "Cyberpower and National Security," 19.
54. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 309.
55. Ibid., 312.
56. Carr, *Inside Cyber Warfare,* 179-182.
57. Ibid., 181.
58. Ibid., 182.
59. Ibid.
60. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 310.

61. Carr, *Inside Cyber Warfare,* 15-17.

62. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* 312.

63. Carr, *Inside Cyber Warfare,* 79-83.

## History and Evolution of MalWare

1. Lincoln University of the Commonwealth of Pennsylvania "Internet History," *Connected: An Internet Encyclopedia*, http://www.lincoln.edu/math/rmyrick/ComputerNetworks/Inet Reference/57.htm (accessed March 21, 2011).

2. Tom Meltzer and Sarah Phillips' "From the first email to the first YouTube video: a definitive internet history," *The Guardian*, October 23, 2009, http://www.guardian.co.uk/technology/2009/oct/23/internet-history, (accessed March 21, 2011); Thomas Chen and Jean-Marc Robert, "The Evolution of Viruses and Worms," published in *Statistical Methods in Computer Security*, W.S. Chen, ed. (Boca Raton, Florida: CRC Press, 2004) http://vx.netlux.org/lib/atc01.html (accessed March 21, 2011).

   The *Creeper* was an experimental self-replicating program written in 1971 by Bob Thomas, a programmer at Bolt, Beranek and Newman, and is generally accepted as the first computer virus. Thomas wrote Creeper to demonstrate a "mobile application." Creeper infected DEC PDP-10 computers running the TENEX operating system to display the message, "I'm the creeper, catch me if you can!" Creeper would start to print a file, then stop, find another Tenex system, and transfer to the other machine. The program did not replicate itself; it jumped from one system to another, removing itself from previous systems as it propagated forward.

3. CIO, *A Brief History of Malware and Cybercrime*, http://www.cio.com/article/116250/A_Brief_History_of_Malware_and_Cybercrime (accessed March 21, 2011); Brad Templeton, *Reaction to the DEC Spam of 1978*, http://www.templetons.com/brad/spamreact.html (accessed March 21, 2011).

   The first spam e-mail was sent in 1978 by a Gary Thuerk, an aggressive Digital Equipment Corporation marketing executive, who emailed to promote a new computer, the Decsystem-20. Thuerk felt the Dec-20 was relevant news to ARPAnet users, in that it was the first major system with ARPAnet software built into it. Defense Communications Agency (DCA) which ran ARPAnet, called Thuerk's boss to register a strong complaint.

4. CIO, *A Brief History of Malware and Cybercrime.* On November 2, 1988, the Morris worm disabled 6,000 computers, roughly 10 percent of the existing network, in just a few hours. Robert Morris, Jr., a Cornell University graduate student, created software designed to automatically replicate itself on computers linked through ARPAnet. While this was not the first worm, it was the first created to propagate across linked computers. Morris said he was using the

worm to measure the size of the Internet. Unfortunately, the worm contained an error that caused it to infect computers multiple times, creating a denial of service. According to the General Accounting Office, the Morris worm infected thousands of government computers and caused $10-$100 million in damage. Morris was convicted of violating the 1986 Computer Fraud and Abuse Act and sentenced to three years' probation, 400 hours of community service, and a fine of $10,050.

5. Internet World Stats, *United States of America Internet Usage and Broadband Usage Report*, http://www.Internetworldstats.com/am/us.htm (accessed March 21, 2011).

6. James Jay Carafano and Eric Sayers, "Building Cyber Security Leadership for the 21st Century," *Backgrounder* no. 2218, December 16, 2008, http://www.carlisle.army.mil/DIME/ documents/bg_2218%5B1%5D.pdf. (accessed March 21, 2011).

7. U.S. Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats* (Washington, DC: U.S. Government Accountability Office, June 2007), 4-9; Audrey Plonk and Anne Carblanc, Malicious Software (Malware): A Security Threat to the Internet Economy, (Paris, France: Organization for Economic Co-operation and Development, March 6, 2008) 10-32, http://www.oecd.org/dataoecd/53/34/40724457.pdf (accessed March 21, 2011).

8. In U.S. military doctrine, there are essentially two forms of unauthorized computer access, an attack on or an exploitation of the computer system. A Computer Network Attack or CNA will "disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." The purpose of a CNA is to deny the owner of the attacked system the use of the system or the information stored in or transmitted by the system. According to this definition, hacking into a computer system to deface a website would constitute an attack. In contrast, hacking the same system to steal information resident in the network is a Computer Network Exploitation or CNE, per U.S. doctrine. CNE are "Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks." The purpose of a CNE is to collect information, not damage the system. CNE can be considered theft or espionage, depending on the identities of the exploiter and the owner of the exploited computer system. See Dennis M. Murphy, ed., *Information Operations Primer*, (Carlisle, Pennsylvania: U.S. Army War College, 2010), 169.

9. Joseph S. Nye, Jr., *Cyber Power* (Cambridge, Massachusetts: Harvard Kennedy School, May 2010), 3-7; Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the "First Battle" in 21st-century War," *Defense Horizons* no. 68 (September 2009): 2-3; U.S. Congress, House of Representatives, House Permanent Select Committee on Intelligence, *Paul B. Kurtz: Cyber Security Hearing*, 110th Cong.,

2nd sess., September 19, 2008, 7-9, http://www.fas.org/irp/congress/2008_hr/091808kurtz.pdf (accessed March 21, 2011).

The People's Republic of China is widely suspected of conducting computer network reconnaissance against foreign governments, businesses and non-governmental organizations: Titan Rain and Ghostnet are two of their more famous operations. The PRC is also believed to have conducted computer network attacks, primarily against the government of Taiwan. Russia has been directly implicated in distributed denial of service attacks against both Estonia and Georgia.

10. Plonk and Carblanc, *Malicious Software (Malware): A Security Threat to the Internet Economy*, 6. The National Institute of Standards and Technology offers a similar definition, "Malware: a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim." Peter Mell, Karen Kent, Joseph Nusbaum, *Guide to Malware Incident Prevention and Handling*, Special Publication 800-83, (Gaithersburg, Maryland: National Institute of Standards and Technology, November 2003), 2-10, www.nist.gov/manuscript-publication-search.cfm?pub_id=150416 (accessed March 25, 2011.

11. Ibid., 9-13; Alex Noordergraaf, *How Hackers Do It: Tricks, Tools, and Techniques* (Santa Clara, California: Sun Microsystems, Incorporated, May 2002), 2-10.

12. Fred Cohen coined the term "computer virus" in his PhD thesis "Computer Viruses - Theory and Experiments," published in 1986. Computer viruses replicate by attaching their program instructions to a program or document within a computer so that the virus' instructions are executed during execution of the host program. A basic computer virus contains at least two subroutines. The first subroutine is the infection itself, seeking out programs or files and attaching its instructions to their own. The second subroutine carries the 'payload,' the actions that will be executed by the infected computer. The payload could be almost anything: deletion of data, installation of backdoors, denial of service agents, etc. See Thomas Chen and Jean-Marc Robert, "The Evolution of Viruses and Worms," published in *Statistical Methods in Computer Security*, W.S. Chen, ed. (Boca Raton, Florida: CRC Press, 2004) http://vx.netlux.org/lib/atc01.html (accessed March 21, 2011).

13. Worms self-replicate much like viruses, but do not attach themselves to host system programs. Worms are stand-alone, automated programs which travel through a network looking for vulnerable computers to infect. Worms need a network, but are not dependent on the execution or operation of a program on the infected computer. Worms have become common with the spread of Internet connectivity. See Chen and Robert, "The Evolution of Viruses and Worms."

14. Mell, Kent & Nusbaum, *Guide to Malware Incident Prevention and Handling*.

15. BitDefender, *Malware History*, copyright 2008-2010, 14-15, http://download.bitdefender.com/resources/files/Main/file/Malware_History.pdf (accessed March 21, 2011); Plonk and Carblanc, *Malicious Software (Malware): A Security Threat to the Internet Economy*, 10.

16. Samuel Greengard, "Brief history of Malware," *Baseline Magazine*, March 17, 2010, http://www.baselinemag.com/c/a/Security/A-Brief-History-of-Malware-291930/ (accessed March 20, 2011); Guillaume Lovet, "40th anniversary of the computer virus," *Help Net Security*, http://www.net-security.org/malware_news.php?id=1668 (accessed March 21, 2011); BitDefender, *Malware History*, 17-18.

    *Elk Cloner* is one of the first known viruses to spread beyond the systems for which it was intended. The virus was written by Rich Skrenta for Apple II systems and spread via floppy disks. Infected computers showed a harmless, humorous poem after every 50th boot. Skrenta had been playing jokes on friends by altering copies of pirated games to self-destruct after a number of plays. Soon, his classmates were getting wary of letting Skrenta near their disks. He came up with the idea to leave a virus in the operating system of the school's Apple II. If the next user didn't do a clean reboot with their own disk, their game program would be infected.

17. A Trojan horse is a self-contained, non-replicating program that appears benign or even advantageous, but actually has hidden malware. Trojan horses either replace existing files with malicious versions or add new malicious files to systems. They often deliver other attacker tools to systems. See Mell, Kent & Nusbaum, *Guide to Malware Incident Prevention and Handling*, 2-4 through 2-5.

18. G Data Software AG, History of malware: A brief history of viruses, worms and Trojans, http://www.gdatasoftware.com/information/security-labs/information/history-of-malware.html (accessed March 21, 2011); BitDefender, *Malware History*, 18-19.

19. G Data Software AG, *History of Malware: A brief history of viruses, worms and Trojans*; BitDefender, *Malware History*, 20-26.

20. In 1991, Symantec (then Norton) released the Norton Anti-virus software. Anti-virus products from IBM, McAfee, Digital Dispatch and Iris were also available. See SpamLaws, "The History of the Computer Virus," http://www.spamlaws.com/history.html (accessed March 25, 2011).

21. Symantec, "Understanding and Managing Polymorphic Viruses," *The Symantec Enterprise Papers*, Volume XXX (Cupertino, California: Symantec, Inc, 1996) 3-5, http://www.symantec.com/avcenter /reference/striker.pdf (accessed March 25, 2011).

    "A polymorphic virus includes a scrambled virus body and a decryption routine that first gains control of the computer then decrypts the virus body. It also includes a mutation engine that generates randomized decryption routines

that change each time a virus infects a new program. In a polymorphic virus, the mutation engine and virus body are both encrypted. When a user runs a program infected with a polymorphic virus, the decryption routine first gains control of the computer, then decrypts both the virus body and the mutation engine. Next, the decryption routine transfers control of the computer to the virus, which locates a new program to infect. At this point, the virus makes a copy of both itself and the mutation engine in random access memory (RAM). The virus then invokes the mutation engine, which randomly generates a new decryption routine that is capable of decrypting the virus, yet bears little or no resemblance to any prior decryption routine. Next, the virus encrypts this new copy of the virus body and mutation engine. Finally, the virus appends this new decryption routine, along with the newly encrypted virus and mutation engine, onto a new program." Symantec, "Understanding and Managing Polymorphic Viruses," *The Symantec Enterprise Papers*, Volume XXX (Cupertino, California: Symantec, Inc, 1996) 3-4, http://www.symantec.com/avcenter/reference/striker.pdf (accessed March 25, 2011).

The *Tequila virus* created a large, expanding black spot in the middle of the computer monitor screen accompanied by the message, "Welcome to T. Tequila's latest production. Beer and Tequila forever!" NetSafe, Internet Safety: Viruses, 2007, http://www.e-learning-computing.com/is01cg/page_25.htm (accessed March 21, 2011).

The *Maltese Amoeba* virus was a polymorphic logic bomb designed to overwrite the first sector of the data storage medium on two specific days of the year. Greengard, "Brief history of Malware."

22. A Mutation Engine (MtE or MTE) is a program designed to generate viruses. Even early virus creation tools were able to generate hundreds or thousands of different, functioning viruses, which were initially undetectable by current scanners. The engine will encrypt virus code each time with a different encryption key. It will also generate a routine to decrypt it, which will also differ each time. Both the decryption routine and the encrypted code will have variable lengths. *Spyware Detail: Mutation Engine MTE*, CA Technologies, posted August 16, 2004, http://gsa.ca.com/pest/pest.aspx?ID=453076400 (accessed March 23, 2011).

23. Symantec, "Understanding and Managing Polymorphic Viruses," *The Symantec Enterprise Papers*, Volume XXX (Cupertino, California: Symantec, Inc, 1996) 5, http://www.symantec.com/avcenter/ reference/striker.pdf, (accessed March 25, 2011); Thomas Chimento, "A Brief History of Malware," briefing slides, November 8, 2010, http://mysite.webroot.com/forms/NAWNHIST0810 (accessed March 25, 2011); Chen and Robert, "The Evolution of Viruses and Worms."

24. Macro language is a special-purpose command language used to automate sequences within an application such as a spreadsheet or word processor. A macro virus is encoded as a macro embedded in a document. Many applications, such

as Microsoft Word, Access, PowerPoint, and Excel, support powerful macro languages. These applications allow a hacker to embed a macro in a document, and have the macro execute each time the document is opened. According to some estimates, 75% of all viruses today are macro viruses. See PC Magazine, Encyclopedia: Macro language, http://www.pcmag. com/ encyclopedia_term/0 ,2542,t=macro+language&i=46466,00.asp (accessed March 21, 2011). See PC Magazine, *Encyclopedia: Macro virus,* http://www.pcmag.com/encyclopedia_ te rm/0,2542,t=macro+virus&i=46469,00.asp (accessed March 21, 2011).

25. When activated, *Concept* flashed the message, "That's enough to prove my point." The virus' name, 'concept,' was probably an indicator that it was a proof of concept program for the macros virus. See Thomas Chen and Jean-Marc Robert, "The Evolution of Viruses and Worms," published in *Statistical Methods in Computer Security*, W.S. Chen, ed., (Boca Raton, Florida: CRC Press, 2004) http://vx.netlux.org/lib/atc01.html (accessed March 21, 2011).

26. G Data Software AG, *History of malware: A brief history of viruses, worms and Trojans*; Chen and Robert, "The Evolution of Viruses and Worms"; BitDefender, *Malware History*, 34-37.

27. *Melissa* was another evolution, having both virus and worm capabilities: It infected Word documents, then sent itself as an e-mail message to 50 addresses in the *Outlook* address book. It not only had a high infection rate, the increased e-mail traffic caused a large number of large corporations' mail servers to crash. It took complete advantage of the fact that *Outlook* had become the industry standard for sending email. See BitDefender, *Malware History*.

28. *BubbleBoy* used a security hole in Internet Explorer that automatically executed Visual Basic Script (VSB) embedded in the body of an e-mail message. The virus arrived as email with the subject "BubbleBoy is back." The message contained an embedded HTML file carrying the viral VBS. When read with *MSOutlook*, the script would run even if the message was only previewed. See Chen and Robert, "The Evolution of Viruses and Worms."

29. *Naked* is a mass mailing worm that disguises itself as flash movie. The attachment is named NakedWife.exe. This worm, after it has attempted to email everyone in the Microsoft Outlook address book, will attempt to delete several system files. This will leave the system unusable, requiring a re-install. See *W32. Naked@mm*, Symantic.com, http://www.symantec.com/security_response/ writeup.jsp?docid=2001-030617-1231-99 (accessed April 7, 2011).

    *LoveLetter* came via email disguised as an anonymous love letter with instructions to run an attached virtual basic script (.vbs) file for details on the sender. The .vbs-based virus would email itself to every person in the Microsoft Outlook address book and, once installed, replacing files with set extensions (e.g., vbs, vbe, js, jse, css, wsh, sct, hta, jpg, jpeg, mp3, mp2) with its own copies. The infection affected local hard-drives and all mapped network drives. Last, LoveLetter would attempt to download WIN-BUGSFIX.exe, a password-

cracking utility that steals passwords from the entire network, and then send the data to the Philippines. See BitDefender, *Malware History*, 44-45.

*Koobface* sets up an infected computer as part of a botnet, then installs a collection of different components that each perform a different task: a downloader, social network propagation, web server, ads pusher and rogue antivirus installer, CAPTCHA breaker, data stealer, web search hijackers, and rogue Domain Name System (DNS) changer. While most malware put all their functionalities into one file, *Koobface* divides each capability into different files that downloaded separately from a command & control center and then work together. Generally, *Koobface* relies on social engineering in order to spread through social networking sites, most prevalently through Facebook.com, tricking recipients into accepting the installation of malware disguised as a video codec or Flash update. For cybercriminals, Koobface represents a new shift in virus propagation, from desktop-based applications to web-based ones, particularly targeting social networking sites. See Jonell Baltazar, Joey Costoya, Ryan Flores, The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained, (Trend Micro Threat Research, July 2009) http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf (accessed March 20, 2011); Nart Villeneuve, KOOBFACE: Inside a Crimeware Network, Infowar Monitor, November 12, 2010, http://www.infowar-monitor.net/reports/iwm-koobface.pdf (accessed March 21, 2001).

30. Social engineering is a way for unauthorized persons to gain access to a computer or network. It relies on weaknesses in physical security rather than software, exploiting people's ignorance of proper information technology security. The purpose of a social engineering email is usually to secretly install spyware or other malicious software on the targeted person's computer or to trick the targeted person into handing over passwords or other sensitive information. See Microsoft Corporation, Microsoft Online Safety: What is social engineering?, http://www.microsoft.com/protect/terms/socialengineering.aspx (accessed March 21, 2011).

31. Cisco, *Cisco 2010 Annual Security Report*, (San Jose, California: Cisco Systems Incorporated, 2010), 19, http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html (accessed March 21, 2011).

32. Mell, Kent & Nusbaum, *Guide to Malware Incident Prevention and Handling*, 2-10; Alex Noordergraaf, *How Hackers Do It: Tricks, Tools, and Techniques* (Santa Clara, California: Sun Microsystems, Incorporated, May 2002), 2-10.

33. In September 2001, *Nimda* distributed an Internet worm which required no user interaction to activate or propagate. *Nimba* used security loopholes in programs alongside emails. Numerous web servers were overloaded and shut down. See G Data Software AG, *History of malware: A brief history of viruses, worms and Trojans*.

34. *StormWorm*, or Small.DAM, was a trojan virus introduced into systems through social engineering. An email would invite computer users to read

breaking news about the severe January 2007 storms that caused havoc in Europe, as well as several other shocking events around the globe. The *StormWorm* was rootkit enabled and downloaded files from various remote IP addresses and executes those files on the local system. See *W32.Storm. Worm*, Symantic.com, http://www.symantec.com/security_response/writeup.jsp?docid=2001-060615-1534-99 (accessed April 7, 2011).

35. Mobile code is software transferred between systems, or across a network, or via a USB flash drive and executed on a local system without explicit installation or execution permission by the recipient. Examples of mobile code include scripts (e.g., JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave, and macros embedded within Microsoft Office documents. See Wayne A. Jansen, Theodore Winograd, Karen Scarfone, *Guidelines on Active Content and Mobile Code*, Special Publication 800-28, (Gaithersburg, Maryland: National Institute of Standards and Technology, March 2008), ES1-ES2, http://csrc.nist.gov/publications/nistpubs/800-28-ver2/SP800-28v2.pdf (accessed March 25, 2011).

36. BitDefender, *Malware History*, 48 & 55.

37. Bots are distributed by hackers to infect a computer system. Once a machine is infected, the code then installs a bot program, making the machine a "zombie." This means that the computer can now receive commands and be controlled by another user through Internet Relay Chat (IRC) channels, which are a type of real time communication enabled over the Internet. The infected machine then contacts a pre-programmed IRC channel to wait for commands from the bot operator. Multiple machines that are infected with this malware will contact the channel, creating a botnet, or network of zombie machines. The spread of bot malware enables its operator to engage in a wide range of cybercrimes, including the distribution of spam, phishing, and secondary malware distribution. Botnets can also be used to perform cyber attacks in the form of Distributed Denial of Service (DDoS) attacks, where each computer in the network attempts to contact a computer or server until the target system becomes flooded with requests and cannot handle the volume, resulting in a loss of services to users. Evidence suggests the number of nodes in a botnet can reach hundreds of thousands of machines depending on the operator. See Bill Chu, Thomas J. Holt, Gail Joon Ahn, *Examining the Creation, Distribution, and Function of Malware On-Line* (Washington, D.C.: U.S. Department of Justice, March 2010), 15-16, www.ncjrs.gov/pdffiles1/nij/ grants/230111.pdf (accessed March 21, 2011).

38. The original variants of *Koobface* were first noticed around May or June of 2008. Koobface sent linked-message to Facebook and MySpace users with message bodies like, 'You should watch my latest video' or 'Watch my newest video'. The message and the domain of the hyperlink were hard coded within the body of the worm. For cybercriminals, *Koobface* represents a new shift in virus propagation, from desktop-based applications to web-based ones,

particularly targeting social networking sites. Since its first discovery, *Koobface* has been removed nearly 200,000 times from over 133,677 computers in more than 140 different locales around the world. There are an estimated 20,000 different variations of Koobface. See Baltazar, Costoya & Flores, *The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained*; Jonell Baltazar, *Web 2.0 Botnet Evolution: KOOBFACE Revisited* (Trend Micro Threat Research, May 2010) http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tweb_2_0_botnet_evolution__koobface_revisited__may_2010_.pdf, (accessed March 20, 2011).

39. A U.S. Department of Justice research report found that stolen data was sold on 10 public web-forums in Eastern Europe and Russia "designed to facilitate the creation, sale, and purchase of malware and hacking." For sale were malware log files containing personal information from victim computers, such as usernames, passwords, account information, and PayPal and Internet casino accounts, the latter two sold at an average of $156.79 per account. Credit card numbers were sold in bulk lots at an average price of $10.66 per card. Scanned passports and other identity documents were sold as means to engage in other forms of fraud. See Chu, Holt & Ahn, *Examining the Creation, Distribution, and Function of Malware On-Line*, 6-8.

40. G Data Software AG, *History of malware: A brief history of viruses, worms and Trojans*; Chu, Holt & Ahn, *Examining the Creation, Distribution, and Function of Malware On-Line*.

41. Plonk and Carblanc, *Malicious Software (Malware): A Security Threat to the Internet Economy*, 39, 40-41.

42. U.S. Government Accountability Office, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats* (Washington, DC: U.S. Government Accountability Office, June 2007), 4-9; Peter D. Gasper, "Cyber Threat to Critical Infrastructure 2010-2015," *The Nexus*, vol. 2/1 (February 24, 2009): 2-3.

43. Plonk and Carblanc, *Malicious Software (Malware): A Security Threat to the Internet Economy*, 39, 42-43.

    The *SQL Slammer* was designed to exploit an unpatched vulnerability in the Microsoft SQL server software. On January 25, 2003, it globally infected hundreds of thousands of computers in span of only a few minutes. The rapid and violent increase in network traffic caused some parts of the Internet infrastructure to completely crash. *SQL Slammer* had no payload – it appears that it was a proof of concept, to see how fast a small, simple worm could spread. See BitDefender, *Malware History*; Chen and Robert, "The Evolution of Viruses and Worms."

44. Nye, Cyber Power, 3-7; Miller and Kuehl, "Cyberspace and the "First Battle" in 21st-century War," 2-3; U.S. Congress, House of Representatives, House Permanent Select Committee on Intelligence, *Paul B. Kurtz: Cyber Security*

*Hearing*, 110th Cong., 2nd sess., September 19, 2008, 7-9, http://www.fas.org/irp/ congress/ 2008_hr/091808kurtz.pdf (accessed March 21, 2011).

The White House had a similar close call. A buffer overflow vulnerability in Microsoft's *Windows NT* and *Windows 2000* Internet Information Server web servers was announced in June 2001. In July, the *Code Red* worm was observed exploiting this vulnerability. *Code Red* randomly scanned internet provider addresses on the standard port for Internet connections and transmitted a Trojan which, between the 20th and 27th of a month, would have launched a denial of service attack against the White House website. Damage to affected systems was estimated at $2 billion. An ad hoc collaboration of government and industry blocked the worm's traffic and removed the virus. See G Data Software AG, *History of malware: A brief history of viruses, worms and Trojans*; Brian Krebs, "A Short History of Computer Viruses and Attacks," *Washington Post*, February 14, 2003, http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26, (accessed March 25, 2011).

45. Noah Shachtman, "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack," *Wired.com*, August 25, 2010, http://www.wired.com/dangerroom/tag/operation-buckshot-yankee (accessed March 21, 2011); William J Lynn III, "Defending a New Domain," *Foreign Affair*s, vol. 89, no. 5 (September/October 2010), 97-109, in ProQuest (accessed March 21, 2011).

46. The *Stuxnet* worm differs from previous malware in that it has a specific, damaging goal: to traverse to industrial control systems so it can reprogram the programmable logic controllers (PLCs), possibly disrupting industrial operations. Stuxnet seems to have been designed to deflect remediation and response actions from security professionals. *Stuxnet* can traverse non-networked systems, which means that even systems unconnected to networks or the Internet are at risk. "*Stuxnet* bears watching in 2011 because it breaks the malware mold," advises Kurt Grutzmacher, network consulting engineer at Cisco. "Malware that is designed to disrupt industrial control systems in critical infrastructure should be a concern for every government." Cisco, *Cisco 2010 Annual Security Report*, (San Jose, California: Cisco Systems Incorporated, 2010), 3, 21-22, http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html (accessed March 21, 2011).

47. Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair*, April 2011, www.vanityfair.com/culture/features/2011/04/stuxnet-201104, (accessed April 1, 2011); Mark Clayton, "Stuxnet 'virus' could be altered to attack US facilities, report warns," *The Christian Science Monitor*, December 15, 2010, http://www.csmonitor.com/USA/2010/1215/Stuxnet-virus-could-be-altered-to-attack-US-facilities-report-warns (accessed accessed April 1, 2011).

48. Plonk and Carblanc, *Malicious Software (Malware): A Security Threat to the Internet Economy*, 30-51.

49. "Despite widespread education on the prevalence and danger of Internet threats, a recent survey found that just 58 percent of consumers said they had a

complete security suite. What's more, when the survey takers actually scanned their computers for the software they discovered that only 37 percent were fully protected. This means that nearly two-thirds of users were leaving themselves exposed and making it easier for the cybercrooks….In the last two years alone, seven million U.S. consumers – or one in 13 households – admitted to giving out their personal information to phishers – scammers who tricked them into revealing information by pretending to be legitimate companies or organizations. And now scammers are aiming attacks at social networks, where younger people in particular like to let their guard down and express themselves. Unfortunately, it's working. Another study shows that social networking users aged 18-24 have experienced a spike in fraud and data exposures compared to other groups." McAfee, *A Good Decade for Cybercrime: McAfee's Look Back at Ten Years of Cybercrime*, (Santa Clara, California: McAfee, Incorporated, 2010), 8. http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf (accessed March 21, 2011).

50. The *Chernobyl* virus (aka Spacefiller, CIH) caused a worldwide outbreak with thousands of infected computers in both homes and corporate environments. It originated in Taiwan, where Chen Ing-hau sent the virus to a local electronic list-serve where it spread via game servers. It erased Flash BIOS (basic input/output system), chips and the partition table of the hard drive so that the computer could no longer reboot. See BitDefender, *Malware History*, 38; G Data Software AG, *History of malware: A brief history of viruses, worms and Trojans*.

51. *LoveLetter* caused losses estimated between $5 to 10 billion. BitDefender, *Malware History*, 44-45.

52. The *AnnaKournikova* virus was an email attachment, promising digital pictures of the tennis star Ana Kournikova. Once downloaded, the virus emailed itself to every person listed in the victim's Microsoft Outlook address book. A relatively benign virus, computer security analysts believed it was written using a software "toolkit" that could allow inexperienced programmers to create new computer viruses. Krebs, "A Short History of Computer Viruses and Attacks."

53. Chen and Robert, "The Evolution of Viruses and Worms."

54. McAfee, *A Good Decade for Cybercrime: McAfee's Look Back at Ten Years of Cybercrime*, 3.

55. There is little likelihood of international cyber law in the near future. The United Nations has pursued an international treaty for more than 10 years through a series of conventions without achieving international consensus. The only international cyberspace treaty is Council of Europe's Convention on Cybercrime, in force since 2004, with 47 members, 10 of them non-European states. The Convention focuses on crime perpetrated through cyberspace: financial and identity theft, child pornography, and intellectual property. The European Council has lobbied for the UN to adopt the Convention as a global standard, however, China and Russia prefer a treaty which will give

governments more control over Internet content and some developing nations see it as written by and for developed nations. See Brian Harley, "A Global Convention on Cybercrime?" *Columbia Science and Technology Law Review*, March 23, 2010, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (accessed March 23, 2011); Mark Ballard, "UN rejects international cybercrime treaty," *ComputerWeekly.com*, 20 April 2010 http://www.computerweekly.com/Articles/2010/04/20/240973/UN-rejects-international-cybercrime-treaty.htm (accessed on March 23, 2011); Greg Masters, "Global cybercrime treaty rejected at U.N.," *SCMagazine*, April 23, 2010, http://www.scmagazineus.com/global-cybercrime-treaty-rejected-at-un/article/168630/ (accessed on March 23, 2011).

56. Colin S. Gray, "Continuity in Change, and Change in Continuity," *Parameters*, vol 40, no. 2 (Summer 2010): 6-8, 11-12. Colin S. Gray, "How Has War Changed Since the End of the Cold War," *Parameters*, vol 35, no. 1 (Spring 2005): 17, 19, 21 and 24.

57. *The Holy Bible*, New King James Version (Nashville, Tennessee: Thomas Nelson, Incorporated, 1982), 3.

# Section Two: Strengthening Defense Support of Civil Authorities

## Reforming Disaster and Emergency Response

1. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5170b(b).

2. Matt A. Mayer, "States: Stop Subsidizing FEMA Waste and Manage Your Own Local Disasters," *Backgrounder* No. 2323, Heritage Foundation, September 29, 2009. http://www.heritage.org/Research/HomelandSecurity/bg2323.cfm (accessed March 22, 2011).

3. U.S. Department of Homeland Security, "National Preparedness Guidelines," (Washington, D.C.: U.S. Department of Homeland Security, September 2007), 1. http://www.fema.gov/pdf/emergency/nrf/National_Preparedness_Guidelines.pdf (accessed March 22, 2011).

4. *The Federal Emergency Management Agency*, About FEMA, http://www.fema.gov/about/history.shtm (accessed March 22, 2011).

5. Ibid.

6. Ibid.

7. Keith Bea, "Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding," Congressional Research Service, March 16, 2010. Summary at http://assets.opencrs.com/rpts/RL33053_20100316.pdf (accessed March 22, 2011).

8. Ibid., 9.
9. *The Robert T. Stafford Disaster and Relief Emergency Assistance Act*, Public Law 93-288, 42 U.S.C. 5170b, Section 403(c).
10. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5187, Section 420.
11. Bea, "Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding," 9-10.
12. *The Federal Emergency Management Agency*, Fire Management Assistance Grant Program Details, at http://www.fema.gov/government/grant/fmagp/details.shtm.
13. Federal Disaster Declarations, http://www.fema.gov/news/disasters.fema?year =2007.
14. 2007 Fire Cost Threshold, http://www.fema.gov/government/grant/fmagp /2007_fct.shtm.
15. *Fire Management Assistance Grant Program Overview*. http://www.fema.gov/ government/grant/fmagp/index.shtm (accessed March 22, 2011).
16. Bea, "Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding," 10.
17. Ibid.
18. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5122, Section 102.
19. The gubernatorial request for a declaration is forwarded to the President through FEMA official. Only the President may issue a major disaster declaration. Code of Federal Regulations, Title 44: *Emergency Management Assistance*, Part 206.48, Factors Considered When Evaluating a Governor's Request for a Major Disaster Declaration. http://cfr.vlex.com/vid/206-considered-evaluating-governor-19833539 (accessed March 22, 2011).
20. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5122(2).
21. *The Federal Emergency Management Agency*, Federal Disaster Declarations – 2007, Disaster Declarations, http://www.fema.gov/news/disasters.fema? year= 2007 (accessed March 22, 2011).
22. Bea, "Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding," 10.
23. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5122, Section 102.
24. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5191(b).
25. Bea, "Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding," 11.

26. *The Federal Emergency Management Agency,* Federal Disaster Declarations, http://www.fema.gov/news/disasters.fema?year=2007 (accessed March 22, 2011).

27. Bruce R. Lindsay and Justin Murray, "Disaster Relief Funding and Emergency Supplemental Appropriations," Congressional Research Service, Report 7-5700, January 26, 2010. Summary at http://www.effectivepeacekeeping.org/sites/effectivepeacekeeping.org/files/04/Disaster%20Relief%20Funding%20and%20Emergency%20Supps%201.10.pdf (accessed March 22, 2011).

28. Bea, "Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding," 18.

29. Ibid., 18.

30. Lindsay and Murray, "Disaster Relief Funding and Emergency Supplemental Appropriations," 18.

31. *The Federal Emergency Management Agency,* Average Total Obligations by Year and by Declaration, http://www.fema.gov/government/grant/pa/stat2.shtm (accessed March 22, 2011).

32. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5170a, Section 402(5).

33. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5170b, Section 403(b).

34. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5170c, Section 404(a).

35. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5172, Section 406(b)

36. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5173, Section 407(d).

37. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5174, Section 408(g) and Section 408(h).

38. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5170, Section 401.

39. Jena Baker McNeill and Matt A. Mayer, "The Solution to FEMA's Budget Woes Is Not More Money," *WebMemo* No. 2875, Heritage Foundation, April 21, 2010, 1. http://www.heritage.org/research/reports/2010/04/the-solution-to-femas-budget-woes-is-not- more-money (accessed March 22, 2011).

40. Ibid., 1.

41. *The Federal Emergency Management Agency*, Disaster Search, at http://www.fema.gov/femaNews/disasterSearch.do?action=Reset (accessed March 22, 2011).

42. Matt A. Mayer, "States: Stop Subsidizing FEMA Waste and Manage Your Own Local Disasters," Heritage Foundation *Backgrounder* No. 2323, September 29, 2009, 4-7, at http://www.heritage.org/Research/HomelandSecurity/bg2323.cfm (accessed March 22, 2011).

43. Ibid., 4-7.

44. U.S. Department of Homeland Security, "Target Capabilities List: A Companion to the National Preparedness Guidelines," (Washington, D.C.: U.S. Department of Homeland Security, September 2007), Preface, http://www.fema.gov/pdf/government/training/tcl.pdf (accessed March 22, 2011).

45. Ibid., Preface.

46. Ibid., v.

47. Federal Emergency Management Agency, "FEMA Fact Sheet: National Planning Scenarios" http://www.fema.gov/pdf/media/factsheets/2009/npd_natl_plan_scenario.pdf (accessed March 22, 2011).

48. Ibid.

49. U.S. Department of Homeland Security, "Target Capabilities List: A Companion to the National Preparedness Guidelines," (Washington, D.C.: U.S. Department of Homeland Security, September 2007), Executive Summary, http://www.fema.gov/pdf/government/ training/tcl.pdf (accessed March 22, 2011).

50. Ibid.

51. *The Robert T. Stafford Act Disaster and Emergency Assistance Act*, Public Law No. 93-288, as amended, 42 U.S.C. 5170, Section 401.

## Homeland Security Regional Unity of Effort

1. Frances F. Townsend. *The Federal Response to Hurricane Katrina Lessons Learned* (Washington, DC: The White House, 23 February 2006), 53.

2. United States Constitution, Preamble.

3. Barrack H. Obama, *Presidential Study Directive-1* (Washington, D.C.: The White House, 23 February 2009), 1.

4. United States Congress, Senate, "Homeland Security and Governmental Affairs Committee Hearing; Earthquake Preparedness: What the United States can Learn from the 2010 Chilean and Haitian Earthquakes," Congressional Documents and Publications September 30, 2010, 2. http://www.proquest.com (accessed January 10, 2011).

5. United States Government, *National Planning Scenarios: Created for use in National, Federal, State, and Local Homeland Security Preparedness Activities, Version 20.1 Draft.* April 2005.

6. U.S. Congress, Senate, Homeland Security and Governmental Affairs Committee Hearing; "Earthquake Preparedness: What the United States can Learn from the 2010 Chilean and Haitian Earthquakes," 2.
7. U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Department of Defense, 20 March 2009), GL-11.
8. Ibid.
9. Federation of American Scientists Presidential Directives Home Page, http://www.fas.org/irp/offdocs/nspd/index.html (accessed 14 November 2010).
10. U.S. Department of Homeland Security, *National Response Framework* (Washington, DC: U.S. Department of Homeland Security, January 2008), i.
11. Congressional Research Service Report for Congress, *Presidential Directives: Background and Overview* (Washington D.C.: Congressional Research Service, November 26, 2008), 3.
12. George Bush, "Homeland Security Presidential Directive 5: Management of Domestic Incidents," 28 February 2003, http://www.dhs.gov.xabout/laws/gc_1214592333605.shtm. (accessed 8 Sep 2010).
13. Ibid.
14. Wikipedia: National Response Plan, http://en.wikipedia.org/wiki/National_Response_Plan (accessed February 5, 2011).
15. Bush, *Homeland Security Presidential Directive 5*.
16. Ibid.
17. Ibid.
18. Congressional Research Service Report for Congress, *Robert T. Stafford Disaster Relief and Emergency Assistance Act: Legal Requirements for Federal and State Roles in Declaration of an Emergency of a Major Disaster* (Washington D.C.: The Library of Congress, 16 September 2005), 1.
19. Bush, *Homeland Security Presidential Directive 5*.
20. Ibid.
21. Ibid.
22. George Bush, "Homeland Security Presidential Directive 8: National Preparedness," 17 December 2003, http://www.dhs.gov.xabout/laws/gc_1214592333605.shtm. (accessed 8 Sep 2010).
23. Tammi K. Franks, "Who's in Charge? How the Law Impacts Chain of Command in Regional Disaster Situations" 1, http://www.fitzhewlaw.com/Whitepapers/RegionalDisasterChainofCommandWhitePaper.pdf (accessed 10 October 2010).

24. U.S. Government Accountability Office, *FEMA Has Made Limited Progress in Efforts to Develop and Implement a System to Assess National Preparedness Capabilities* (Washington, DC: U.S. Government Accountability Office, October 29, 2010), 6.
25. Townsend. *The Federal Response to Hurricane Katrina Lessons Learned*, 52.
26. Ibid, 51.
27. Ibid, 53.
28. Ibid, 66.
29. Ibid, 2.
30. Franks, *Who's in Charge?*, 2.
31. Townsend, *The Federal Response to Hurricane Katrina Lessons Learned,* 66.
32. U.S. Congress, "The Bill of Rights," December 15, 1791, http://www. archives.gov/exhibits/charters/bill_of_rights_transcript.html (accessed 11 October 2010)
33. Townsend, *The Federal Response to Hurricane Katrina Lessons Learned*, 70.
34. Spencer Hsu, "DHS to Unveil New Disaster Response Plan; FEMA Will Regain Power; State, Local Input Included," *Washington Post*, January 19, 2008.
35. Ibid.
36. Obama, *Presidential Study Directive-1*, 2.
37. Stew Magnuson and Matthew Russling, "DHS Pilot Program to Focus on State Emergency Planning," *National Defense* 93, issue 663 (February 2009): 13, in ProQuest (accessed January 10, 2011).
38. Ibid.
39. U.S. Congress, Senate, "Homeland Security and Governmental Affairs Committee Hearing; Earthquake Preparedness: What the United States can Learn from the 2010 Chilean and Haitian Earthquakes."
40. Barack Obama, Executive Order 13528: *Establishment of the Council of Governors* (Washington, DC: The White House, 11 January 2010), 1.
41. George W. Bush. The National Strategy for *Homeland Security.* (Washington D.C.: The White House, 16 July 2002), vii.
42. U.S. Government Accountability Office, *FEMA Has Made Limited Progress in Efforts to Develop and Implement a System to Assess National Preparedness Capabilities* (Washington, DC: U.S. Government Accountability Office, October 29, 2010), 1.
43. Ibid, 6.
44. Ibid.

45. Disaster Preparedness Report Shows Modest Progress. *Congressional Documents and Publications,* October 15, 2010, 1. http://www.proquest.com/ (accessed January 10, 2011).

46. Barrack Obama. *National Security Strategy.* (Washington D.C.: The White House, May 2010), 19.

47. Homeland Defense and Civil Support Net Forum. Guy Gahres, "Quick NIMS Framework_flow_emac," https://forums.bcks.army.mil/CommunityBrowser.aspx?id=1243678&lang=en-us. (accessed December 22, 2010).

48. U.S. Department of Homeland Security, *Joint Field Office Activation and Operations, Interagency Integrated Standard Operating Procedure* (Washington, DC: U.S. Department of Homeland Security, Version 8.3, Interim Approval April 2006), 14.

49. Ibid.

50. U.S. Department of Homeland Security, *National Response Framework*, (Washington, DC: U.S. Department of Homeland Security, January, 2008), 55.

51. Ibid, 56.

52. Ibid, 57.

53. Ibid, 60.

54. Townsend, *The Federal Response to Hurricane Katrina Lessons Learned*, 17.

55. U.S. Department of Homeland Security, *National Response Framework*, 61.

56. Ibid, 62.

57. Whitaker, Alan G., Smith, Frederick C., & McKune, Elizabeth (2010). *The National Security Policy Process: The National Security Council and Interagency system.* (Research Report, October 8, 2010 Annual Update, Washington, D.C.: Industrial College of the Armed Forces, National Defense University, U.S. Department of Defense), 61.

58. Homeland Defense and Civil Support Net Forum. "DSCA 101 Briefing," https://forums.bcks.army.mil/CommunityBrowser.aspx?id=1191308&lang=en-us. (accessed December 22, 2010).

59. U.S. Congress, Senate, "Homeland Security and Governmental Affairs Committee Hearing; Earthquake Preparedness: What the United States can Learn from the 2010 Chilean and Haitian Earthquakes," 1.

60 . Ibid.

61. Ibid.

62. Franks, *Who's in Charge?*, 4.

63. Whitaker, Smith, & McKune, *The National Security Policy Process: The National Security Council and Interagency system*, 61.

64 Ibid.

65. Ibid.
66. Ibid.
67. Ibid.
68. U.S. Department of Homeland Security, *Joint Field Office Activation and Operations, Interagency Integrated Standard Operating Procedure*, (Washington, DC: U.S. Department of Homeland Security, Version 8.3, Interim Approval April 2006), 16.
69. Valery C. Keaveny, Jr., "Brigade C2 Trends at JRTC," briefing slides with commentary, Fort Polk, LA JRTC, May 2010.
70. Ibid.
71. U.S. Congress, Senate, "Hearing; Earthquake Preparedness," 5.
72. Ibid, 9.
73. Craig Fugate, "A Whole of Community Framework for Catastrophic Planning and Response," briefing slides, Washington DC, U.S. Department of Homeland Security, FEMA, September 10, 2010.
74. Townsend, *The Federal Response to Hurricane Katrina Lessons Learned*, 54.

## Military Police Mutual Aid and the Posse Comitatus Act

1. Griffin, Larry. Army report: Fort Rucker MPs in Samson after shooting a violation. *The Dothan Eagle,* October, 2009. http://www2.dothaneagle.com/dea/news/local/article/army_report_fort_rucker_mps_in_samson_after_shooting_a_violation/101682.
2. Ibid.
3. Young, Stephen, (2003). *The Posse Comitatus Act of 1878: A Documentary History.* William S. Hein & Co., Inc. Buffalo, NY: 451.
4. Coakley, R.W., (1988). *The Role of Federal Military Forces in Domestic Disorders, 1789-1878.* Government Printing Office, Center of Military History, Washington, DC.: 22.
5. Young, *The Posse Comitatus Act of 1878: A Documentary History,* 452.
6. Brinkerhoff, John. "The Posse Comitatus Act and Homeland Security." *The Leadership Journal* (Department of Homeland Security, February, 2002): 2. http://www.homelandsecurity.org/journal/Articles/Brinkerhoff possecomitatus.html.
7. Trebilcock, C.T. "The Myth of Posse Comitatus." *The Leadership Journal.* Department of Homeland Security, 2000: 11. http://www.homelandsecurity.org/journal/articles/Trebilcock.htm
8. Matthews, Matt. "The Posse Comitatus Act and the United States Army: A Historical Perspective." *Occasional Paper* 14, 2006. Combat Studies Institute Press, Fort Leavenworth, KS: 82.

9. Dunn, Michael. "History of Fire Fighting and Mutual Aid in America." Emergency Response Training, Inc. website. http://www.ertrescue.com/Article-TheHistoryofFireFighting.html.

10. U.S. Government, 2008. *National Response Framework.* Department of Homeland Security, January, 2008: 3. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

11. U.S. Government. National Incident Management System Introduction. (Department of Homeland Security, December, 2008): 1. http://www.fema.gov/emergency/nims/AboutNIMS.shtm.

12. U.S. Government. *Law Enforcement on Federal Installations*. DoDI 5525.5, 18 U.S.C. 1382, 2005: 1-8.

13. U.S. Government. *Security of DOD Installations*. Department of Defense Instruction 5200.8, 2005, with amendments 2010.

14. Brinkerhoff, John. "The role of federal military forces in domestic law enforcement title." *The Joint Center for Operational Analysis Journal*, December, 2004: 37. http://www.globalsecurity.org/military/library/report/call/call_10-16-ch11.htm.

15. U.S. Army Regulation 190-56, 2007. *Department of the Army Civilian Police*. Chapter 1: 1-3.

16. U.S. Code, Title 18, Part I, Chapter 67, Section 1835 (Posse Comitatus Act of 1878).

17. Ibid.

18. Matthews, Matt. "The Posse Comitatus Act and the United States Army: A Historical Perspective." *Occasional Paper* 14, 2006 (Combat Studies Institute Press, Fort Leavenworth, KS)

19. Young, *The Posse Comitatus Act of 1878: A Documentary History,* 438.

20. Coakley, *The Role of Federal Military Forces in Domestic Disorders, 1789-1878*.

21. Young, *The Posse Comitatus Act of 1878: A Documentary History*, 451.

22. Ibid.

23. Brinkerhoff, "The Posse Comitatus Act and Homeland Security," 4

24. Ibid.

25. Trebilcock, "The Myth of Posse Comitatus," 18.

26. U.S. Government Center for Law and Military Operations. *Domestic Operational Law Handbook 2009 for Judge Advocates*. July, 2009: 36. https://www.jagcnet.army.mil/8525751D00557EFF.

27. Ibid.

28. Brinkerhoff, "The Posse Comitatus Act and Homeland Security," 2.

29. U.S. Government Center for Law and Military Operations, *Domestic Operational Law Handbook 2009 for Judge Advocates,* 38.

30. Currier, Donald. *The Posse Comitatus Act: A Harmless Relic from the Post-Reconstruction Era or a Legal Impediment to Transformation?* Strategic Studies Institute Monograph, September, 2003: 19. http://www.carlisle.army.mil/ssi.

31. Ibid.

32. Ibid.

33. Trebilcock, "The Myth of Posse Comitatus," 2-3.

34. Ibid., 3.

35. Uniform Code of Military Justice. Joint Service Commission on Military Justice, Washington, DC., 2005.

36. Zink, Dennis. *Military Police Support*. Unpublished essay for Capella University, June, 2010. Available upon request.

37. Dunn, "History of Fire Fighting and Mutual Aid in America."

38. Ibid.

39. U.S. Government. *National Response Framework*, 23.

40. Reiss, Albert. "Police Organization in the Twentieth Century." *Crime and Justice Journal,* April, 1992, 32.

41. Ibid.

42. Homeland Security Presidential Directive-5. Management of Domestic Incidents. February, 2003. http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm#0.

43. U.S. Government, *National Response Framework.*

44. U.S. Government, *National Incident Management System Introduction.*

45. Buck, David, Trainor, James, and Aguirre, Benjamin. "A Critical Evaluation of the Incident Command System and NIMS" *Journal of Homeland Security and Emergency Management*, V.3, 2006, 27.

46. U.S. Code, Title 18, Part I, Chapter 67, Section 1835 (Posse Comitatus Act of 1878).

47. Winn, P. (2009). "Alabama Sheriff asked for MPs; Questions Army Investigation into Civilian Troop Use." *CNSNews.com* on-line journal, 19 March 2009. http://www.cnsnews.com/public/ content/article.aspx?RsrcID=45314

48. Zink, Dennis. *What I saw on July 4th*. Unpublished essay for Capella University, June, 2010, 2 (available upon request).

49. Winn, "Alabama Sheriff asked for MPs; Questions Army Investigation into Civilian Troop Use."

50. Griffin, L. (October 2009). Army report: Fort Rucker MPs in Samson after shooting a violation. *The Dothan Eagle.* http://www2.dothaneagle.com/

dea/news/local/article/army_report_fort_rucker_mps_in_samson_after_shooting_a_violation/101682.

51. U.S. Government Center for Law and Military Operations. *Domestic Operational Law Handbook 2009 for Judge Advocates*. July, 2009, 38. https://www.jagcnet.army.mil/8525751D00557EFF.

52. U.S. Government. *Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities*. FEMA 592, June, 2007. http://www.fema.gov/pdf/about/stafford_act.pdf.

53. U.S. Government. *Strategy for Homeland Defense and Civil Support*. Department of Defense, June 2005. http://www.defense.gov/news/Jun2005/d20050630homeland.pdf.

54. U.S. Government (2007). *National Strategy for Homeland Defense.* The National Homeland Security Council. http://www.dhs.gov/xlibrary/assets/nat_strat_homeland security_2007.pdf.

55. Ibid.

56. Ibid.

57. Posner, Richard A., "Precise: The Constitution in a Time of National Emergency." Published in the National Security and Constitutional Law section of the Israel Law Review. Volume 42, Issue 217 (2009), 217-224.

58. Brinkerhoff, "The role of federal military forces in domestic law enforcement title."

59. Louden, Robert. *Who's in Charge Here? Some Observations on the Relationship Between Disasters and the American Criminal Justice System*. Unpublished paper for Georgian Court University, 2006, www.georgian.edu.

60. Ibid.

61. Brinkerhoff, "The role of federal military forces in domestic law enforcement title."

62. Kennebock. J. USAMPS Legal training for MPs, United States Army Military Police School, Fort Leonard Wood, Missouri. Date unknown. Available upon request.

63. U.S. Government. *Security of DOD Installations*. Department of Defense Instruction 5200.8, 2005 with amendments 2010.

64. U.S. Army Military Police School, *Military Police Corps Regimental History*, 1986.

65. U.S. Army. Military Police School Law Enforcement Legal Training, 2010, unpublished. (Available upon request).

66. Ibid.

67. Ibid.

68. U.S. Government. *Field Manual 3-19.4 Military Police Leaders Handbook*. GPO, 2002.

69. Currier, Donald. "The Posse Comitatus Act: A Harmless Relic from the Post-Reconstruction Era or a Legal Impediment to Transformation?" Strategic Studies Institute Monograph, September, 2003, 19. http://www.carlisle.army.mil/ssi.

70. Louden, Robert. *Who's in Charge Here? Some Observations on the Relationship Between Disasters and the American Criminal Justice System*. Unpublished paper for Georgian Court University, 2006, www.georgian.edu.

71. Currier, "The Posse Comitatus Act," 19.

72. U.S. Government. *Pentagon Force Protection Agency Regulation No. 9101 – Limited Statutory Authority and Jurisdiction* (Department of Defense, September, 2008), 1-18.

73. U.S. Government. *Designation & Physical Protection of DoD High Risk Personnel DoDi 0-2000.22.* (Controlled document – dated January, 2008, Change 1, July, 2008).

74. Elsea, Jennifer. *The Posse Comitatus and Related Issues: A Sketch*. CongressionalResearch Service Report, 2005. http://www.history.navy.mil/library/online/posse%20comit.htm#apply.

75. Becraft, Larry. "Federal Jurisdiction," *The Dixieland Law Journal*, 2011, http://home.hiwaay.net/~becraft/

76. Ibid.

77. Personal Interview with Brigadier General Michael Richie, National Guard Joint Task Force Katrina Commander, 2005. Recorded December 2010.

78. Ibid.

79. Ibid.

80. U.S. Government, *National Incident Management System Introduction,* 1.

81. U.S. Government, *National Response Framework.*

82. Currier, "The Posse Comitatus Act" 19.

83. Bolgiano, David. 2001 military support to civilian LE – working within the PCA. December 2001 FBI Law Enforcement Bulletin. http://www2.fbi.gov/publications/leb/2001/december2001/dec01p16.htm.

84. Elsea, *The Posse Comitatus and Related Issues: A Sketch*.

85. Ibid.

86. Ibid.

87. Ibid.

88. Ibid.

89. Banks, William. "Troops Defending the Homeland: The Posse Comitatus Act and the Legal Environment for a Military Role in Domestic Counter Terrorism." *Terrorism and Political Violence Journal*, Volume 14, No. 3, Autumn, 2002. http://web.ebscohost.com. library.capella.edu

90. Brinkerhoff, "The Posse Comitatus Act and Homeland Security," 2.

## Contingency Dual Status Commander: Balancing Title 10 and 32 Responsibilities

1. Alice R Buchalter, *Military Support to Civil Authorities: The Role of the Department of Defense in Support of Homeland Defense* (Federal Research Division, Library of Congress, Washington D.C., February 2007): 2.

2. Joint Chiefs of Staff, *Joint Publication 5-0, Joint Operation Planning* (Washington D.C., 26 September 2006): III-17.

3. Matt Mathews, *The Posse Comitatus Act and the United States Army: A Historical Perspective* (Combat Studies Institute Press, Fort Leavenworth, KS, 2006): 5.

4. Ibid.

5. Ibid., 33.

6. Ibid., 41-42.

7. Ibid., 42.

8. Sean McGrane, "Katrina, Federalism and Military Law Enforcement: A New Exception to the Posse Comitatus Act," *Michigan Law Review* 108, no. 7, May 1, 2010: 1321.

9. U.S. Constitution, art I, cl. 15.

10. Mathews, *The Posse Comitatus Act and the United States Army: A Historical Perspective,* 7.

11. Daniel Crockett, *The Insurrection Act and Executive Power to Respond with Force to Natural Disasters*, 5. http://www.law.berkley.edu/library/disasters/Crockett.pdf (accessed November 11, 2010).

12. Thaddeus Hoffmeister*, An Insurrection Act for the 21st Century*: 12-15. http://works.bepress.com/thaddeus_hoffmeister/6/ (accessed November 11, 2010)

13. Mathews, *The Posse Comitatus Act and the United States Army: A Historical Perspective*, 12.

14. Hoffmeister*, An Insurrection Act for the 21st Century*, 14-15.

15. Ibid., 21-24.

16. Law Brain, *Disaster Relief,* http://lawbrain.com/wiki/Disaster_Relief (accessed December 12, 2010).

17. Jason David Rivera and DeMond Shondell Miller, *A Brief History of the Evolution of United States' Natural Disaster Policy*, Journal of Public Management and

Social Policy,. vol. 12, is. 1 (2006). http://www.jpmsp.com/volume12issue1 (accessed December 18, 2010).

18. Federal Emergency Management Agency, *Robert T. Stafford Disaster Relief and Emergency Assistance Act P.L. 93-288, as amended*, FEMA PowerPoint Briefing, http://www.ncs.gov/tpos/esf/homestead/3%20-%20Bearden-Stafford%20Act.ppt (accessed December 18, 2010)

19. McGrane, *Katrina, Federalism and Military Law Enforcement: A New Exception to the Posse Comitatus Act*, 1324-1325.

20. Elizabeth C. Borja, *Brief Documentary History of the Department of Homeland Security 2001-2008* (History Associates Incorporated for U.S. Department of Homeland Security History Office, Washington D.C., 2008): 12.

21. Federal Emergency Management Agency, *FEMA History*, http://www.fema.gov/about/history.shtm (accessed November 13, 2010).

22. Borja, *Brief Documentary History of the Department of Homeland Security 2001-2008*, 25.

23. 109th U.S. Congress, *John Warner National Defense Authorization Act for Fiscal Year2007,* H.R. 5122 (Public Law 109-364, Washington D.C., October 17, 2006): 2404-2405.

24. 110th U.S. Congress, *National Defense Authorization Act for Fiscal Year 2008,* H.R. 4986 (Public Law 110-181, Washington D.C., January 28, 2008): 325-326.

25. Rivera and Miller, *A Brief History of the Evolution of United States' Natural Disaster Policy*, 5.

26. U.S. President, Executive Order January 11, 2010, *Establishment of Council of Governors*: 1. http://www.whitehouse.gov/sites/default/files/2010executive_order.pdf (accessed September 29, 2010)

27. *Contingency Dual-Status Commander Concept*, PowerPoint Briefing by U.S. Northern Command, November 2, 2010.

28. COL John T. Gereski, Jr. and LTC Christopher R. Brown, *Two Hats Are Better Than One: The Dual-Status Commander in Domestic Operations* (Army Law, June 2010): 72-73.

29. Gereski and Brown, *Two Hats Are Better Than One: The Dual-Status Commander in Domestic Operation,* 73.

30. *Contingency Dual-Status Commander Concept*, PowerPoint Briefing by U.S. Northern Command, November 2, 2010.

31. In a telephone conversation between LTC William J Prendergast and COL John T. Gereski, USNORTHCOM Director of Operations Law, concerning the Dual Status Commander Concept and Posse Comitatus, December 18, 2010. The barrier to command simultaneously is from U.S. Supreme Court, Perpich v. Department of Defense, 496 U.S. 334 (1990)

32. Prendergast and Gereski, TELCON. It is important to note that the design of DSC is to protect the Title 32 role in Posse Comitatus and not have a legal challenge and decision that places forces in a Title 32 Status under the Posse Comitatus Act as Title 10 forces.

33. John Goheen, "Historic Response," *National Guard Magazine*, Washington D.C., October 2005, Vol. 59, Is. 10, http://www.ngaus.org/content.asp?bid=982&False (accessed September 15, 2010).

34. In a conversation with LTC William J Edwards, who was assigned as the S-3 Air in the 41st eSB during the brigade's deployment to Hurricane Katrina.

35. Ibid.

36. *Contingency Dual-Status Commander Concept,* PowerPoint Briefing by U.S. Northern Command, November 2, 2010.

37. Carl Von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret. (Princeton, NJ: Princeton University Press, 1989): 119-121.

38. Headquarters, Department of the Army, *Field Manual 3-28 Civil Support Operations (Final Approved Draft)*, Washington D.C., June 29, 2010: 7-1 – 7-6. When compared to the USNORTHCOM Concept Brief.

39. Federal Emergency Management Agency, *About the National Incident Management System,* http://www.fema.gov/emergency/nims/AboutNIMS.shtm (accessed November 13, 2010).

40. U.S. Department of Homeland Security, *National Response Framework* (Washington D.C., January 2008): 11. http://www.fema.gov/NRF

41. Headquarters, Department of the Army, *Field Manual 3-28 Civil Support Operations (Final Approved Draft),* 2-1 – 2-2.

42. Federal Emergency Management Agency, *Incident Command System (ICS)* http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm#item3 (accessed November 14, 2010).

# Section Three: Border Security

## The Mexican Cartels and Jihadist Terrorism: The Nightmare Next Door

1. Charlie Savage & Scott Shane, "Iranians Accused of a Plot to Kill Saudis' U.S. Envoy," *New York Times,* October 12, 2011. In addition to the assassination of the Saudi Ambassador the arrangement called for embassy bombings in Washington and Venezuela, as well as offering a major opium deal.

2. Max G. Manwaring, *Insurgency, Terrorism, and Crime: Shadows from the Past and Portents for the Future* (Norman, Oklahoma: University of Oklahoma

Press, 2008): 112-113. Identifying domestic crime as Central America's biggest security threat. For a theoretical analysis on blending of "Immigration" and Security." See Didier Bigo, Migration and Security, *Controlling a New Migration World,* (New York: Routledge, 2001): 121.

3. See NORTHCOM Travel Advisory Subject: HQ USNORTHCOM FORCE PROTECTION DIRECTIVE 11-118 (MEXICO TRAVEL RESTRICTIONS) DTG: 281432Z Apr 11, at http://www. pacom.mil/web/PACOM_Resources/pdf/J34-NORTHCOM_FP_DIR_11-118_(Mexico_Travel _Restrictions)_281432Z_APR%2011.pdf.

4. Comparatively casualties for the same period in Iraq totaled 49,035. See http://icasualties.org/iraq/index.aspx. In Afghanistan totaled 7169; http://icasualties.org/OEF/index.aspx*and*http://www.guardian.co.uk/news/data blog /2010 /aug/10/afghanistan-civilian-casualties-statistics#zoomed-picture. Phillip Smith, "Mexican Drug War Update," December 7, 2011; and http://stopthedrugwar.org/topics/drug_war_issues/source_countries/mexican_drug_war (accessed December 14, 2011).

5. Michael Hoefer, Nancy Rytina, and Christopher Campbell, *Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2005* (Washington D.C.: Department of Homeland Security, 2006)

6. U.S. Government Accountability Office, "U.S. Assistance Has Helped Mexican Counternarcotics Efforts, but the Flow of Illicit Drugs into the United States Remains High" (Washington, D.C.: U.S. Government Accountability Office, October 2007) 2.

7. Douglas Farah, *Money Laundering and Bulk Cash Smuggling: Challenges for the Mérida Initiative* (San Diego: Woodrow Wilson International Center for Scholars, Mexico Institute, May 2010). See also Senators Dianne Feinstein, Charles Schumer and Sheldon Whitehouse, *Halting U.S. Firearms Trafficking to Mexico* (Washington D.C., United States Senate Caucus on International Narcotics Control, June 2011).

8. A complete analysis of each individual TCO is beyond the scopes of this article. They are generally labeled along geographical lines with the Gulf Cartel, The Sinaloa Cartel, The Juarez Cartel, and the Tijuana Cartel occupying most analysis. However, there are other non-geographically aligned Cartels such as La Familiar (The Family), and Los Zetas. Additionally certain Cartels are identified based on the founding leaders and are still referred to by those names, such as the Arellano Felix Organization (AFO) and the Beltran-Levya Organization (BLO). A definitive explanation of 1st through 3rd generation gangs can be found in Manwaring, *Insurgency, Crime and Terrorism*, 109.

9. "Jihadist" Is a general term used throughout this article to describe al Qaeda, its affiliates, Hezbollah, and other such Islamic fundamentalist who have evidenced an anti-U.S. position, coupled with violent action.

10. Sarah Womer & Robert J. Bunker, Surenos Gangs and Mexican Cartel Use of Social Networking Sites*, Small Wars & Insurgencies* 21, no. 1 ( March 2010): 81. A great report on the emerging similarities in Information Operations techniques between the TCOs and Jihadist terrorists.

11. Manwaring, *Insurgency, Terrorism, and Crime*, 108. See also note vi.

12. Richard H. Shultz Jr. & Andrea J. Dew, *Insurgents, Terrorist, and Militias: The Warriors of Contemporary Combat* (New York: Columbia University Press, 2006). This publication provides an overall treatise on the nature of emerging non-state armed groups.

13. Richard A. Clark, *Recreating our Borders, The Forgotten Homeland,* (Washington D.C.: Century Foundation Press, July 2006): 213, for details regarding the ability of Jihadist to cross the U.S. Cartel at governed checkpoints, let alone ungoverned. Also see page 215 for details on the 150,000 "Other-than Mexican" (OTMs) illegal's that that cross the southwestern border each year.

14. John P. Sullivan & Robert J. Bunker, Drug Cartels, *Small Wars & Insurgencies* 13, no. 2 (Special Issue 2002): 45-53, quoted in Manwaring, *Insurgency, Terrorism, and Crime*, 117. Which capstones the emergence of the terror-narco irregular fighter, a condition known as the "Sullivan-Bunker" Cocktail, in this passage: "If the irregular attacker-criminal gangs, terrorist, insurgents, drug cartels, militant environmentalist, or a combination of the above-blends crime, terrorism, and war, he can extend his already significant influence. After embracing advanced technology weaponry, including weapons of mass destruction (including chemical and biological agents), radio frequency weapons, and advance intelligence gathering technology, along with more common weapons systems, the attacker can transcend drug running, robbery, kidnapping, and murder and pose a significant challenge to the nation-state and its institutions. Then, using complicity, intimidation, corruption, and indifference, the irregular attacker can quietly and subtly co-opt individual politicians and bureaucrats and gain political control of a given geographical or political enclave. Such corruption and distortion can potentially lead to the emergence of a network of government protection of illicit activities and the emergence of a virtual criminal state or political entity. A series of networked enclaves could then, become a dominant political actor within a state or group of states. Thus, rather than violently competing directly with a nation-state, an irregular attacker can criminally co-opt and begin to seize control of the state indirectly."

15. Alternatively known as an Ungoverned Area. Robert D. Lamb, *Ungoverned Areas and Threats From Safe Havens, Final Report of the Ungoverned Areas Project* (Washington D.C.: Office of Deputy Assistant Secretary of Defense for Policy Planning, 2008): 15. A complete report and synopsis on Safe Havens is beyond the scope of this article. Suffice it to say that Safe Havens and counter-measures against them will be of critical importance to security professionals in the

coming decades. To learn more about them read *Ungoverned Areas and Threats from Safe Havens* and *Ungoverned Territories* cited below.

16. Angel Rabasa and John E. Peters, Dimensions of Ungovernability, & Dimensions of Conduciveness, *Ungoverned Territories: Understanding and Reducing Terrorism Risk* (Santa Monica, CA: Rand Corp. 2007): 7.

17. Manwaring, *Insurgency, Terrorism, and Crime*, 118.

18. Ibid. Also, Shahram Khosravi, *Illegal Traveler* (Hampshire, England: Palgrave Macmillan, 2010): 19-20.

19. David H. Petraeus, Gen. & James F. Amos, LTG., eds., *The U.S. Army Marine Corps Counter-Insurgency Field Manual* (Chicago, University of Chicago Press, 2007)

20. As an example, the situation got so bad that a 20-year-old college girl, Marisol Valles Garcia, was made Police Chief of Guadalupe Distrito Bravo, Mexico. "20-year-old woman student is police chief of violent Mexican town," October 20, 2010, *NDTV*, http://www.ndtv.com/article/ world/20-year-old-woman-student-is-police-chief-of-violent-mexican-town-61051 (accessed October 1, 2011). Her tenure ended with her seeking political asylum in the United States within five months. "Young Mexican police chief Marisol Valles Garcia may seek US asylum." March 5, 2011, *The Christian Science Monitor,* http://www.csmonitor.com/World/2011/0305/Young-Mexican-police-chief-Marisol-Valles-Garcia-may-seek-US-asylum (accessed October 1, 2011).

21. Manwaring, *Insurgency, Terrorism, and Crime*, 124. For a brief and excellent report on such see the TV news magazine Vanguard's special "Narco Wars Next Door" at http://current.com/shows/vanguard/video/.

22. Jason Lange, "From spas to banks, Mexico economy rides on drugs," Jan 22, 2010 linked from *Reuters,* http://www.reuters.com/article/2010/01/22/us-drugs-mexico-economy-idUSTRE60L0X120100122. This distorted economy occurs when grossly disproportionate drug profits allow narco-traffickers to overtake the legitimate economy creating a dependence on them by legitimate business people. The narco-economy creates an artificial consumer pattern; evidenced by disposable, luxury-type goods and affluent lifestyles out of place with cultural and social norms. This is further exasperated by hyper-inflation resulting from the ready amounts of "drug-cash" and the ever present cycle of ultra-violence that bars legitimate economic development from occurring. An American example can be found within the Rio Grande Valley in Texas.

23. Ibid.

24. Manwaring, *Insurgency, Terrorism, and Crime*, 105-109. Identifying the need for TCOs to replace the State. At this point the only remedy would be a complete full-scale counterinsurgency campaign or alternatively the unacceptable option of using first-world military technology upon the population – think Chechnya.

25. Womer, Surenos Gangs," 81. For a synergy of MS 13 and AQ. Manwaring, *Insurgency, Terrorism, and Crime*, 113-119. For the role of MS 13 and MS 18 in El Salvador.

26. Mark Krokorian, *The New Case Against Immigration: Both Legal and Illegal,* (New York: Penguin, 2008): 112.

27. Robert Maril, *Patrolling Chaos* (Lubbock, Texas: Texas Tech University Press, 2004): 269.

28. Ibid., 113. Describing the case of Mahmoud Kourani, an advanced, well trained (counter-intelligence, and spy craft in both Iran and Lebanon) Hezbollah operative who was apprehended at the San Diego/Tijuana crossing point in the trunk of a car. As the enemy adapts his techniques, one has to wonder if the loss of such an operative has caused Jihadists to start using foot movement within the interior of the border. The Brownsville Texas area has been inundated with Other-Than-Mexicans.

29. Stephen Castle & Mark J. Miller, *The Age of Migration; International Population Movements in the Modern World,* (New York: The Guilford Press, 2009): 213.

30. Manwaring, *Insurgency, Terrorism, and Crime*, 109. *Supra* note viii.

31. Lisa J. Campbell, "Los Zetas: Operational Assessment," *Small Wars & Insurgencies*, 21, no. 1 (March 2010): 55.

32. Ibid., 75.

33. ABC News, "Border Patrol are Attacked," August 16, 2008. *YouTube.* http://www.youtube.com/watch?v=uUlhYkJVu0Q (accessed November 18, 2011).

34. Pamela L. Bunker, Lisa J. Campbell, & Robert J. Bunker, "Torture, Beheadings and Narcocultos," *Small Wars & Insurgencies*, 21, no. 1 (March 2010): 169.

35. Ibid., 165-168. *See* Robert Maril, *Patrolling Chaos*, 135. Providing a detailed description of the 1989 murder, beheading, and human sacrifice of American college student Mark Kilroy along the Mexican Atlantic coast in Matamoros/Brownsville. So prevalent were Saint Muerto symbols and tattoos that customs officials began using evidence of such as a tip-off that the suspect was engaged in TCO activities.

36. Campbell, "Los Zetas,"

37. Graham H. Turbiville, Jr., "Firefights, Raids, and Assassinations: Tactical Forms of Cartel Violence and their Underpinnings," *Small Wars & Insurgencies*, 21, no. 1 (March 2010): 133.

38. Ibid., 132.

39. Grupo Savant, *Los Zetas Threaten a Nation State: A Indications and Warning Analysis"* (Washington D.C.: Grupo Savant, 2011): 2. For a detailed deport on Los Zetas attempt to recruit members of the Kaibiles, the Guatemalan Special Forces. One of the toughest special operations forces in the world.

40. Ibid.

41. John P. Sullivan, "Counter-supply and Counter-violence Approaches to Narcotics Trafficking," 21, *Small Wars & Insurgencies*, 21, no. 1 (March 2010): 179. This provides a detailed description on TCO adaptability.

42. U.S. Department of Justice, *National Drug Threat Assessment 2011* (Johnstown, PA: National Drug Intelligence Center, 2011): 11. U.S. Department of Justice, *Attorney General's Report to Congress on the Growth of Violent Street Gangs in Suburban Areas 2011* (Johnstown, PA: National Drug Intelligence Center, April 2008) Appendix C, http://www.justice.gov/ndic/pubs27/27612/appendc.htm#Top (accessed October 1, 2011). U.S. Department of Justice, *National Drug Threat Assessment 2009* (Johnstown, PA: National Drug Intelligence Center, December 2008) http://www.justice.gov/ndic/pubs31/31379/TCOs.htm (accessed October 1, 2011). "Mexican TCOs are the greatest drug trafficking threat to the United States; they control most of the U.S. drug market and have established varied transportation routes, advanced communications capabilities, and strong affiliations with gangs in the United States." As an example the two most feared gangs in El Salvador (MS-13 and MS-18) originated from the streets of Los Angeles, where they successfully engaged in 1st generation gang activities. For many gang members eventual criminal convictions were followed with deportation back to El Salvador. Once in Central America, freed from advanced law enforcement interference, they were able to expand from 1st generation street gangs into 3rd generation TCOs (Manwaring, *Insurgency, Terrorism, and Crime*, 116). Such gangs "find themselves at the intersection of crime and war" performing as mercenaries for asymmetrical groups (Ibid, 120-122). Within Latin and South America the techniques used to counter TCOs range across law enforcement and military options. All most all have been thwarted.

43. Turbiville, "Firefights, raids, and assassinations" 127. *See also* Grupo Savant, Biweekly Intelligence Report 7311, (Washington D.C.: Grupo Savant, March 20 2011): 5.

44. Maarten van Delden, "La pura gringuez" The Essentials United States in Jose Agustin, Carlos Fuentes & Ricardo Aguilar Melantzon," *Mexico Reading the United States* (Nashville, Tennessee: Vanderbilt University Press, 2009) 154. This provides an excellent discourse on anti-Americanism among Mexican artist and intelligentsia. See Robert Maril, *Patrolling Chaos,* 137, for a detailed description of mutual racism along the Texas/Mexico Border.

## Securing the U.S. Southern Land Border: Enhancing the Interagency Effort

1. *Internet Encyclopedia of World Biography*, http://www.encyclopedia.com (accessed December 13, 2010).

2. Congressional Research Service, *Border Security: Key Agencies and Their Missions* (Washington, DC, Congressional Research Service, January 26, 2010): 1.
3. Ibid.
4. Ibid.
5. Ibid.
6. The Department of Homeland Security Home Page. http://www.dhs.gov (accessed September 30, 2010).
7. Ibid.
8. Congressional Research Service, *Border Security: Key Agencies and Their Missions* (Washington, DC, Congressional Research Service, January 26, 2010): 2.
9. Ibid., 2.
10. Ibid., 2.
11. Customs and Border Protection Home Page. http://www.cbp.gov (accessed January 14, 2011).
12. Office of Air and Marine Operations at www.cbp.gov (accessed December 15, 2010)
13. U.S. Immigration and Customs Enforcement, *Border Security and Immigration Enforcement Overview*. http://www. ice.gov (accessed December 15, 2010)
14. U.S. Immigration and Customs Enforcement, *Office of Investigations Homeland Security Investigations Fact Sheet*. http://www.ice.gov (accessed December 15, 2010)
15. Congressional Research Service (CRS), *Border Security: Key Agencies and Their Missions* (Washington, DC, Congressional Research Service, January 26, 2010): 3.
16. Transportation Security Administration web site. http://www.tsa.gov (accessed February 12, 2011)
17. CRS, *Border Security*, 5.
18. USNORTHCOM home page. http://www.northcom.mil (accessed December 15, 2010)
19. Ibid.
20. Ibid.
21. Ibid.,4.
22. Federal Emergency Management Agency home page. http://www.fema.gov (accessed February 12, 2011).
23. Congressional Research Service, *Securing America's Borders: The Role of the Military* (Washington, DC, Congressional Research Service, June 16, 2010), 3; and Title 14, United States Code, Section 89.
24. Ibid., 3, 4.

25. George W. Bush, *National Strategy for Homeland Security* (Washington, DC: The White House, October 2007): 1.
26. Ibid., and the *National Response Framework* (NRF), January 2008, DHS website. http://www.dhs.gov (accessed January 15, 2011).
27. Bush, *National Strategy for Homeland Security*, 4.
28. Various news articles and government statements.
29. Bush, *National Strategy for Homeland Security*, 9-11.
30. Various news articles including *CBS online*, *Los Angeles Times*, and Mexican government press releases.
31. Various news articles and DOD reports.
32. E.G. Austin, "How Dangerous is Arizona?" *The Economist*, http://www.economist.com (accessed on December 15, 2010).
33. Customs and Border Protection home page, U.S. Customs Today Newsletter, October 2002. http://www.cbp.gov (accessed January 14, 2011).
34. U.S. Department of Justice home page. http://www.justice.gov (accessed January 14, 2011).
35. Ibid.
36. Ibid.
37. Fact Sheet, Office of National Drug Control Policy, *High Intensity Drug Trafficking Area (HIDTA) Program*. http://www.whitehousedrugpolicy.gov (accessed January 14, 2011).
38. Ibid.
39. Excerpts from Secretary Napolitano's testimony before the Senate Committee on the Judiciary, "Oversight of the Department of Homeland Security," The Department of Homeland Security home page. http://www.dhs.gov (accessed September 30, 2010).
40. The Department of Homeland Security home page. http://www.dhs.gov (accessed September 30, 2010).
41. Ibid.
42. Ibid.
43. Ibid.
44. Ibid.
45. Ibid.
46. Ibid.
47. Ibid.
48. Ibid.

49. "Of Substance" press release from, ONDCP, Executive Office of the President of the United States, posted November 18, 2010. http://www.whitehouse.gov (accessed January 14, 2011).
50. White House Press Release, "U.S.-Mexico Border Security Policy: A Comprehensive Response & Commitment" (March 24, 2009, The White House) http://www.whitehouse.gov (accessed October 28, 2010).
51. "Of Substance BLOG," Executive Office of the President of the United States, ONDCP website, posted November 18, 2010 (accessed January 14, 2011).
52. Horst Rittel and Melvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences*, Vol. 4 (Elsevier Scientific Publishing Company Inc., Amsterdam, 1973) http://www.unidata.ucar.edu (accessed January 14, 2011).
53. National Incident Management System (December 2008), and National Response Framework (January 2008) http://www.dhs.gov (accessed January 15, 2011).
54. Ibid.
55. Ibid.
56. Ibid.
57. Agencies currently represented at EPIC include the Drug Enforcement Administration; Department of Homeland Security; Customs & Border Protection; Immigration & Customs Enforcement; U.S. Coast Guard; Federal Bureau of Investigation; Bureau of Alcohol, Tobacco, Firearms and Explosives; U.S. Secret Service; U.S. Marshals Service; National Drug Intelligence Center; Internal Revenue Service; U.S. Department of the Interior; National Geospatial–Intelligence Agency; U.S. Department of Defense; Joint Task Force–North; Joint Interagency Task Force–South; Texas Department of Public Safety; Texas Air National Guard; and the El Paso County Sheriff's Office. From DOJ website. http://www.doj.gov (accessed January 15, 2011).
58. CBP Press Release, *CBP Announces Arizona Joint Field Command*, http://www.cbp.gov (accessed February 14, 2011).
59. Ibid.

## U.S.-Mexico Security Cooperation: The Time to Act is Now

1. STRATFOR, "Mexican Drug Cartels: An Update" http://www.stratfor.com/print/162432?fn=3917412488 (accessed October 22, 2010).
2. William Booth, "In Mexico's Nuevo Laredo, drug cartels dictate media coverage," *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/01/AR2010080103481.html (accessed December 16, 2010).
3. National Drug Intelligence Center, *National Drug Threat Assessment 2010,* (Washington DC: U.S. Department of Justice, 2010): 1. http://www.justice.gov/ndic/pubs38/38661/38661p.pdf (accessed November 15, 2010).

4. Clare Seelke and June Beittel, *Mérida Initiative for Mexico and Central America: Funding and Policy Issues*, (Washington, DC: Congressional Research Service, 2009): 2. http://assets.opencrs.com/rpts/R40135_20100419.pdf (accessed October 20, 2010).
5. Embassy of Colombia, Plan Colombia: General Description, http://colombiaemb.org/index.php?option=com_content&task=view&id=82&Itemid=165 (accessed December 16, 2010).
6. Jennifer Jo Janisch, "Plan Colombia: A Model for Success?" WNET.orgProperties LLC. http://www.pbs.org/wnet/wideangle/blog/plan-colombia-a-model-for-success/6185/ (accessed December 16, 2010).
7. Shannon O'Neill, "Mexico – U.S. Relations: What's Next?" *Americas Quarterly* (Spring 2010): 69-70.
8. Jeffery Davidow, *The U.S. and Mexico: The Bear and the Porcupine* (Princeton, NJ, Markus Wiener Publishers, 2004): 18.
9. Terra, "México y Chile más inmunes ante presión EE.UU. por Iraq." http://www.noticias.terra.com/articulo/html/act137726.htm (accessed November 11, 2010).
10. The Americas Post, "Armies of Mexico, U.S.A. and Canada, plus other security forces in North America will join efforts in the war on drugs in Mexico," http://www.theamericaspostes.com/994/armies-of-mexico-u-s-a-and-canada-plus-other-security-forces-in-north-america-will-join-efforts-in-the-war-on-drugs-in-mexico (accessed December 16, 2010).
11. Mary Beth Sheridan, "Military Broadens U.S. Push to Help Mexico Battle Drug Cartels," *Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2010/11/09/AR2010110907297.html (accessed November 10, 2010).
12. In 2008, Congress recognized the need for separate focus; it created the Caribbean Basin Security Initiative (CBSI) for Haiti and the Dominican Republic and the Central America Regional Security Initiative (CARSI); the remainder of the Mérida Initiative applying to Mexico. See General Accountability Office, *MÉRIDA INITIATIVE: The United States has Provided Counternarcotics and Anticrime Support but Needs Better Performance Measures*, (Washington, DC: U.S. General Accountability Office, 2010): 5. http://www.gao.gov/new.items/d10837.pdf (accessed October 20, 2010).
13. Seelke and Beittel, *Mérida Initiative for Mexico*, 12.
14. Ibid.
15. Davidow, *The U.S. and Mexico*, 93-94.
16. Marc Lacey, "Mexico Still Waiting for U.S. Aid, Report Says," *New York Times*, http://www.nytimes.com/2009/12/04/world/americas/04mexico.html (accessed November 11, 2010).

17. RTTNews.com, "Modern U.S. Helicopters To Fight Drug-related Violence In Mexico." http://www.borderlandbeat.com/2010/11/modern-us-helicopters-to-fight-drug.html (accessed December 11, 2010).
18. Ken Ellingwood, "Once a conduit, now a consumer," *Los Angeles Times.* http://articles.latimes.com/2008/oct/15/world/fg-mexaddict15 (accessed November 15, 2010).
19. Laura Carlsen, "A Primer on Plan Mexico," *Scoop Independent News.* http://www.scoop.co.nz/stories/HL0805/S00074.htm (accessed September 29, 2010).
20. Joint Statement of Hillary Clinton and Patricia Espinosa, U.S. State Department. http://www.state.gov/secretary/rm/2010/03/139196.htm (accessed November 3, 2010).
21. Barack Obama, *National Security Strategy* (Washington, DC: Executive Office of the President, 2010): 14. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed November 3, 2010).
22. Bob Killebrew and Jennifer Bernal, *Crime Wars: Gangs, Cartels, and U.S. National Security* (Washington, DC: Center for a New American Security, 2010): 44. http://www.cnas.org/files/documents/publications/CNAS_CrimeWars_KillebrewBernal_3.pdf (accessed December 28, 2010).
23. O'Neill, "Mexico – U.S. Relations," 71.
24. Carlsen, "A Primer."
25. Frontline, WGBH Educational Foundation, "Thirty Years of America's Drug War: A Chronology" http://www.pbs.org/wgbh/pages/frontline/shows/drugs/cron/ (accessed November, 15, 2010).
26. Claire Suddath, "Brief History: The War on Drugs," *Time.* http://www.time.com/time/world/article/0,8599,1887488,00.html (accessed December 28, 2010).
27. Barack Obama, *2010 National Drug Control Strategy* (Washington, DC: Executive Office of the President, 2010): 6 and 109. http://www.whitehousedrugpolicy.gov/publications/policy/ndcs10/ndcs2010.pdf (accessed November 11, 2010).
28. U.S. Department of State, "ATF Fact Sheet: Project Gunrunner" http://www.usembassy-mexico.gov/eng/texts/et080116eTrace.html (accessed December 28, 2010).
29. Jerry Seper, "Gun Flow to Mexico Unabated," *The Washington Times.* http://www.washingtontimes.com/news/2010/nov/9/report-gun-flow-to-mexico-unabated/ (accessed December 11, 2010).
30. Mary Beth Sheridan, "Treaty to curb gun smuggling to Mexico remains stalled," *Washington Post.* http://www.washingtonpost.com/wp-dyn/content/article/2010/10/21/AR2010102106890.html (accessed October 22, 2010).
31. Shannon O'Neil, Prepared Statement before the Committee on Foreign Affairs: Subcommittee on the Western Hemisphere; and Committee on Homeland

Security: Subcommittee on Border, Maritime, and Global Counterterrorism, U.S. House of Representatives, Washington D.C. Hearing on "U.S.-Mexico Security Cooperation: Next Steps for the Merida Initiative," May 27, 2010. http://www.cfr.org/publication/22221/moving_beyond_merida_in_usmexico_security_cooperation.html (accessed October 20, 2010).

32. Carlsen, "A Primer."

33. Michael R. Gordon, "In Baghdad, Justice Behind the Barricades," *New York Times.* http://www.nytimes.com/2007/07/30/world/middleeast/30military.html?_r=1&emc=eta1 (accessed December 27, 2010).

34. Joint Statement of Hillary Clinton and Patricia Espinosa, U.S. State Department, http://www.state.gov/secretary/rm/2010/03/139196.htm (accessed November 3, 2010).

35. From Joint Pub 3-27: "The Security and Prosperity Partnership of North America is an agreement between the United States, Canada, and Mexico, established to identify new avenues of cooperation to make the continent safer and more secure, businesses more competitive, and economies more resilient." None of the three countries have expressed an interest in moving this initiative forward since the last meetings were held in August 2009. See The White House, "Joint Statement by President Bush, President Fox, and Prime Minister Martin." March 23, 2005. http://georgewbush-whitehouse.archives.gov/news/releases/2005/03/print/20050323-2.html (accessed December 17, 2010).

36. New Democratic Party of Canada, "Press Release: New Democrats celebrates victory over SPP" http://www.ndp.ca/press/new-democrats-celebrates-victory-over-spp#ixzz18OLwWG00 (accessed December 17, 2010); Philip Dine, "Urban Legend of 'North American Union' Feeds on Fears," *St. Louis Post-Dispatch*. http://seattletimes.nwsource.com/html/nationworld/2003713518_rumor19.html (accessed December 17, 2010).

37. U.S. Customs and Border Protection, "SNAPSHOT: A summary of CBP facts and figures" http://www.cbp.gov/linkhandler/cgov/about/accomplish/snapshot.ctt/snapshot.pdf (accessed December 17, 2010).

38. Joint Statement of Hillary Clinton and Patricia Espinosa, U.S. State Department, http://www.state.gov/secretary/rm/2010/03/139196.htm (accessed November 3, 2010).

39. Carlos Reyna Izaguirre, "Hard-Learned Lessons: Plan Colombia and Democracy in Peru" http://www.fpif.org/articles/hard-learned_lessons_plan_colombia_and_ democracy_in_peru (accessed December 27, 2010).

40. U.S. Agency for International Development, "Telling our Story: Creating a Road Map to a New Life," http://www.usaid.gov/stories/colombia/fp_col_julio.html (accessed December 27, 2010). Also of interest, the NGO Actuar por Bolívar was incorporated three years after its inception by Shell, ECOPETROL, and the Chamber of Commerce. See http://www.actuarporbolivar.org/entrada_ING.html (accessed December 27, 2010).

41. U.S. Agency for International Development, "Telling our Story: Farms Swap Coca Crop for Dairy Products" http://www.usaid.gov/stories/colombia/ss_co_dairy.html (accessed December 27, 2010).

42. Possible Cabinet-level Agencies include, but are not limited to: Defense, Education, Health and Human Services, Homeland Security, Interior, Justice, State, Transportation, Treasury, Veteran Affairs, and the Small Business Administration.

43. A listing of Appropriations Bills is located at: http://thomas.loc.gov/home/approp/app11.html (accessed November, 15, 2010).

44. Barack Obama, *Budget of the U.S. Government* (Washington, DC: Executive Office of the President, 2010): 4. http://www.whitehouse.gov/sites/default/files/omb/budget/fy2011/assets/message.pdf (accessed November 11, 2010).

45. Bob Kerrey, Mark Alderman and Howard Schweitzer, "Federal Government needs a chief operating officer," *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/04/AR2010110406882.html (accessed November 11, 2010).

46. Personal experience of the author while serving as the Senior Military Assistant to the Under Secretary of Defense for Comptroller, Office of the Secretary of Defense, from May 2009 to August 2010. For ARRA execution within the DoD, the Principal Deputy Under Secretary of Defense for Comptroller Michael McCord was designated the Senior Accountable Official for the Department of Defense; Lester A. Weilacher, e-mail message to author, December 17, 2010.

47. La Plaza, "Former Mexican President: Legalize Drugs," *Los Angeles Times*, http://latimesblogs.latimes.com/laplaza/2010/08/vicente-fox-legalization-drugs-mexico.html (accessed December 11, 2010).

48. Mothers Against Drunk Driving. http://www.madd.org/about-us/mission/ (accessed December 11, 2010). The Foundation for a Smoke-Free America. http://www.anti- smoking.org/theproblem.htm (accessed December 11, 2010).

49. Schaffer Library of Drug Policy, http://www.druglibrary.org/think/~jnr/12 reason.htm (accessed December 11, 2010); Jeffrey A. Miron and Katherine Waldock, "Making an Economic Case for Legalizing Drugs," *CATO Institute*, http://www.cato.org/pub_display.php?pub_id=12192 (accessed December 11, 2010).

50. Lance Winslow, Guaranteeing Workplace Safety in the Age of Legalized Drugs Considered. http://ezinearticles.com/?Guaranteeing-Workplace-Safety-in-the-Age-of-Legalized-Drugs-Considered&id=5301644 (accessed December 11, 2010).


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA


U.S. ARMY WAR COLLEGE
Carlisle Barracks, PA


CENTER for STRATEGIC LEADERSHIP
CSL