Nothing Virtual About It:

An Emerging Safe Haven for an Adaptive Enemy

A Monograph
by
MAJ David M. Williams Jr.
U.S. Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2010

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
12-10-2010

3. REPORT TYPE AND DATES COVERED
SAMS MONOGRAPH JAN 2010-DEC 2010

4. TITLE AND SUBTITLE
NOTHING VIRTUAL ABOUT IT: AN EMERGING SAFE HAVEN FOR AN ADAPTIVE ENEMY

5. FUNDING NUMBERS

6. AUTHOR(S)
Major David M. Williams Jr., United States Army

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

School of Advanced Military Studies
250 Gibbon Avenue
Fort Leavenworth 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved For Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

While it is no secret that Islamic terrorists utilize the internet, the assertion that the internet is a virtual safe haven more important than any geographical safe haven is rarely made. As a result of the expansion of the Internet capabilities over the last two decades and the loss and disruption of geographic safe havens worldwide, Islamic terrorists are now becoming all the more reliant upon the internet as a safe haven from which to recruit, finance, communicate, train, and survive to continue to conduct operations and further their cause. An examination of the geographical safe havens, the emergence of the Internet in warfare, and the adaptation of Al Qa'ida following 9/11, reveals how Al Qa'ida and other Islamic terrorist organizations have grown dependent on the Internet. A comparison between the capabilities that the Internet's cyberspace offers and what a geographic safe haven can provide suggests that in some functions the Internet is more effective and safer than physical space for Al Qa'ida and its affiliates. These conclusions lead to a discussion that the United States is ignoring a very real front in its efforts to "disrupt, dismantle, and defeat" al Qa'ida and its affiliates, Islamic terrorists enjoy operating on the internet with minimal disruption and risk to accomplish many of the same tasks that used to require geographical space to conduct.

14. SUBJECT TERMS
Internet, Safe Haven, Sanctuary, Al Qa'ida, Cyberterrorism
Islamic Terrorism, Jihad

15. NUMBER OF PAGES
57

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
(U)	(U)	(U)	(U)

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major David M. Williams Jr.

Title of Monograph: Nothing Virtual About It: An Emerging Safe Haven for an Adaptive Enemy

Approved by:

Daniel G. Cox, Ph.D. — Monograph Director

Joseph S. McLamb, LTC, IN — Second Reader

Wayne W. Grigsby, Jr., COL, IN — Director,
School of Advanced
Military Studies

Robert F. Baumann, Ph.D. — Director,
Graduate Degree
Programs

Disclaimer: Opinions, conclusions, and recommendations expressed or implied within are solely those of the author, and do not represent the views of the US Army School of Advanced Military Studies, the US Army Command and General Staff College, the United States Army, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Abstract

NOTHING VIRTUAL ABOUT IT: AN EMERGING SAFE HAVEN FOR AN ADAPTIVE ENEMY by MAJ David M. Williams Jr., U.S. Army, 57 pages.

While it is no secret that Islamic terrorists utilize the internet, the assertion that the internet is a virtual safe haven more important than any geographical safe haven is rarely made. As a result of the expansion of the Internet capabilities over the last two decades and the loss and disruption of geographic safe havens worldwide, Islamic terrorists are now becoming all the more reliant upon the internet as a safe haven from which to recruit, finance, communicate, train, and survive to continue to conduct operations and further their cause. An examination of the geographical safe havens, the emergence of the Internet in warfare, and the adaptation of Al Qa‘ida following 9/11, reveals how Al Qa‘ida and other Islamic terrorist organizations have grown dependent on the Internet. A comparison between the capabilities that the Internet‘s cyberspace offers and what a geographic safe haven can provide suggests that in some functions the Internet is more effective and safer than physical space for Al Qa‘ida and its affiliates. These conclusions lead to a discussion that the United States is ignoring a very real front in its efforts to —disrupt, dismantle, and defeat" al Qa‘ida and its affiliates, Islamic terrorists enjoy operating on the internet with minimal disruption and risk to accomplish many of the same tasks that used to require geographical space to conduct.

Table of Contents

Introduction

Whenever most politicians, political candidates, or military officers explain why the United States is still in Afghanistan nearly ten years after 9/11, almost without exception, they will refer to the need to prevent Afghanistan from being a sanctuary for Al Qa'ida again. This statement is mirrored in the *2010 National Security Strategy* (NSS). The 2010 NSS states that the United States is renewing its focus on Afghanistan as part of a commitment to ―disrupt, dismantle, and defeat al Qa'ida and its affiliates" and deny it from being a safe haven for them.[1] Additionally, the United States and its allies have the task of attempting to ―deny the Taliban the ability to overthrow the government, and strengthen the capacity of Afghanistan's security forces and government so that they can take lead responsibility for Afghanistan's future."[2] In Afghanistan, the United States is fighting an insurgency against a resurgent Taliban and elements of Al Qa'ida that for the better part of this decade has enjoyed a geographic safe haven in the autonomous tribal regions along the Pakistani and Afghan border. The Taliban and Al Qa'ida, have had time to recover, reset, recruit, and train for both regional insurgent operations and international terrorism within those safe havens with relative impunity up until recently.

The recent increased penetration by Pakistani Army forces and United States unmanned aerial vehicles (UAV) Predator drone strikes in Pakistan resulted in key senior leaders in Al Qa'ida and the Taliban being killed or captured and the disruption of their geographic safe havens. Within the last few years, attempted terrorist attacks within the United States have also brought more attention to other geographic safe havens Al Qa'ida and its affiliates utilize in the weak and failed states of Yemen and Somalia. Indeed, a major line of effort for this conflict against Al Qa'ida and its affiliates is the denial and disruption of terrorist sanctuaries, ―safe-havens", or ungoverned territorial space. Since the beginning of the so-called ―Global War on Terrorism," the United States has spent billions of dollars and lost thousands of American lives on preventing Al Qa'ida and its affiliates from establishing geographic safe

[1] U.S. President, *National Security Strategy*, (May, 2010): i.

[2] Ibid. 20

havens. Most of these billions in treasure have been spent on direct large-scale US occupations of Afghanistan and Iraq; however, billions have also been spent on Foreign Internal Defense (FID) assisting other nations with their own defense and development. FID helps prevent Al Qa‘ida and its affiliates from establishing safe havens in their countries through military, economic, diplomatic, and information means. In doing so, the United States and its allies have been relatively successful at denying, disrupting, and putting unrelenting pressure upon Islamic terrorists groups in ungoverned geographical spaces within the Middle East, Central and Southeast Asia, and Africa by means of direct military action, law enforcement, and FID operations. Despite this success, Al Qa‘ida and its affiliates, in many ways, appear stronger and more resilient than they did a decade ago. There has been an increasing number of ‗homegrown‘ Islamic terror attacks, foiled attacks, or arrests made within the US the past two years, which are inspired or even directed by Al Qa‘ida. How is this possible if Al Qa‘ida and its affiliate‘s safe havens, are shrinking under the weight of US and allied success in disrupting such safe havens?

Within the Information age, safe havens are so much more than simple geographical locations outside the reach of government authority within weak and failing states. Over the last decade, the massive expansion of the Internet has provided Islamic terrorists with another ungoverned space that they could exploit to conduct recruiting, online radicalization, propaganda, financing, internal command and control, offensive cyber-terrorism, and training. Despite the success of efforts in applying growing pressure on Al Qa‘ida and its affiliates‘ geographical safe havens, Islamic terrorists operate on the Internet with minimal disruption and risk to accomplish many of the same tasks they used to require geographical space to conduct.

While it is no secret that Islamic terrorists utilize the Internet, the assertion that the Internet is a virtual safe haven that has become increasingly more important than geographic safe havens to terrorists is rarely made. This monograph builds upon the research by David Gray and Albon Head. The context of Gray and Head‘s eight-page research paper discusses the importance of the Internet safe havens in comparison to geographic ones for terrorists in terms of the functions of communications, training, planning/coordination, fundraising, and recruiting.[3] This monograph seeks to assess if the Internet, as a safe haven, is more important to Al Qa'ida and its affiliates for its survival and operational functions than geographical safe havens.

Evidence addressing the research question and illustrating how important the Internet has become to Islamic terrorists came from a combination of primary sources, secondary, and tertiary sources. Primary sources included the terrorist websites themselves, United States military doctrine, official United States government documents, and an interview with a Department of the Army civilian specializing in how Islamic extremists are operating and networking online. Numerous secondary sources books and articles provided source documents to analyze ungoverned space, complex systems science, and social science theories regarding the Internet and Islamic terrorism. This research also includes some tertiary sources that provided some details into recent events involving online Islamic radicalization with ―homegrown" Islamic terrorists.

The monograph's research methodology is loosely based on a complex systems science framework as outlined in Alex Ryan's article ―The Foundation for an Adaptive Approach: Insights from the Science of Complex". This monograph seeks to demonstrate that Al Qa'ida is a complex adaptive system and describe how it emerged and adapted to survive in its complex new post 9/11 environment. This adaptation, in part due to the Internet, another complex adaptive system, provides a specific explanation behind the increasing migration from geographical to Internet safe havens as a sanctuary of Islamic extremism. This monograph begins with a detailed look at geographic safe havens. This provides a base of understanding to enable comparison in the final subsection between the capabilities provided by Internet and geographic safe havens. In between the comparison-based subsections, the monograph has a

[3] David Gray and Albon Head, ―The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven," *European Journal of Scientific Research* 25, no.3 (2009): 396-404.

subsection discussing the emergence of Al Qa'ida in the 1980s and 1990s and a subsection dedicated to Al Qa'ida's post 9/11 adaptation.

WHAT ARE SAFE HAVENS?

> Wherever al-Qa'ida or its terrorist affiliates attempt to establish a safe haven—as they have in Yemen, Somalia, the Maghreb, and the Sahel—we will meet them with growing pressure. We also will strengthen our own network of partners to disable al-Qa'ida's financial, human, and planning networks; disrupt terrorist operations before they mature; and address potential safe-havens before al-Qa'ida and its terrorist affiliates can take root. These efforts will focus on information-sharing, law enforcement cooperation, and establishing new practices to counter evolving adversaries. We will also help states avoid becoming terrorist safe havens by helping them build their capacity for responsible governance and security through development and security sector assistance.[4]
>
> – *National Security Strategy* (2010)

Weak and Failing States and other Safe Havens

Army Field Manual (FM) 3-0 *Operations* states that the ―problem of failed or failing states can result in the formation of safe havens in which adversaries can thrive."[5] Many of these failed or failing states provide ungoverned territory that are ripe for Al Qa'ida and its affiliates to utilize as safe havens. Angel Rabasa in *Ungoverned Territories* defines ungoverned territory as ―an area in which a state faces significant challenges in establishing control…[that] can be failed or failing states, poorly controlled land or maritime border, or areas within otherwise viable states where the central government's authority does not extend."[6] Some of the variables that Rabasa measures as potential indicators of ungoverned territories are the level of state penetration in society, the state's monopoly on the use of force, the state's control of the border, and the external influences by other states.[7] Rabasa admits, ―Not all ungoverned territories are equally suitable as terrorist sanctuaries or conducive to the presences of terrorist and insurgent groups," so

[4] U.S. President, *National Security Strategy*, (May, 2010): 21.

[5] U.S. Department of the Army, *Field Manual 3-0 Operations*, (Washington, DC: February 27, 2008): 1-3.

[6] Angel Rabasa et al., *Ungoverned Territories: Understanding and Reducing Terrorism Risks*. (Santa Monica, CA: Rand Corporation, 2007), xv.

[7]Ibid., xvii.

he adds additional variables under the dimension of conduciveness within the analytical framework.[8] Rabasa measures conduciveness with four variables: adequacy of infrastructure and operational access, availability of sources of income, favorable demographics, and invisibility.[9]

As stated in the 2010 NSS, Rabasa points out that the United States ―tends to emphasize security cooperation and military assistance in dealing with the security problems that ungoverned territories generate."[10] Rabasa recommends ten specific actions that the United States government takes to address the lack of effective states and conduciveness of these ungoverned territories to the presence of terrorist groups. The majority of these recommendations focus on promoting competent governance and penetration through infrastructure improvements; promoting regional security architectures and organizations; addressing state corruption; reducing terrorists‘ exploitation of infrastructure and assistance programs; and denying terrorists their local sources of income and invisibility.

Rabasa‘s approach mirrors many of the idealistic indirect approaches advocated to deny safe havens to Al Qa‘ida mentioned in the 2010 NSS. Many of Rabasa‘s recommendations are long-term expensive investments that some would label as ―nation building." Rabasa‘s ideas would perhaps be more palatable if it was 2001 again and the United States did not possess $13 trillion worth of debt and nine years of ―nation building" fatigue in Iraq and Afghanistan. Rabasa‘s over idealistic recommendations, within a few years, will likely be difficult to implement simply because of funding shortfalls. Rabasa also gives no credence to an adapting enemy operating in the information age and also that many of the recent terrorist attacks originate from the United States and Western Europe, not ungoverned territories. Despite this, the 2010 NSS outlines many of Rabasa‘s recommendations as an approach to deny safe havens to Al Qa‘ida and its affiliates.

[8] Ibid., xvi.

[9] Ibid.

[10] Ibid., xix.

Cristiana Kittner takes a similar stance as Rabasa on the conditions that are necessary for the establishment of a specifically Islamic terrorist safe haven. Kittner‘s theory is that ―geographic features, weak governance, history of corruption and violence, and poverty” establish the critical conditions that ―produce ideal circumstances that Islamist terrorists exploit to enhance their capabilities.”[11] For the purposes of her article, Kittner defines safe havens as ―geographical spaces where Islamist terrorists are able to successfully establish an organizational and operational base.”[12] This operational base may include one, some, or all of the following capabilities: Fundraising, a communications network for efficient command and control and intelligence gathering, operational space for training, and a ―logistical network to enable travel, the movement of money, the access to fraudulent documents, and weapons material.”[13] Interestingly enough, Kittner‘s theory is that the Tri-Border Area of South America where the frontiers of Argentina, Brazil, and Paraguay meet possesses the critical conditions that would make it an ideal sanctuary for Islamic terrorists. She also provides evidence that Islamic terrorists are actually utilizing it as a sanctuary, very far from where one would think Islamic extremists would possess a geographic safe haven. Kittner suggests similar approaches to Rabasa in eliminating this sanctuary like infrastructure and economic development and improved intelligence and finance monitoring. Kittner‘s final argument is that the US with its allies ―must focus not only on the known and visible threat, but also on those threats that remain unknown.”[14] Kittner‘s argument is sound in describing the ideal conditions for Islamic terrorists or any other terrorist or criminal organization to exploit and fester within. However, it does not address the current reality that many homegrown terrorists are Muslims coming from Western Europe and the United States that have established their organizational and operational base out of their own homes.

[11] Christina. C. Brafman Kittner, ―The Role of Safe Havens in Islamic Terrorism,” *Terrorism and Political Violence* 19, no. 3 (Spring/Summer 2005): 307.

[12] Ibid., 308.

[13] Ibid.

[14] Ibid., 325.

Thomas Bruscino‘s *Out of Boundaries-Transnational Sanctuary in Irregular Warfare* links the importance of sanctuary to current conflicts by discussing in detail the strategic importance of sanctuary to the insurgents in the Vietnam War and the Soviet-Afghan War. Bruscino states, ―denying sanctuaries is an essential, and often overlooked, step to success" in American military counterinsurgency doctrine.[15] This lack of discussion about sanctuaries in doctrine occurs despite the greater acceptance of counterinsurgencies and stability operations as an essential responsibility of the US military since the 1990s. Even though the lessons learned in Vietnam and from observing numerous other conflicts where sanctuaries played a strategic role in the outcome, Bruscino highlights how US military strategists and doctrine writers have ―spent little time on the vital importance of denying insurgents transnational sanctuary".[16] This doctrinal gap, up until the publication of Army Field Manual (FM) 3-24 *Counterinsurgency* in 2006, in conjunction with a political reluctance to expand conflicts to additional countries provided ―American leaders and military commanders in the global war on terrorism [with] little doctrinal guidance on the topic" of sanctuaries and safe havens.[17]

FM 3-24 *Counterinsurgency* is the first piece of US military doctrine to go beyond discussing the importance of border security in counterinsurgencies. FM 3-24 discusses the issue of safe havens as an essential dynamic of an insurgency. FM 3-24 states how sanctuaries, both in neighboring countries and areas outside the control or influence of host nation forces, provide insurgents the political, psychological, and material resources necessary to rebuild and reorganize without fear of interference. FM 3-24 recognizes the connection between insurgents and non-state actors like transnational terrorist organizations. FM 3-24 states that terrorists ―often team up with insurgents and, in this sense, profit from

[15] Thomas A. Bruscino, ―Out of Bounds-Transnational Sanctuary in Irregular Warfare," in ―Global War on Terrorism," special issue, *Occasional Paper* 17 (2006): 82.

[16] Ibid.

[17] Ibid.

the conflict."[18] The —teaming up" of Al Qa'ida and the Sunni insurgency in Iraq and the Pashtun Taliban insurgency in Afghanistan provide excellent examples of what the combined effects are when terrorists and insurgents work together.

Michael Innes in *Denial of Sanctuary* adds that prisons, urban areas, diaspora communities, mosques, financial institutions, the Internet and even laws are providing safe havens and sanctuary to Islamic terrorists.[19] All of these other safe havens deserve detailed analysis and attention like Rabasa provides to geographic safe havens in *Ungoverned Territories.* In many of those other safe havens, particularly financial institutions, the US and other governments are applying —growing pressure" upon them. This monograph, however, argues that the greatest safe haven where America's enemies have taken root, the most conducive of all —ungoverned territories," perhaps as much as geographical safe havens, is the one that we apply the least amount of —growing pressure" towards, that being the virtual safe haven that the Internet provides.

Virtual Safe Haven "The Internet"

Virtual safe havens exist online in the Internet. —Some safe havens emerge not in places *per se* but in situations or environments that facilitate Al Qa'ida activities, such as communication networks and social networks."[20] The propensity of the United States government is to focus its elements and instruments of national power on geographical safe havens for terrorists that can be located and penetrated with physical force. The United States government recognized in the 2006 *National Strategy for Combating Terrorism* that —the Internet provides an inexpensive, anonymous, geographically

[18] U.S. Department of the Army, *Field Manual 3-24 Counterinsurgency,* (Washington DC: December 15, 2006): 1-16

[19] Michael A. Innes, —Cracks in the System: Sanctuary and Terrorism After 9/11," in *Denial of Sanctuary*, ed. Michael Innes (Westport CT: Praegar Security International, 2007), 1-20.

[20] U.S. Department of Defense, *Ungoverned Areas and Threats from Safe Havens* by Robert D. Lamb. Prepared for the Office of the Under Secretary of Defense for Policy. (Washington, DC, 2008): 16.

unbounded, and largely unregulated virtual haven for terrorists."[21] Within this plan is an emphasis to ―deny the Internet to the terrorists as an effective safe haven for their propaganda, proselytizing, recruitment, fundraising, training, and operational planning."[22] Despite these stated goals, four years later the Internet is essentially a growing and increasingly worrisome unmolested safe haven that provides the Islamic terrorists freedom of operations with little fear of being ‗disrupted, dismantled, and defeated' within.

Within the United States military, there is scant recognition of the Internet as a safe haven. FM 3-24 *Counterinsurgency* provides the only DOD definition of sanctuary that includes the Internet. It states, ―The meaning of term sanctuary is evolving. Sanctuaries traditionally were physical safe havens, such as base areas, and this form of safe haven still exists. But insurgents today can also draw on ―virtual" sanctuaries in the Internet, global financial systems, and the international media."[23] Until the recent publication of the United States Army Training and Doctrine Command (TRADOC) Pamphlet 525-7-8 *Cyberspace Operations Concept Capability Plan 2016-2028* in February of 2010, there was only one military definition involving the Internet itself. It was Joint Publication (JP) 1-02's definition of cyberspace as ―a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[24] While TRADOC Pamphlet 525-7-8 neglects the discussion of the Internet as a safe haven and focuses primarily on other types of cyber threats, it takes a comprehensive look and provides a conceptual framework on how the United States Army will leverage and integrate cyberspace into the full spectrum of its military operations.[25] The

[21] U.S. Government, *National Security Strategy for Combating Terrorism*, (Washington DC: 2006): 17.

[22]Ibid.

[23] U.S. Department of the Army, *Field Manual 3-24 Counterinsurgency,* 1-16.

[24] U.S. Department of Defense, *Joint Publication 1-02 Dictionary of Military and Associated Terms*, (Washington, DC: 2010): 121.

[25] U.S. Department of the Army, *TRADOC Pamphlet 525-7-8 Cyberspace Operations Concept Capability Plan 2016-2028,* (Washington, DC: 2010): iii.

TRADOC pamphlet also establishes ten new definitions to the doctrinal common lexicon on this matter to include cyber attack, cyber defense, cyberspace warfare, dynamic cyberspace warfare, cyber exploitation, and cyber situational awareness (See Appendix for definitions).

Army Field Manual (FM) 3-0 *Operations* states that the ―future operational environment will probably include areas not defined by geography, such as cyberspace" and ―with the exception of cyberspace, all operations will be conducted ‗among the people‘ and outcomes will be measured in terms of effects on populations."[26] Even though FM 3-0 was published only two years ago, the future operational environment it describes, in terms of cyberspace, is arguably upon us and has been part of the operational environment for most of the last decade. Furthermore, the enemy is using cyberspace ‗amongst the people‘ with terrific outcomes in terms of its effects on individuals within populations globally, including the United States. Meanwhile, it appears from the official US military‘s perspective that this war in cyberspace is a future fight rather than the current one. The currently unregulated conditions online benefit rogue states, criminals, and terrorist extremists, therefore, ―the way military thinkers approach doctrine relevant to the potential for Internet warfare must change."[27] Al Qa‘ida and their affiliates‘ actions indicate that they have largely lifted and shifted their efforts to their online safe haven, while the US military‘s efforts continue its focus on countering the enemy within geographic safe havens.

Conclusion

The United States continues the costly and bloody efforts of slugging it out against a conglomeration of numerous local insurgent groups, many of which are simply fighting Allied forces because of their own presence there, while largely chasing increasingly irrelevant Al Qa‘ida figureheads in Iraq, Pakistan, and Afghanistan who take refuge within those insurgent groups‘ sanctuary. In places

[26] U.S. Department of the Army, *Field Manual 3-0 Operations,* 1-4.

[27] Huba Wass de Czege, ―Warfare by Internet-The Logic of Strategic Deterrence, Defense, and Attack," *Military Review* XC, no. 4 (July-August 2010): 86.

where US regular troops are not fighting, the US penetrates geographic safe havens with Special Forces raids, drone attacks, and by helping its allies build their capacity for responsible governance and security through development and security sector assistance that prevents the establishment of terrorist safe havens. The Internet as a safe haven, however, goes relatively unmolested despite its growing significance and importance to Al Qa‘ida and its affiliates. In order to highlight this trend and offer solutions one must first demonstrate how the Internet is increasingly becoming equal to or greater in importance than geographical safe havens for Al Qa‘ida. In order to do that, we must first discover how the Internet became so conducive to Al Qa‘ida, how they adapted to relying on it so heavily, and discuss how they are using the Internet now in comparison to their past emphasis on geographical safe havens.

THE DUAL EMERGENCE

This subsection discusses the emergence of radical transnational Islamic terrorist organizations in the 1980s, and their initial probing into the emerging new Internet and the positive feedback they received from it during the 1990s. The first part of this subsection, The Soviet-Afghan War, highlights some of the difficulties associated with conducting ‗Jihad‘ prior to the introduction of the Internet. This comparison facilitates understanding of why the Internet is growing in importance to Islamic terrorist organizations. The second part of this subsection introduces how and why emerging Internet technology and forms of new media in the 1990s was a conducive and intriguing new tool for Al Qa‘ida and other terrorist organizations.

Pre-Cyber Jihad: The Soviet Afghan War (1979-1989)

The Soviet-Afghan war provides a window into a ‗pre-cyber Jihad‘ while simultaneously introducing the Islamic terrorist ideology and some of the key players that emerged out of that conflict. Ironically, some of those key players the United States supported are now the same ones we are fighting in the same places twenty years later. To be clear, even though the overwhelming majority of the Afghan Mujahedeen ‗Muj‘ were fundamentalist Muslims, this monograph is not contending that they were terrorists. They were simply insurgents reacting to the invasion of their country whose devout faith and primitiveness was often misinterpreted, purportedly by the Soviets, as being barbaric Islamic radicalism. In fact, Afghans did not possess the Islamic vitriol demonstrated in Iran and Lebanon at the time that led to terrorist acts against the West. This is in part because of Afghanistan‗s historic isolation and the fact it was never colonized by the west like most Muslim countries. The Afghan Muj never purposely singled out civilians as targets of terrorism throughout the war. ―Even toward the Soviets… the Afghans cultivated a simpler, less personalized hatred, one that did not reduce noncombatants to enemies the way the Middle Eastern terrorists did." [28] The Afghan Muj essentially was a movement of seven different insurgent groups without rhetoric, a supreme leader, ideology, politics, and extremism.[29]

The Soviet Afghan War was a classic guerrilla war with a foreign invader propping up a puppet government and fighting a counterinsurgency against rebel forces. This insurgency, like all insurgencies, requires some type of geographical sanctuary or safe haven in which the insurgents can train, rest, equip, and prepare for future operations. The Pakistan border regions, in particular the cities of Peshawar and Quetta, served the role as the safe haven for the Afghan Muj. From this safe haven, the Afghans received their American, Pakistani ISI and Saudi-funded weapons and training, kept their headquarters, and launched attacks into Afghanistan. The ―availability of sanctuaries to the resistance was not merely helpful, it was indispensable" to the Afghan Muj in their eventual victory over the Soviets.[30]

One of the greatest difficulties experienced by the Afghan Muj was their problems associated with information operations. Despite a war by a superpower that killed 1.3 million people, made over five million refugees, and created two million Internationally Displaced Persons (IDPs) it received very little western media attention. ―Afghanistan was too physically rough an assignment and offered too few rewards to draw the world‗s best television cameramen…who hold the key to a television story‗s

[28] Robert D. Kaplan, *Soldiers of God- With Islamic Warriors in Afghanistan and Pakistan,* (New York: Vintage Departures, 2001), 108.

[29] Ibid.,17.

[30] Robert F. Baumann, ―Compound Warfare Case Study: The Soviets in Afghanistan," in *Compound Warfare*: *That Fatal Knot*, ed. Thomas Huber (Leavenworth,KS: U.S. Command and General Staff College Press, 2002), 295.

impact."[31] Reporters were made to ―walk up and down mountains as much as fourteen hours a day" for days if not weeks and months exposed to mines, disease, exhaustion, and horrid food to get their story.[32] The fact the Soviets stated that they would kill reporters embedded with the Muj exasperated this lack of access and coverage. All of this, combined with a lack of satellite stations, hotels, and electricity resulted in ―for nearly a decade, the public was shown the same monotonous film clips of smoke billowing in the distance and of bearded, turbaned guerillas with old rifles sniping at convoys-images that only increased the war‘s unreality."[33] Robert Kaplan, a reporter who spent years with the Muj, felt that ―the scale of human suffering vastly overshadowed any other military conflict of the 1980s, was, quite simply, almost unconsciously ignored." [34]

Muj information operations aimed at the Soviet soldiers were also a very difficult undertaking. Robert Kaplan describes an exciting story of a Lithuanian activist/reporter‘s participation in an Information Operations (IO) mission.[35] He had to hike over mountains, dodge Soviet helicopters, be bombed by Soviet jets, and be shot at in ambushes for four weeks to get to Kabul in order to simply post dozens of forged Soviet newspapers on buildings that encouraged Soviet Soldiers to quit fighting and go home.

As long as there is guerilla warfare, the critical requirement for geographical sanctuary in insurgencies, as demonstrated in the Soviet-Afghan War and many other conflicts exists and for many insurgencies perhaps is its operational center of gravity from which it derives its strength. Many of the difficulties for an insurgent caused by time and distance illustrated during the Soviet-Afghan War no longer apply since the advent of the Internet. The Internet, as we have witnessed this decade in Iraq and Afghanistan, is both a critical requirement to have and a critical capability for insurgents to use as it

[31] Robert D. Kaplan, *Soldiers of God- With Islamic Warriors in Afghanistan and Pakistan*, 15.

[32]Ibid., 9.

[33] Ibid., 15.

[34] Ibid., 227.

[35] Ibid., 74-78.

enables them unlike anything preceding it historically to mobilize, train, communicate, and conduct information operations. To Al Qa‘ida and its affiliates who have limited geographical safe havens, the Internet is becoming of equal or greater importance if not their center of gravity.

The Birth of Al Qa’ida

In order to understand how the Internet as a safe haven is becoming increasingly important for adapting terrorist organizations, one must discuss how the leading Islamic terrorist organization emerged from the Soviet Afghan War. A handful of the Muj, mostly foreign fighters called ‗Afghan Arabs‘, empowered by their Islamic victory over the Soviet superpower in Afghanistan, would later form the senior leadership of Al Qa‘ida, the Taliban, and other Islamic militant and terrorist organizations throughout the world. These Arab and non-Afghan Muslims emerged from the war in Afghanistan with the attributes of ―combat experience, self-confidence, increased religious faith, ambitions for a borderless Islamic world, leadership skills, [and] hatred of the United States.” [36] Their leaders recognized that this was also an unprecedented opportunity and victory, compared to the numerous defeats Muslims had received from Jews and Hindus in recent times, which had inspired rejuvenation of armed Jihad across the Islamic World.[37]

Leading this group of Afghan Arabs was none other than Osama Bin Laden. The Pakistani ISI wanted a Saudi Royal Prince to ―lead the Saudi contingent in order to show Muslims the commitment of the Royal Family to Jihad.”[38] Bin laden, was not royal, but close enough to royality and wealthy enough to be a good alternative to a Saudi prince. Bin Laden‘s actual participation in combat in the Afghan War is disputed and debated. However, no one questions Bin Laden‘s monetary support, leadership, and

[36] Michael Scheuer, *Through our Enemies’ Eyes: Osama bin Laden, Radical Islam, and the Future of America*, (Washington, D.C: Potomac Books, Inc., 2006), 117.

[37]Ibid., 114

[38] Ahmed Rashid, *Taliban: Militant Islam, Oil & Fundamentalism in Central Asia,* (New Haven: Yale University Press, 2001), 131.

engineering support that were critical in establishing schools and base camps for Non-Afghan Arab fighters in Pakistan and Afghanistan. [39] In 1989, Bin Laden established Al Qa‘ida (*The Base* in Arabic) as a service center for Arab-Afghans and their families and to forge a broad based alliance amongst them.[40] Bin Laden‘s participation in the Afghan War and his leadership of Non-Afghan Arab fighters against the Soviets and the Afghanistan government was an ―indispensable stepping-stone toward the leadership role he has risen to in the Islamic world.”[41]

―Between 1982 and 1992 some 35,000 Muslim radicals from 43 Islamic countries in the Middle East, North and East Africa, Central Asia and the Far East” came to fight against the Soviets in Afghanistan.[42] Tens of thousands of foreign Muslim radicals would go to school in the Madrassas that the government of Pakistan had established along the Afghan/Pakistan border. In sum, up to 100,000 were exposed to Jihad either by fighting or by studying in the Madrassas between 1982 and 1992.[43] Once the war was over in 1992 when the Afghanistan government collapsed, the metaphoric ‗Frankenstein‘ that the United States, the Saudis, and the Pakistanis had created was now unleashed to begin global Jihad against Arab regimes and the West. ―The war left behind an uneasy coalition of Islamist organizations intent on promoting Islam against all non-Muslim forces. It also left a legacy of expert and experienced fighters, training camps and logistical facilities, and elaborate trans-Islam networks of personal and organization relationships.”[44]

After Osama Bin Laden was barred from entering Saudi Arabia following the first Gulf War, he and his senior followers enjoyed the safe haven of a supportive Islamic regime in Sudan until he was asked to leave there in 1996. Bin Laden was also active in Bosnia during the 1990s, the neglected truth

[39] Michael Scheuer, *Through our Enemies' Eyes*, 97-117.

[40] Ahmed Rashid, *Taliban,* 132.

[41] Michael Scheuer, *Through our Enemies' Eyes*, 98.

[42] Ahmed Rashid, *Taliban*, 130.

[43]Ibid.

[44] Samuel P. Huntington, *The Clash of Civilizations and the Remaking of the New World Order*, (New York: Touchstone, 1996), 247.

being that Bosnia —played an identical role in the global jihad to that of Afghanistan in the 1980s, serving as a convenient place to wage war against the infidel while providing sanctuary and training for the next generation of militants." [45] In fact the mastermind of 9/11 Khalid Sheikh Muhammad and two of the 9/11 hijacker pilots were veterans of the Bosnian Jihad.[46] Following his expulsion from Sudan and the end of the war in Bosnia, Bin Laden returned to Afghanistan where Al Qa'ida enjoyed not only the safe haven of the Pakistani frontier, but by 1996 all of Afghanistan itself as the Taliban eventually took control of all Afghanistan with the support of Pakistan.[47]

In addition to the well-structured, linear core organization that was forming in Afghanistan during this time, Al Qa'ida possessed a —moderately coupled network of terrorist cells which allowed some degree of directing" by senior Al Qa'ida leadership but provided enough decentralization —thus granting the system great resilience to large-scale perturbations."[48] This network of self-forming cells, comprised of the most radical individuals emerging primarily from the Afghan War expanded Al Qa'ida's operational reach and penetration throughout the globe. According to Bousquet, Marion and Uhl-Bien's —Complexity Theory and Al Qa'ida" presentation highlights the interactive non-linear bottom-up dynamics behind the self-organization of Al Qa'ida in which Bin Laden and other senior leadership are an emergent phenomenon.[49] Marion and Uhl-Bien stated, —Leaders do not create the system but rather are created by it, through a process of aggregation and emergence."[50] Al Qa'ida's momentum of aggregation and emergence would only garner more strength and speed throughout the 1990s.

[45] John R. Schinder, *Unholy Terror-Bosnia, Al Qa'ida, and the Rise of Global Jihad*, (St.Paul MN: Zenith Press, 2007), 8.

[46] Ibid.

[47] Ahmed Rashid, *Taliban.*

[48] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity,* (New York: Columbia University Press, 2009), 207.

[49] Ibid., 206.

[50] Russ Marion and Mary Uhl-Bien, —Complexity Theory and Al-Qaeda: Examining Complex Leadership", (Presentation, Fort Meyers, FL, December 2002).

1st Blood-Somalia 1993

The common perception was that those who perpetrated the ―Blackhawk” down incident in which 19 US Soldiers were killed in Mogadishu, Somalia in 1993 were simply Somali warlords with their armed gangs. For the most part this is true, but unknown to most at the time and for a few years following the incident, Al Qa‘ida was also a key player in the shadows that enabled the warlords‘ success from Sudan. Al Qa‘ida‘s perception was that the introduction of UN and American troops into Somalia in 1992 on a humanitarian mission was both a threat and an opportunity. Fearing that the US presence in Somalia would threaten Sudan and bin Laden‘s sanctuary there, Al Qa‘ida attacked American forces in both Yemen and Somalia to get them to leave the Horn of Africa region.[51]

Al Qa‘ida had struck its first blow against the West in Yemen by detonating two bombs in December 1992 at hotels that UN and American troops were staying in as they transited through Yemen into Somalia. Following that incident, the Americans quickly left Yemen as Bin Laden stated later in 1998, ―The US received our warning and gave up the idea of setting up its military bases in Yemen. This was the first Al Qa‘ida victory scored against the Crusaders.”[52]

Bin Laden stated in 1998 that he had sent 250 ―Afghan Arab” veteran fighters to help Aideed, the wanted Somalia warlord leader, and other Somali leaders fighting the US-led forces. These advisors instructed the Somalis on how to shoot down helicopters by utilizing techniques they had learned in Afghanistan against the Soviets. Some of the Al Qa‘ida advisors claimed to have taken part and killed Americans in the Mogadishu firefight that killed 18 US Servicemen on 3 October 1993.[53] The images on TV and in newspapers the next day of dead American Soldiers dragged through the streets of Mogadishu had a powerful impact on both Americans and Al Qa‘ida. This incident involving the deaths of 18

[51] Hamid Mir, ―Interview of Osama Bin Laden,” *Daily Pakistan*, March 18, 1997.

[52]Ibid.

[53]Ibid.

Soldiers resulted in the complete withdrawal of 25,000 Soldiers from Somalia within a few months time. Al Qa‘ida had seen Somalia as a second landmark win against the United States within less than a year.[54]

This iteration of learning in Somalia served two valuable teaching points for the young terrorist organization during its infancy. The first being their perception that the United States was much weaker than the Russians and it would easily abandon its causes and its allies with the public images of dead American Soldiers being dragged naked through the streets of Mogadishu. Bin Laden summed this up himself,

> The youth, [al Qa‘ida fighters in Somalia] were surprised at the low morale of the of the American soldiers and realized more than before that the American soldier was a paper tiger and would after a few blows run in defeat. And American forgot all the hoopla and media propaganda…about being the world leader and the leader of the New World Order, and after a few blows they forgot about this title and left, dragging their corpses and their shameful defeat.
>
> -Osama Bin Laden[55]

This inspired Al Qa‘ida for further actions against the United States with American troops remaining in the Arabian Peninsula following the Gulf War. The second learning point was the appreciation of the power of media images of causalities and the effect it could have on foreign governments as ―one serious skirmish was enough to cause US policy to shift dramatically overnight.” [56] Interestingly enough, either by design in an effort to be covert or by not understanding how to run successful information operations, Bin Laden and Al Qa‘ida did not take credit for what occurred in Somalia for another four to five years. Nonetheless, this would be the last time that Al Qa‘ida and other Islamic extremist organizations would allow somebody else, this time being the Somalia warlords, to get all the media credit. Understanding Al Qa‘ida‘s concealed role in Somalia and the effects they witnessed from the spectacular media images of

[54] Ibid.

[55] Hamid Mir, ―Interview of Osama Bin Laden,” *Daily Pakistan*, March 18, 1997.

[56] Timothy L. Thomas, ―Manipulating the Mass Consciousness: Russian & Chechen ―Information War” tactics in the second Chechen-Russian Conflict,*”* in *The Second Chechen War*. Ed. Anne Aldis(London: Conflict Studies Research Centre. UK Ministry of Defense, June 2000). 112.

dead Americans and resulting change in United States foreign policy allows for an appreciation for why the Internet would become so appealing to them later.

Chechen Wars and the First Use of the Internet Safe Haven (1994-96 & 1999-2000)

Hamas is credited with being —one of the first terrorist groups to make effective use of the Internet"[57] in the mid-1990s, but perhaps the first time any warring insurgent and counterinsurgent parties utilized the Internet for information operations was in the Second Chechen War in 1999 and 2000. The power of the Internet would soon be utilized to circumvent media control as Chechens directly reported from battle zones with no intervening media filter online.[58] To understand how the Internet emerged in the Second Chechen War, one must first understand the conditions resulting from the First Chechen War (1994-1996), and how this explains the use of the Internet during the second war.

The First Chechen War between Russia and the Republic of Chechnya was a public relations disaster for the Russians. The Russian military completely ignored the media, banned any interaction between it and its soldiers and leaders during the first few months of the war, and conducted little counter-propaganda. As a result, the Russians lost control of the information war and their message. On the other hand, the Chechens welcomed the press and TV coverage with open arms. The Chechens exploited the Russian weakness and manipulated world opinion by taking reporters to locations the Chechens wanted them to see and telling them the narrative the Chechens wanted them to hear. As a result, most of the news stories throughout Russia and the world had a pro-Chechen slant causing great tension within the Russian government and adding to the unpopularity of the war with the Russian people. The result, similar to what the Americans experienced in Somalia, was a total information war defeat for the Russians and they did not deny it.[59]

[57] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges*, (Washington D.C: United States Institute of Peace Press, 2006), 82.

[58] Tim L. Thomas, —Manipulating the Mass Consciousness," 113.

[59] Ibid.

> Yes, the Russian authorities lost the information war…How splendidly Chechen Information Minister Movladi Ugugov is operating, how skillful and adroit he is at feeding the press with all kinds of lies, distortions, and misrepresentations of the facts.
>
> –Sergei Stepashin, head of the Russian Federal Security Service, March 1995[60].

The Second Chechen War would not only be a second attempt to defeat the Chechens, but a second attempt to get the information war right this time for the Russians. Russian success would depend on public opinion within Russia for long-term success. Russian President Boris Yeltsin instituted Russian Federation Resolution No. 1538. ―This resolution was designed to filter military information from Chechnya, and to select which foreign information would be disseminated in Russia about the conflict."[61] Essentially, the Russians attempted to establish an information blockade with only one gate for information to flow from that the Russians themselves controlled.

This Russian control was facilitated by the fact that foreign and Russian reporters no longer sympathized with the Chechens as they did during the first war. This was because the Chechens had killed and kidnapped many reporters and foreign aid workers during the first war and between the wars and the fact that the Chechens had invaded Dagestan to initiate the second war. For the first few months of the conflict, Russian control of the media was relatively successful. However, the Russian military had incidentally created an information vacuum and once again closed the doors on the mass media. The Russian door closed even more coinciding with the fact combat operations had gone badly and more and more information became "classified".[62]

The Russian tight control of the media, the media‗s reluctance to embed with the Chechens, and the introduction of the Internet combined to set the conditions that enabled the startup of Chechen Internet sites to get their own story out. The Chechens reportedly had nearly 100 web sites situated throughout the

[60] Ibid.

[61] Ibid.

[62] Ibid., 115.

world that produced information in 20 languages.[63] Many of these websites were very dynamic and easily accessible in the West. On the Chechen website, www.qoqaz.net, for example, one could —download videos of attacks on Russians, view photos of Chechens in action and of Russian prisoners of war, find news items, read profiles of Chechen commanders, and read interviews with various Chechen leaders and fighters." [64] Chechens, unlike their Afghan brothers a decade earlier, would no longer have to drag foreign news reporters up and down and in and out of mountains to get a story out of the battlefield; they could do it themselves with a few mouse clicks on a website.

The information blockade and difficulty in accessing the battlefield resulted in the media becoming hungry for information and they turned to the Internet where Chechen reports were becoming available. Many foreign Muslim media Internet sites were utilizing the Chechen sites as their source to write their stories and the –news-starved Russian reporters would repeat these reports, thereby circumventing the Russian information blockade."[65] Despite establishing many websites of their own, hacking into and closing down Chechen sites, the Russians had once again lost control of the message. The Russians did not lose total control as they did in the First Chechen War, but by exerting too much control, they forced the Chechens to experiment and probe extensively with the Internet. The feedback from these efforts online was overwhelmingly positive. Warfare and terrorism would never be the same and the use of the Internet would only grow at the beginning of the new millennium.[66]

Conclusion

The emergence of the Internet as a weapon of warfare during the late 1990s increased the complexity of Islamic extremist organizations and served as one of the underlying enablers for their continued emergence and self-organization during the 2000s. The lessons learned, particularly the

[63] Ibid., 121.

[64] Ibid.

[65] Ibid.,115.

[66] Ibid., 112-126.

importance of information operations and their effects, in Afghanistan the lack of it, and in Somalia, the power of it, resonated in the minds of Islamic extremists throughout the 1990s. When the Russians tried to implement an informational blockade in Chechnya, the Internet provided a medium that outflanked the Russians. The Internet essentially served as a 21st century metaphoric –blockade runner" in this conflict within the new information age. The Chechen War was also a warning sign of this emerging capability online and the –extremists‘ use of the Internet has developed rapidly since the Chechen-Russian conflict."[67] The United States and its allies would discover this a few years later in Iraq and Afghanistan. Stated best by Thomas Friedman in *The World is Flat*, —the flat world makes it much easier for terrorists to transmit terror. With the Internet, they don‘t even have to go through Western or Arab news organizations but can broadcast right into your computer. It takes much less dynamite to transmit so much more anxiety." [68]

The Chechen conflict was clearly just an early probe into using the Internet though; the Islamic extremists essentially enjoyed geographic safe havens in Sudan, Somalia, Yemen, Afghanistan, Muslim-controlled areas of Bosnia and Chechnya, the Pakistani frontier, and many other parts of Asia and Africa with little or no risk or threats. The five years between Bin Laden‘s publication of the *Declaration of War against the Americans Occupying the Land of the Two Holy Places* after his arrival in Afghanistan in 1996 and the 9/11 attacks –constitute the –golden age" of Al Qa‘ida."[69] It was during this –golden age" that Al Qa‘ida emerged as a more formal self-organizing global Islamic terrorist organization comprised of the most world‘s most militant Islamic fundamentalists.

[67] Timothy L. Thomas, –Countering Internet Extremism," *IOsphere* (Winter 2009), 16.

[68] Thomas Friedman, *The World is Flat: A Brief History of the 21st Century,* (New York: Picador/Farrar, Straus, and Giroux, 2007), 597.

[69] Marc Sageman, *Leaderless Jihad-Terror Networks in the Twenty-First Century,* (Philadelphia: University of Pennsylvania Press, 2008), 43.

Al Qa‘ida established terrorist training camps and possessed a well-structured chain of command organized into committees for ―finance, religion, military affairs, and propaganda.”[70] Al Qa‘ida would have to adapt when they lost many of those geographic safe havens, and the Internet would fill many of those lost gaps in terms of capacity and capabilities. As Liddell Hart tells us, ―adaptability is the law which governs survival in war as in life--war being but a concentrated form of the human struggle against the environment,” and the Islamic extremists would truly have to adapt after 9/11 to survive.[71]

ADAPTATION

> Emergent Complexity without adaptation is like the intricate crystals formed by a snowflake: it‘s a beautiful pattern, but it has no function.[72]
>
> –Steven Johnson

In the first decade of this millennium, Islamic terrorist organizations transformed America‘s mindset and vision of what ―The New World Order” following the end of the Cold War would look like by penetrating its borders and intervening in its citizens‘ daily lives with the constant fear of terror they can brandish. They successfully demonstrated that ―winning wars often requires changing societies as well as changing oneself”.[73] Al Qa'ida and their affiliates have arguably altered both Islamic and Western societies and Al Qa‘ida has clearly changed itself.

Islamic terrorist organizations are themselves complex adaptive systems. Their initial successful probes with the Internet in the 1990s demonstrated that Islamic extremist groups were successfully beginning to adapt to cope with the complexity of a new online global world.[74] The positive feedback they received from a relatively small injection of energy online yielded a disproportionately large return

[70] Marc Sageman, *Leaderless Jihad,* 45.

[71] B. H. Liddell Hart, *Strategy*, 2nd ed. (New York: Signet, 1974), 330.

[72] Steven Johnson, *Emergence: The Connected Lives of Ants, Brains, Cities, and Software,* (New York: Scribner, 2001), 20.

[73] Alex Ryan, ―The Foundation for an Adaptive Approach: Insights from the Science of Complex,” *Australian Army Journal,* VI, no.3 (Summer 2009): 73.

[74]Ibid., 78.

on their investment on the ground. They discovered a lever for transforming the system of warfare in a new era that was cheap, fascinating, global, and readily available. Information operations would no longer have to require the burden and delays associated with escorting a foreign journalist a hundred miles into and out of conflict to get good film footage and a good story as they did in Afghanistan. They no longer had to have their message lost within an informational blockade as they learned in Chechnya. They could be their own journalists with their own narrative in a matter of minutes with a laptop from any location and instantly penetrate geographical space and boundaries to receptive audiences across the globe.

The Internet was becoming the equivalent of an air force and navy to Al Qa‘ida and their affiliates; they could penetrate just about anywhere with it. During this time, around the turn of the millennia, Islamic terrorist organizations were not the only ones changing and adapting to the Internet, the entire world was becoming more dependent upon its use. For the purposes of comprehending how this adaption occurred within Islamic terrorist organizations, the linkages between the growth of the Internet within the Islamic society and how the religion of Islam itself is adapting to the Internet as a whole cannot be overlooked.

Internet Growth in the Islamic Society

―The history of communication in the Muslim world reveals three transformations of Islamic culture, each brought about by information technology: paper, the printing press, and the advanced communication technologies of today.”[75] The growth of the Internet in the last decade has essentially changed the fabric of human interactions within all societies, peoples, and religions on every continent. Islamic societies are certainly no exception. Traditionally Islam has been slow if not resistant to embrace change and openness that modern technologies provide, but the Internet has been the exception to that rule. Despite the many negative aspects on the Internet, like access to pornography and anti-Islamic

[75] Ziauddin Sardar, ―Paper, Printing, and Compact Disks: The Making and Unmaking of Islamic Culture,” *Media, Culture, & Society* (January 1993): 43.

material, which countries like Pakistan and Saudi Arabia have gone to great lengths to disrupt, overall Muslims have incorporated the power of the Internet for the benefit of Islam. As Gary Bunt points out while describing how religious police in Saudi Arabia utilize the Internet to receive anonymous reports about religious transgressions, ―there can be a complex relationship between paradigmatic religious practices and technical innovation in which one can often balance out the other."[76]

The Muslim world embraced the Internet and it is fundamentally changing the way the religion is practiced in many ways in terms of space, time, and perspectives. Bunt explores the increasing impact the Internet has had on Muslims and Non-Muslims worldwide in shaping their perceptions of Islam, changing traditional Islamic societies and networks, and dramatically influencing forms of Islamic activism and radicalization. Bunt argues that the ―Internet has supplemented, and in some cases supplanted, traditional approaches to Islamic knowledge management and dissemination."[77] This Internet ―wiring" of the House of Islam ―represents one of the most significant historical changes in approach toward how information about Islam and Muslims is processed, networked and disseminated."[78]

Internet World Stats provides statistical proof of the rapid growth of the Internet within the predominately-Muslim Middle East and Muslim dominated countries in Asia. Despite the fact that the Middle East Internet users comprise only 3.1% of the world's population and 3.3% of the world's Internet users, the 29.8% percentage or penetration of the population with access to the Internet is above the rest of the world on average. The most astounding statistic is the 1,825.3% user growth percentages from 2000 to 2010 in the Middle East. In Asia, the predominately-Muslim country of Pakistan with its estimated 18.5 million users, has an unbelievable 13,716.3% percentage growth over the past decade and

[76] Gary R. Bunt, *iMuslims-Rewiring the House of Islam,* (Chapel Hill: The University of North Carolina Press, 2009), 15.

[77] Ibid.

[78] Ibid., 5.

Indonesia, a predominately-Muslim nation, with its 30 million users has a 1,400.0% percentage growth rate.[79]

Bunt notes that for many Muslims being online in the name of Allah represents an obligation. An Islamic website removes the prospect of physical compartmentalization of religion and facilitates this constant obligation to Allah, allowing web users constant linkage to their mosque‘s website or worldview connection to a specific Islamic website. This constant linkage enabled by BlackBerrys and iPhones with browsers fixed to a particular site or receiving emails and RSS feeds allows Allah to be always on and integrated into a Muslim‘s daily life.

Traditional Islam has adapted to the 21st century innovation of the Internet so well that in terms of contemporary expansion of Islamic discourse, it is without precedent since the beginnings of Islam itself. Bunt states that the rapid expansion and networking of Islam from the Internet we see today is unlike anything seen in Islam ―since the seventh century...from its emergence in the Arabian Peninsula…being instructed by God to ―Recite!" in 610, to its expansion across continents as far as Western Europe, China, India, and sub-Saharan Africa 100 years later."[80] Today, throughout the Muslim world the Internet and other modern information technology is providing a new wave of critical religious thought to a mass Islamic audience not seen since the advent of the printing presses.[81] As such, it is degrading the power of traditional religious scholars and remaking Islamic culture to the benefit of the radical Islamic groups. ―What is happening in the Islamic world is more than religiously-motivated, isolated acts of violence; it is an attempt to unite the Muslim world behind a radical agenda."[82] Thomas Friedman points out that one cannot understand the rise of Al Qa‘ida without referring to the flattening of the world through

[79] ―Internet usage in the Middle East," Internet World States, http://www.Internetworldstats.com/stats5.htm (accessed August 19, 2010).

[80] Gary R. Bunt, *iMuslim,* 276.

[81] Timothy Bailey and Michael Grimaila, ―Running the Blockade: Information Technology, Terrorism, and the Transformation of the Islamic Mass Culture," *Terrorism and Political Violence,* 17, no. 3 (Spring/Summer 2005): 525.

[82] Ibid.

globalization and the Internet. Friedman states, ―Globalization..has been al-Qaeda‗s friend in that it has helped solidify a revival of Muslim identity and solidarity…thanks to the Internet and satellite television.‖[83] The Internet‗s conduciveness to the religion of Islam itself directly affects how the Internet, as a complex adaptive system in itself, has become conducive to Islam‗s extreme radicals. So conducive was the Internet that the Al Qa‗ida movement would eventually adapt themselves within this complex adaptive system and make it their safe haven.

Al Qa'ida as a Complex Adaptive System

Complex systems science focuses on complex adaptive systems and while there is no agreed upon definition of complexity from complex system scientists, ―The essence of complexity is related to the amount of variety within the system, as well as how interdependent the different components are.‖ [84] In the context of this monograph, the interdependent relationship between the religion of Islam, Muslims, and Islamic terrorists is comprised of many different varieties, groups, and perspectives on Islam; nationalities, languages, and cultures of Muslims; and the numerous Islamic militant groups that exist illustrate the dynamic characteristics and scale of this complex system. According to Dr. Alex Ryan, ―Interdependence means that changes in the system generate many circular ripple effects.‖[85] Militant radical Islam in its numerous forms across multiple scales has had a huge ripple effect on Muslims and non-Muslims alike. This ripple effect continues to expand with the growing dependence radical Islam has on the Internet and interdependence amongst radical Islamists groups, networks, and actors that are enabled and hosted by the Internet.

In the study of networks, the information revolution has favored terrorist, insurgents, gangs, and criminal type networks like Al Qa‗ida and encouraged their growth ―by making it possible for diverse,

[83] Thomas Friedman, *The World is Flat,* 596.

[84] Alex Ryan, ―The Foundation for an Adaptive Approach,‖ 71.

[85] Ibid.

dispersed actors to communicate, consult, coordinate, and operate together across greater distances and on the basis of more and better information than ever before."[86] Arquilla and Ronfeldt predicted as early as 1997 that these new-networked organizations would result in new types of conflicts emerging and that ―those actors which are the most successful at adopting these new modes of conflict pose serious challenges to their most rigidly hierarchical rivals, typically established states and armies."[87] After 9/11, much of the study and attention of networked organizations focused on Al Qa‘ida and other radical Islamic militants and terrorists. This is largely due to the ―nebulous and dispersed nature of these organizations [that] has invited their analysis in terms of decentralized networks and complex adaptive systems."[88]

Both Al Qa‘ida and the practice of Islam online are examples of complex adaptive systems that are ―open to flows of energy, matter, and information, which flow through networks of positive and negative feedback."[89] This feedback (further creating interdependence and adding to its complexity) from Al Qa‘ida‘s use of the Internet are some of the underlying causes that allowed Al Qa‘ida to survive, reemerge, self-reorganize, maintain their capabilities, expand globally, and overall adapt into an almost completely different complex organization, if not a social movement, in a post 9/11 environment.[90]

9/11 and the Loss of a Safe Haven

The 9/11 attacks marked the end of the ‗golden age‘ of Al Qa‘ida and the end of its time as being a semi-linear system or structured organization. ―Whereas outputs are always proportional to inputs in linear systems,"[91] Al Qa‘ida‘s relatively minor terrorist attacks or outputs prior to 9/11 on the USS Cole

[86] John Arquilla and David Ronfeldt, ―Cyberwar is coming!" in *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: RAND Corporation, 1997), 26-27.

[87] Ibid.

[88] Antoine Bousquet, *The Scientific Way of Warfare,* 206.

[89] Alex Ryan, ―The Foundation for an Adaptive Approach," 71.

[90] Ibid., 72.

[91] Ibid.

and the embassies in Tanzania and Kenya resulted in a proportional response to them that Al Qa‘ida could absorb. The relative proportional inputs to outputs Al Qa‘ida received from the United States in the form of some cruise missiles hitting some of their suspected camps and facilities in Afghanistan and Sudan following the embassy and Cole bombings did not disrupt the linear balance Al Qa‘ida maintained. It only emboldened Al Qa‘ida to provoke a larger terrorist attack. The massive 9/11 attacks, however, caused a fundamental change and reframing of US policy and actions towards Al Qa‘ida. The United States and its allies had finally entered Al Qa‘ida‘s systems after 9/11 and the effects of this penetrating new presence and input would have a dramatic effect that would cause Al Qa‘ida‘s systems to change.

The linear organization of Al Qa‘ida could not magnify the positive feedback it received from its successful attack on the United States with the Islamic world nor effectively counteract the negative feedback resulting from the United States and its allies attack on its geographical safe havens in Afghanistan. Because of its loss of safe havens and the effects of the Global War on Terrorism on Al Qa‘ida, Al Qa‘ida could no longer maintain its balance as a linear type organization. The original Al Qa‘ida organization itself was essentially defeated after the US-led assaults on its strongholds in Afghanistan and largely contained within Pakistan‘s Waziristan region. Marc Sageman states, ―in the wake of the closure of the training camps in Afghanistan, the halt of financial transfers, and the detention or death of key personnel, Al Qa‘ida Central has receded in importance.”[92] Perhaps so, but Al Qa‘ida adapted and only became more of a complex problem for the United States and its allies to try to solve because ―in its place, of no less concern to those trying to understand terrorists and their actions, is a looser social movement with its own strengths and vulnerabilities.”[93]

A key concept of complex systems science is that of local autonomous agents of change. These self-interested agents make local decisions acting on local information ―within a complex system and

[92] Marc Sageman, *Leaderless Jihad,* 31.

[93] Ibid.

naturally generate variety, because each agent has a slightly different context.”[94] In the context of this topic, these autonomous agents are the numerous global violent Islamic extremist organizations, small groups, and lone-wolf individuals that would join and pledge allegiance to the organization known as Al Qa‘ida. Inspired and influenced by Al Qa‘ida Central, these autonomous agents, heavily dependent upon the Internet in many operational ways, would quickly fill in the leadership and operational power vacuum caused by the receding importance of Al Qa‘ida Central.

Sageman makes an important distinction between the original organization or Al Qa‘ida Central and the common usage of the term —Al Qa‘ida” in describing the expanding social movement of global Islamist terrorism. Sageman believes that the social movement should not be called —Al Qa‘ida” as it is indiscriminately referring to both the organization and to the growing social movement.[95] Al Qa‘ida as a —social movement has spread far beyond the original organization” allowing Al Qa‘ida to adapt and survive in its transition from a linear to a non-linear organization and completing its emergence in becoming a complex adaptive system.[96]

Conclusion

—The resilience and adaptability of the network has been further demonstrated by events following September 11 and the American response.”[97] Al Qa‘ida had to adapt in order to initially avoid extinction and continually function in a post 9/11 environment. The United States response essentially penetrated into Al Qa‘ida‘s systems and broke the non-complex linearity of its systems. In doing so, Al Qa‘ida had to become a non-linear and more complex system to survive in its hostile new operating environment that it essentially brought upon itself. As Cohen stated, —Indeed, the ability to adapt is probably most useful to any military organization and most characteristic of successful ones, for with it, it

[94] Alex Ryan, —The Foundation for an Adaptive Approach,” 72.

[95] Marc Sageman, *Leaderless Jihad,* 31.

[96] Ibid.

[97] Antoine Bousquet, *The Scientific Way of Warfare,* 208.

is possible to overcome both learning and predictive failures."[98] Al Qa‘ida has learned from its mistakes by transitioning its organizational structure to fit in its new environment. After the US-led assaults on Al Qa‘ida‘s strongholds in Afghanistan, ―the organization changed its format to a rapidly changing multi-cellular transnational structure spanning the entire globe."[99] A key enabler to Al Qa‘ida‘s rapid change in format has been the Internet that at the same time was spanning the globe in a transnational form during this time.

The Internet has also been unprecedented in Islamic history as a medium for discourse about Islam and the Islamic society has largely fully embraced integrating the Internet into Islamic practices. This is an essential part of the environmental frame into understanding how Al Qa‘ida adapted and transitioned in a post 9/11 hostile environment. Sageman states, ―There was no central intent of moving the terrorist social movement online; it just happened by itself, like a Darwinian evolution by natural selection."[100] He also describes the terrorist social movement to the Internet as a ―spontaneous evolution…not planned by any central organization; it simply coincided with the growth of the Internet and the close monitoring of physical meeting spaces."[101]

Al Qa‘ida was utilizing the Internet for propaganda purposes prior to 9/11 to some extent, but the ―American attacks on Al Qa‘ida terrorist training camps in Afghanistan forced the terrorists to move some of their operations to the Internet."[102] For the purposes of this monograph in illustrating the growing importance of the Internet as a safe haven in comparison to geographical safe havens, we will take a detailed look at some of those Al Qa‘ida operations that have moved online. In doing so, we will see that

[98] Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War*, (New York: Free Press, 1990), 94.

[99] Gabriel Weimann, *Terror on the Internet,* 116.

[100] Marc Sageman, *Leaderless Jihad,* 121.

[101] Marc Sageman, *Leaderless Jihad,* 110.

[102] Gabriel Weimann, *Terror on the Internet,* 127.

many operations conducted within the virtual safe haven online are equal to or are even more beneficial to Al Qa'ida and its affiliates than geographical safe havens.

WHY THE INTERNET SAFE HAVEN IS BECOMING INCREASINGLY AS IMPORTANT AS GEOGRAPHICAL SAFE HAVENS TO ISLAMIC TERRORISTS

> May Allah bless you lions of the front, for by Allah, the fruits of your combined efforts--sound, video, and text—are more severe for the infidels and their lackeys than the falling of rockets and missiles on their heads
>
> - Abu Yahya Al Libi[103]

The Internet is both a safe haven and a battlefield. In many ways, the Internet is more important than a real physical battlefield, a real physical act of terrorist violence, or a real geographic safe haven to Al Qa'ida and its affiliates. This monograph has explained up to this point how Al Qa'ida and its affiliate's use of the Internet originally emerged and how it was critical to their adaption in a post 9/11 environment. This subsection attempts to compare the capabilities that an Internet safe haven provides in comparison to geographical safe havens and geographic battlefields in order to make the distinction between the virtual and physical spaces in which this war is really taking place. In doing so, it will illustrate that even though ―Islamist militant groups might be using medieval methods of violence, such as beheading, ... the skill with which they are using the Internet indicates that their feet are firmly placed in the 21st century."[104]

Not Cyberterrorism, but Just as Dangerous

> *Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation...The threats we face range from individual*

[103] Abu Yahya al Libi, ―Shaykh Abu Yahya al-Libi-To the Army of Difficulty in Somalia-Muharram," WorldAnalysis.net, http://worldanalysis.net/postnuke/html/index.php?name=News&file=article&sid=209 (accessed September 15, 2010).

[104] Sudha Ramachandran, ―Logging onto to Terror.com," Asia Times Online, http://www.atimes.com/atimes/Front_Page/FG14Aa02.html (accessed August 11, 2010).

> *criminal hackers to organized criminal groups, from terrorist networks to advanced nation states*[105]
>
> - *National Security Strategy* (2010)

This monograph is not about cyberterrorism. Many people incorrectly lump together the offensive ‗hacking‘ of the Internet and terrorist‘s utilization of the Internet as cyberterrorism, the latter is not cyberterrorism. All of the media hype and political attention addressing the need to protect America‘s critical Internet networks and nodes from a ‗electronic Pearl Harbor‘ attack; combined with the failure to identify who is a cyberterrorist and what constitutes cyberterrorism, has created a confusion and angst over what cyberterrorism actually is.[106] ―The net effect of all this attention has been to create a climate in which instances of hacking into government web sites, online thefts of proprietary data from companies, and outbreaks of new computer viruses are all likely to be labeled by the media as suspected cases of cyberterrorism."[107]

Often there is no distinguishing between hackers, ‗hacktivists‘ or hacker activists with a cause, deliberate nation state or state-sponsored cyberattack, and actual terrorist organizations when discussing cyberterrorism in western lexicon. Despite the ―psychological, political, and economic forces that have combined to promote the fear of cyberterrorism", and ―despite all the gloomy predictions of a cybergenerated doomsday, no single instance of real cyberterrorism has been recorded."[108] Neither Al Qa‘ida nor any other terrorist organizations have attempted to stage a serious cyberattack, yet this does not mean it will not happen someday and that no precautions are required to defend America‘s networks against any types of cyber threats. Cyberattack by terrorists is a real threat, but these cyber fear headlines shadow how Al Qa‘ida is actually utilizing the Internet as a safe haven. In doing so though, the United States diverts massive government and civilian budgets, time, energy, and personnel towards the new

[105] U.S. President, *National Security Strategy*, (May, 2010): 27.

[106] Gabriel Weimann, *Terror on the Internet,* 148-171.

[107] Ibid., 152.

[108] Gabriel Weimann, *Terror on the Internet,* 148-152.

profitable industry that emerged to defend against cyberterrorism.[109] Although it is outside the scope of this monograph to go into detail about how the United States is countering the Internet safe haven; essentially the United States is spending billions of dollars and thousands of lives in attacking their geographic safe havens, billions more defending its Internet networks, and probably only a few million in monitoring their Internet safe havens. Meanwhile, Al Qa'ida is mostly utilizing the Internet for many other operational purposes besides the possibility of using the Internet for offensive cyberterror from its Internet safe haven.

Comparing Safe Havens

As stated earlier, the Internet is becoming equal to or even greater in importance than geographical safe havens to Al Qa'ida and its affiliates. The Anti-Defamation League pointed out as early as 2002 that ―In many ways, the Internet is a tool tailor-made for these Islamic extremists, who uses it covertly and overtly to plan attacks, raise money, and spread…propaganda".[110] The capabilities offered by the Internet utilized by Al Qa'ida and other Islamic extremists have only expanded and grown with the Internet since that time. Weimann notes that it is ―possible to identify no fewer than seven different, albeit sometimes overlapping, instrumental uses of the Internet" that terrorists utilize. [111] These functions include data mining, networking, recruitment and mobilization, training (Instructions and online manuals), planning and coordination, fund-raising and even attacking other terrorists. [112]

Kittner's article describes essentially the same key functions in describing the benefit of geographical safe havens to Islamic terrorist networks.[113] Gray compares Weimann's noted functions to geographic safe havens depicted in Kittner's article stating that the comparison ―reveals that the

[109]Ibid.*,* 148-171.

[110] Anti-Defamation League, ―Jihad online: Islamic terrorists and the Internet," Anti-Defamation League Web Site. Pdf file, http://www.adl.org/Internet/jihad_online.pdf. (accessed August 19, 2010).

[111] Gabriel Weimann, *Terror on the Internet,* 111.

[112] Ibid.

[113] Brafman Kittner C., ―The Role of Safe Havens in Islamic Terrorism," 307-329.

capabilities offered by the Internet afford many of the benefits of traditional safe havens."[114] Very much in line with the thesis of this monograph, Gray's article states that the ―Internet is more capable of replacing the need for territorial safe havens with respect to some of the categories mentioned."[115]

Communications and Social Networks

Thomas Hegghammer who researches Islamist Web sites at the Norwegian Defense Research Establishment says, ―In a sense, [the Internet] replaced Afghanistan as a meeting place."[116] This short statement illustrates two important facts. The first fact is that many geographical safe havens, like Afghanistan, are no longer entirely safe in the post 9/11 environment for terrorists. Efforts by the international community have resulted in the killing and capturing of thousands of Al Qa'ida terrorists throughout the world. There is probably no place on Earth considered by terrorists to be a completely enduring safe haven to meet face to face these days and with cell phones being susceptible to interception, the Internet is truly become a meeting place for terrorists that Hegghammer describes.

Al Qa'ida terrorists are no longer geographically constrained within a particular location or have to travel and incur risk to meet in person. As such, the Internet ―allows terrorists to convey their messages to international and distant audiences with whom it would otherwise be difficult to communicate."[117] Originally, terrorists' online content was mostly for reading only on their own web sites or text-based messages posted on forums, but the recent technological advances of high-tech, cheap, and user-friendly hand held video cameras and interactive online social networking have again changed terrorist online communications. The recent growth of social networks on the Internet like Facebook, Twitter, MySpace,

[114] David Gray and Albon Head, ―The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven," 396-404.

[115] Ibid.

[116] Sudha Ramachandran, ―Logging onto to Terror.com," *Asia Times Online*, July 14, 2006. http://www.atimes.com/atimes/Front_Page/FG14Aa02.html (accessed August 11, 2010).

[117] Gabriel Weimann, ―Terror on Facebook, Twitter, and YouTube," *The Brown Journal of World Affairs* 16, no. 11 (Spring/Summer 2010): 46.

and YouTube has exponentially increased the terrorists' capability to communicate online. Weimann states these social networks have ―provided terrorists with a whole new virtual realm to conduct their sinister back-ally transactions."[118] In fact, research by Evan Kholmann who runs the Global Terror Alert website found that ―90 percent of terrorist activity on the Internet takes place using social networking tools, be it independent bulletin boards, Paltalk, or Yahoo! eGroups…These forums act as a virtual firewall to help safeguard the identities of those who participate."[119] Skype goes further in its capabilities for terrorists to communicate as it essentially provides a secure and free video-teleconference (VTC) capability to terrorists. The fact that these social networks can be accessed now from wireless 3G smart phones only increases the 24/7 capabilities of terrorist communication as they no longer even have to be in front of a laptop or desktop.

The University of Arizona's Artificial Intelligence (AI) Lab scientifically studies the estimated 4,300 Islamic terrorist websites in existence today. The AI Lab's Dark Web project is a long-term scientific research program that aims to study and understand the international Jihadist terrorism phenomena via a computational, data-centric approach. With a team of 16 research assistants led by Hsinchen Chen, Dark Web aims to collect web content generated by international terrorist groups, including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, and other forms of web-based communications. ―The methodology incorporates information collection, analysis, and visualization techniques, and exploits various Web information sources."[120] The University of Arizona's Artificial Intelligence Lab conducted a study of 39 terrorist and terrorist supporter web sites and their combined 94, 326 web pages in 2008 in order to obtain a comprehensive picture and conduct

[118] Ibid., 53.

[119] Yuki Noguchi, ―Tracking Terrorists Online," *Washington Post*, April 19, 2006. http://washingtonpost.com/wp-dyn/content/discussion/2006/04/11/DI2006041100626.html (accessed September 15, 2010).

[120] Hsinchun Chen et al., ―Uncovering the Dark Web: A Case Study of Jihad on the Web," *Journal of the American Society for Information Science and Technology* 59, no. 8 (January 4, 2008): 1349.

analysis of terrorist activities on the web.[121] Even though the the AI Lab Dark Web study illustrates just the hyperlink relationship between only 39 of the 4,300 estimated Islamic terrorist web sites in existence; it demonstrated that various web site group clusters possess some degree of an interdependent relationship amongst various radical Islamic groups and viewers on the web. These relationships online allows terrorists from various Islamic terrorists groups across the globe ―to exchange not only ideas and suggestions but also practical information about how to build bombs, establish terror cells, and carry out attacks."[122]

The Dark Web study analyzed how six Al Qa'ida websites utilize the six dimensions or categories of terrorist use of the Internet. The study utilized multivariate data originating from a star plot representation within a normalized scale between zero and one for an activity index. Dark Web has discerned that all the clusters of Islamic terrorist groups ―use the web to share ideology and to propagate ideas, especially to its members."[123] The study found that the Al Qa'ida clusters (group of six sites) demonstrates that Al Qa'ida primarily utilizes its website for sharing its ideology and as a method of communications.

The Internet has increased the ability of Islamic terrorists to conduct global operations utilizing simultaneity and depth in a strategic sense as their global operations can complement each other in different parts of the globe to achieve strategic objectives. Perhaps the best example of this would be the Madrid train bombings in 2004 that killed 201 people, wounded 1,240 and resulted in a reversal of the anticipated election results that in turn resulted in Spain's exodus from military operations in Iraq. Much of the detailed planning and coordination conducted by the actual terrorists who executed the attack was online. In addition, the Media Committee for the Victory of the Iraqi People (Mujahidin Services Center) posted the strategic political design behind an attack on Spain online three months prior to the attack. The

[121] Ibid.

[122] Gabriel Weimann, *Terror on the Internet,* 117.

[123] Hsinchuan Chen et al., ―Uncovering the Dark Web: A Case Study of Jihad on the Web," 1356.

Norwegian Defense Research Establishment (FFI) located this strategic document and filed it, but the FFI incorrectly assumed the Spanish government had also intercepted this document as well and did not notify Spanish authorities.[124]

It is not within the scope of this monograph to address the extent of the complexity or the means required in countering this online battleground, but the Spanish Train bombing incident demonstrates the lack of a global allied effort to even pass this critical information between NATO countries. This lack of a global effort coupled with the legal constraints, encryption protections, anonymity, language barriers, constant switching of web addresses on unknowing servers, and the vastness of the Internet itself sets the conditions to make it a safe haven just like a remote jungle or inaccessible mountain valley cave. NATO General Secretary Jaap de Hoop Scheffer stated, ―When it comes to video, we are frankly in the Stone Age…We are also barely on the field when it comes to the Web".[125]

Another aspect of communications is the ability for Al Qa'ida senior core leadership and local actor cell leaders to command and control. United States Army Field Manual 6-0 *Mission Command* states that the characteristics of command and control is the ability to identify and react to changes in the situation; the ability to provide a continuous, interactive process of reciprocal influence among the commander, staff, and available forces; and the ability to reduce chaos and lessen uncertainty.[126] Throughout the history of warfare, command and control of forces has been difficult and has evolved primarily around technologies and a degree of decentralization out of necessity due to the increasing size of armies since the Napoleonic era. For example, during the Soviet-Afghan War, Mujahedeen Commanders were constantly shuffling themselves or sending messengers between the front in Afghanistan and the headquarters facilities in Peshawar in order to attend meetings and conduct command

[124] Gabriel Weimann, *Terror on the Internet,* 133.

[125] Jaap de Hoop Scheffer, ―Public Diplomacy in NATO-led Operations," (NATO Secretary General address, Copenhagen, October 8, 2007).

[126] U.S. Department of the Army, *Field Manual 6-0 Mission Command-Command and Control of Army Forces*, (Washington, DC: August 11, 2003): 1-2.

and control efforts. Command and control during this war was especially difficult since it could take days or weeks for a message to be passed and that information was often ‗overcome-by-events' (OBE) in military terms, due to the time delay over the geographic distance.[127]

From a terrorist organization's perspective today, however, the ―Internet is the perfect terrorist command and control tool. It mirrors the framework of their operations: decentralized, basically anonymous, and offering fast communication to a dispersed audience"[128] ―Command and control on the Internet is not hindered by geographical distance or by the lack of sophisticated communications equipment" since the Internet is available almost anywhere on the planet and with the small price required for a computer and its accessories. [129] One of Al Qa'ida's websites, alneda.com, following the loss of Al Qa'ida's geographical safe havens, ―supported Al Qa'ida's effort to disperse its forces and enable them to operate independently, providing leadership via strategic guidance."[130] Tim Thomas states, ―The Internet's potential for command and control can vastly improve an organization's effectiveness if it does not have a dedicated command and control establishment, especially in propaganda and internal coordination areas."[131] The Internet is not just a means for commanding and controlling forces for Al Qa'ida and its affiliates, but it also expands their capabilities to plan attacks and conduct data mining or open-source intelligence gathering on its enemies.

Cyberplanning

> Al-Qa'ida and its allies must not be permitted to gain or retain any capacity to plan and launch international terrorist attacks, especially against the U.S. homeland. Al Qa'ida's core in Pakistan remains the most dangerous component of the larger network, but we also face a growing threat from the group's allies worldwide. We must deny these groups the ability to conduct operational

[127] Robert D. Kaplan, *Soldiers of God.*

[128] Timothy Bailey and Michael Grimaila, ―Running the Blockade," 523-543.

[129] Timothy L. Thomas, *Cyber Silhouettes: Shadows Over Information Operations* (Fort Leavenworth: Foreign Military Studies Office (FMSO), 2005),37.

[130] Ibid., 117.

[131]Ibid.

plotting from any locale, or to recruit, train, and position operatives, including those from Europe and North America[132]

– *National Security Strategy* (2010)

According to Tim Thomas, ―Cyberplanning may be a more important terrorist Internet tool than the much touted and feared cyberterrorism option"[133] Although no source defines cyberplanning, Thomas states it ―refers to the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed."[134] Unlike physically conducting reconnaissance or surveillance, by stretching geographical distances over the Internet, terrorists can plan their attacks from anywhere in the world to be executed anywhere with little to no risk. For example, a terrorist sitting in his basement in Chicago can plan an attack on an American military installation in Europe or the Middle East by utilizing a collage of open source website information. Open source information online includes detailed satellite imagery, street maps, photos of buildings in the surrounding areas, news reports and other forms of information that can be found online using any number of Web site search engines.[135]

In fact, an Al Qa'ida manual captured in 2003, long before Google Earth and the social networking sites we have today, stated, ―Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy."[136] Perhaps that level of gatherable information is about 90% for Al Qa'ida today. A website operated by the Muslim Hackers Club even goes so far as to ―feature links to U.S. sites that purport to disclose sensitive information such as code names and radio frequencies used by the U.S. Secret Service."[137] In addition to providing cyberplanning information and providing links to other militant Islamic and terrorist websites,

[132] U.S. President, *National Security Strategy*, (May, 2010): 20.

[133] Tim Thomas, *Cyber Silhouettes,* 32.

[134] Ibid., 33.

[135] Janet Brachman and James J.F. Forest, ―Exploring the Role of Virtual Camps," in *Denial of Sanctuary*, ed. Michael Innes (Westport, CT: Praegar Security International, 2007), page 134.

[136] ―Citing Al Qa'ida Manual, Rumsfeld Re-Emphasizes Web Security," *InsideDefense.com*, http://www.insidedefense.com, 15 January 2003.

[137] Gabriel Weimann, *Terror on the Internet,* 113.

the Muslim Hackers Club offers cyberoffensive tutorials on ―creating and spreading viruses and devising hacking stratagems, undertaking network sabotage, and developing codes."[138] Despite Al Qa‘ida‘s desire to recruit high-tech operators like those in the Muslim Hackers Club, any terrorist that can use a search engine or surf the web in chat rooms and discussion groups can effortlessly and cheaply data mine information on persons or targets of interest. For example, an Al Qa‘ida laptop captured in Afghanistan possessed detailed structural information about a US dam to include effect simulations on the catastrophic damage incurred if the dam failed. Another Islamist website almotaq.org provided a link within its *how to construct explosives* section to the state of Nevada‘s website that contained a counterterrorist report on how to store and ship high-level nuclear waste, the routes for moving it, and the weapons that could be used to attack such shipments.[139]

The Internet has provided a means for terrorists to transfer information between each other with greater anonymity and lower risk than a satellite phone conversation or traditional Cold War ‗dead-drop‘ or suit-case type of exchange likely seen in the movies. Islamic terrorists can pass on ―instructions in the form of maps, photographs, directions, and technical details of how to use explosives are often disguised by means of steganography, which involves hiding messages inside graphic files."[140] Terrorists, however, don‘t even need to get that high-tech in using steganography to communicate effectively on the web. For example, Mohammad Atta‘s final email message to the other eighteen terrorists who carried out the attacks on 9/11 is reported to have read: ―The semester begins in three more weeks, We‘ve obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and

[138] Gabriel Weimann, *Terror on the Internet,* 113.

[139] Ibid., 114.

[140] Ibid., 131.

the faculty of engineering."[141] By utilizing pre-arranged code words, terrorists can plot and plan terrorist attacks almost overtly online with little fear or risk of being compromised.

Although online cyberplanning can occur from a geographical safe haven or anybody's Motorola Droid or mom's basement for that matter, it occurs through the rich and resourceful safe haven that the Internet provides. The World Wide Web is a vast digital library offering ―more than a billion pages of information, much of it free, and much of it to interest of terrorist organizations."[142] There has been no equivalent data source or means of communications for terrorists to exploit in the history of humankind like the Internet.

Fundraising

> Allah gives you the opportunity to take part in the struggle for Muslim rights—Jihad…Even if you cannot take part physically in Jihad, you can help us by the means of financial aid.
>
> – Posted online by Lashkar e-Tabya (LeT).[143]

Al Qa'ida, like many other organizations, utilizes the Internet as a means to raise funds and is heavily dependent on donations from Islamic charities, nongovernmental organizations, and other financial institutions. From a fundraising perspective, it is difficult to compare geographic versus virtual safe havens. It is best to compare fundraising capabilities before and after the introduction of the Internet to discern the impact the Internet has had on Islamic terrorist fund raising. Prior to the Internet, fund transfer occurred through the ancient *hawala* transfer system or through direct solicitation of donations in mosques or approaching potential supporters for direct donation. Sometimes funding came through state-

[141] Yossi Melman, ―Virtual Soldiers in a Holy War," *Haaretz (Israel)*, September 17, 2002. http://www.haaretz.com/print-edition/features/virtual-soldiers-in-a-holy-war-1.34332 (accessed September 15, 2010).

[142] Gabriel Weimann, *Terror on the Internet,* 111.

[143] Cited in Anti-Defamation League, ―Jihad online: Islamic terrorists and the Internet," Anti-Defamation League Web Site. Pdf file, http://www.adl.org/Internet/jihad_online.pdf. (accessed August 19, 2010).

sponsored support, like the United States funding of radical Islamic groups in Afghanistan Mujahedeen during the 1980s and Bosnian Muslims during the 1990s.

Since the advent of the Internet, fundraising, especially prior to 9/11, had been exponentially easier to conduct. Some ―terrorist web sites now solicit donations or try to raise funds through the sale of videos, audios, or other items—in some cases, even accepting credit cards or other forms of electronic payment."[144] By utilizing the Internet, terrorists can also screen demographics to target users that may have the right profile as a potential sympathizer towards a similar cause or issue and unwilling solicit donations from them through a front group usually through email.[145] This type of fundraising targeting and mass solicitation would have been almost impossible prior to the advent of the Internet. In this age of globalization and with some countries possessing looser banking regulations and laws than others, ―The Internet also provides an easy mechanism to move organizational funds from one part of the world to another, and often in a manner that is difficult (if not impossible) for government authorities to trace."[146]

Clearly, the Internet provides instant online services for fundraising to a global audience with a certain degree of anonymity that pre-Internet fundraising could not accomplish. Assuming most terrorist organizations are no longer state funded to some degree like they were prior to 9/11, the Internet does provide those organizations with another outlet for fundraising to make up for the lack of state funds. On the other hand, since 9/11 the US and its allies have aggressively sought to freeze Islamic terrorist assets and close fundraising organizations to include those operating online. The results of these efforts may link to evidence by the 2008 scientific research study by the University of Arizona‗s Dark Web AI Lab that points out that Al Qa‗ida and the other terrorist organizations show low evidence rates of fundraising online probably because ―such uses have gone underground or do not appear on the web."[147]

[144] Jarret Brachman and James J.F. Forest, ―Exploring the Role of Virtual Camps," 133.

[145] Tim Thomas, *Cyber Silhouettes,* 34.

[146] Jarret Brachman and James J.F. Forest, ―Exploring the Role of Virtual Camps," 133.

[147] Hsinchuan Chen et al., ―Uncovering the Dark Web," 1357.

Sharing Ideology: Mobilization, Recruitment, and Radicalization

> Whether Bin Laden, and [his] colleagues are on a mountain in the Hindu Kush or living with their beards shaved off in a suburb of Karachi no longer matters to the organization. They can inspire and guide a worldwide movement without physically meeting their followers - without even knowing who they are.[148]
>
> –Paul Eedle

The 2003 United States Army Field Manual FM 3-*13 Information Operations: Doctrine, Tactics, Techniques, and Procedures* has only three references to the Internet all of which are in the context of taking defensive measures against hackers. The 2007 version of FM 3-05.301 *Psychological Operations Process Tactics, Techniques, and Procedures* does little more than note the Internet‗s capabilities as an open-source of information and a dissemination outlet that should be utilized in psychological operations. FM 3-05.301 points out that the ―Internet has become an integral part of U.S. and other societies, and has become a preferred source of information in many regions of the world."[149] The United States current adversaries, primarily Al Qa‗ida and its affiliates, would concur with the United States Army doctrine‗s recent revelation of the importance of the Internet since those organizations are arguably almost completely dependent on it for a variety of operational functions. Tim Thomas states, ―Today, the spin on Arab specialist T.E. Lawrence‗s 1920 idea that ‗the printing press is the greatest weapon in the armory of the modern commander‗ would be that the Internet is the greatest weapon in the armory of the modern jihadist."[150] Thomas made this point in his article highlighting the absence of cyber-related terms in US Joint and Army doctrine and pointing out ‗cyber mobilization‗ as an overlooked modern phenomenon.

[148] Paul Eedle, ―Terrorism.com," *Guardian (London)*, July 17, 2002. http://www.guardian.co.uk/technology/2002/jul/17/alqaida.g2/print (accessed September 15, 2010).

[149] U.S. Department of the Army, *Field Manual 3-05.301 Psychological Operations Process Tactics, Techniques, and Procedures*, (Washington DC: Government Printing Office, 30 August 2007) 6-53.

[150] Timothy L Thomas, ―Cyber Mobilization: The Neglected Aspect of Information Operations and Counterinsurgency Doctrine," In *Countering Terrorism and Insurgency in the 21st Century*, ed. James J.F Forest. 3 vols. (Santa Barbara: Greenwood Press, 2007), 360.

Thomas states ―Cyber mobilization capabilities are designed to conduct psychological warfare activities, to propagandize insurgent success and counter coalition allegations, and to recruit.”[151]

Thomas stated in an oral interview with the author of this monograph that there were two milestones in the cyber mobilization use of the Internet by Islamic extremists. The first milestone was the introduction of it in the armed conflict in Chechnya and the second milestone was the beheading video of Nicholas Berg in 2004 by Al Qa‘ida in Iraq leader Abu Musab Zarqawi.[152] The year 2004 corresponds with Michael Sageman‘s assessment that ―starting around 2004, communications and inspiration shifted from face-to-face interaction at local halal ethnic restaurants or barber shops in the vicinity of radical Islamist mosques to interaction on the Internet.”[153] One must consider it was in 2004 that the insurgency in Iraq picked up significant speed with the influx of foreign fighters from across the globe to participate in Jihad against the American occupiers. The Internet, in part, was an essential part of motivating, radicalizing, and recruiting many of these foreign fighters to Iraq and arguably still is in Afghanistan. Rita Katz, author of *Terrorist Hunter* and director of the SITE Institute that monitors Islamic websites, says, ―We know from past cases—from captured Al Qa‘ida fighters who say they joined up through the Internet—that this is one of the principal ways they recruit fighters and suicide bombers.”[154]

It should be pointed out, that most Islamic websites are extremely well created with artistic qualities of attractive colored backgrounds, high quality motivational video, and inspiring music. These websites in their multiple language formats have a strategic ability to penetrate not only Middle Eastern Islamic cultures, but also cultures across the world to motivate, radicalize, recruit, and tell their side of the story to an intrigued and curious global audience. As far as recruiting and radicalizing online, Sageman, points out that online forums and the discourse that occurs within them inspires more Muslims to

[151] Tim Thomas, ―Cyber Mobilization,” 359.

[152] Tim Thomas, interview by author, Ft. Leavenworth, KS, 6 May 2010.

[153] Marc Sageman, *Leaderless Jihad,* 109.

[154] Quote by Rita Katz cited from Gabriel Weimann, *Terror on the Internet,* 120.

radicalize and participate in armed Jihad than passive yet intriguing websites.[155] Sageman goes on to state that since —physical militant sites, like radical mosques, are closely monitored by law enforcement authorities, militants have moved online. The new forums have the same influence that these radical mosques played in the previous generation of terrorists.”[156]

Through a process of self-selection to a particular forum and the egalitarianism type of society that an online forum possesses, people of all types of beliefs, likes, and interests can find each other online. No longer do people have to post ads on bulletin boards or hang out at certain places to meet or potentially recruit for the cause some like-minded individuals. The Internet‘s anonymity shields a person from the civility and social awkwardness that typically occurs in face-to-face conversations. As such, people are quite candid with one another and act or say (write) things they would not dare to in person. One sees this often in email practices as people fire off the occasionally ‗angry‘ and insulting emails in reply to all sends within organizations. This Internet phenomenon applies to every aspect of human society and social networks and not just Islamic terrorism. Within the world of Islamic extremism, numerous competing forums exist to debate and discuss Jihad. Sageman states, —The true leader of global Islamist terrorism is the collective discourse of the half-dozen influential jihadi forums.”[157] Within this discourse, Sageman points out that —some [terrorist] networks were created wholesale from [online] forums, which radicalized their members”[158] This fact is in line with the University of Arizona‘s AI Lab Dark Web study (see figure 3) that illustrates that the ‗sharing ideology‘ function is the most utilized facet of Al Qa‘ida‘s use of the Internet.

We have discussed earlier how the survival of the core of the Al Qa‘ida organization itself was in jeopardy following the US-led response in Afghanistan. Indeed, following the —post-9/11 scramble to

[155] Marc Sageman, *Leaderless Jihad,* 116.

[156] Ibid.

[157] Ibid., 118.

[158] Ibid., 115.

keep their movement motivated and coherent…the Internet became not only a useful way to replace their dismantled training camps and reconnect their weakened organizational leadership, but one of the ways to sustain the global jihadi movement."[159] The Internet serves the dual purpose of sustaining the global violent jihadi movement as a means of maintaining its current members and attaining new ones. Like any organization, new recruits are a critical requirement for Al Qa‘ida and its affiliates in order to survive. Recruiting is especially difficult and risky when operating from within an area not considered a physical safe haven. Since 9/11, the increased law enforcement attention towards Muslims demonstrating extreme Islamic views in Western, Asian, and Middle Eastern countries has driven many terrorist groups underground. Operating under these constraints, recruiters are naturally inclined to the safety and anonymity that the Internet provides. Also ―by replacing a physical base with a virtual sanctuary, counterterrorism and law enforcement authorities face a more difficult task in dismantling terrorist organizations and capturing individual terrorists."[160] Hence, not only have recruiters expanded their potential recruiting pool, but they have also increased the chances of their own survival by utilizing the Internet.

On the other hand, some studies point out that recruitment and radicalization online does not occur on the scale portrayed by others. The Combating Terrorism Center (CTC) an independent educational and research institution at the U.S. Military Academy at West Point states, ―While some sources have cited the Internet‘s role in recruitment, it is believed that few hardcore jihadists are recruited online. Much of this face-to-face recruitment is now allegedly conducted in coffee shops and clubs, avoiding conspicuous locations such as mosques."[161]

[159] Jarret Brachman and James J.F. Forest, ―Exploring the Role of Virtual Camps," 125.

[160] Aidan Kirby Winn and Vera L. Zakem, ―Jihad.com 2.0: The New Social Media and the Changing Dynamics of Mass Persuasion," in *Influence of Warfare*, ed. James Forest (Westport, CT: Praegar Security International, 2009), 28.

[161] Christopher Boucek, ―The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia," *CTC Sentinel* 1, no. 9 (August 2008): 2.

Either way, the Internet‘s ability to strategically penetrate cultures and motivate, recruit, radicalize, and gain support by financing, administrative or logistical support, or convincing somebody to be a suicide bomber is possible on the Internet. The Internet is a step in the process of radicalization and recruitment. Although the Internet may not always complete recruitment from start to finish, in many cases it often acts as a filtering screen to gain initial trust and establish the set-up for a face-to-face meeting to occur.

Virtual Training Camps

> Oh Mujadhid [holy warrior] brother, in order to join the great training camps you don‘t have to travel to other lands. Alone, in your home or with a group of your brothers, you too can begin to execute the training program. You can all join the Al Battar Training Camp.
>
> –Al Battar (the online manual of Al Qa‘ida), vol. 1[162]

―While it can easily be argued that the Internet can support most if not all of a terrorist network‘s strategic communications, the case that the Internet can act as a virtual training camp is more controversial."[163] Authors Weimann , Brachman, Forest, and Sageman utilized for sources in this monograph believe that the Internet can serve as a virtual training camp. Brachman and Forest state, ―Although these virtual combat classrooms do not render physical training camps obsolete, information technologies do change the nature of education, indoctrination, and participation."[164] Gabriel Weimann states, ―A person in the United States can literally take a terrorist training course within the privacy of their own bedroom".[165] In this sense, physical safe havens for terrorist to train exist everywhere, not just in remote ungoverned space locations of Waziristan, Somalia, or Yemen. The evidence of such Do-It-

[162] Steven Coll and Susan B. Glasser, ―Terrorists Turn to the Web as base of operations," *Washington Post*, August 7, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138_pf.html (accessed September 15, 2010).

[163] David Gray and Albon Head, ―The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven," 400.

[164] Jarret Brachman and James J.F. Forest, ―Exploring the Role of Virtual Camps," 131.

[165] Gabriel Weimann, ―Terror on Facebook, Twitter, and YouTube," 53.

Yourself-Terrorist manuals combined with online radicalization has often made headlines in the past two years with the increase in ‗homegrown terrorists‘ in the United States and Great Britain in particular. As of February 2010 , the ―30-odd attempted terrorist plots against the United States…that have been foiled since 9/11, roughly a third have been uncovered in the past year alone."[166] Most of these ―budding perpetrators were initially indoctrinated inside the United States, with help from extremist websites or Islamic preachers."[167] These incidents, within the United States, most of them committed by American Citizens who embraced radical Islam, illustrates that with the loss of geographic safe havens for Al Qa‘ida, online training is the next best alternative. Paul Eedle points out, ―[Al Qa‘ida operatives] have to replace their physical bases in Afghanistan somehow and so long as there is a small number of highly trained people to lead groups, then these detailed manuals of how to write recipes for explosives are all crucial."[168]

These videos and manuals exist all over the Internet for all types of insurgents, criminals, and other terrorist organizations to harvest as either groups or individuals. A large proportion of these distance learning activities of terrorist-related material available on the Internet is meant to inspire individual action with the primary goal of providing a ―global audience with the knowledge of how and why to conduct a terrorist attack."[169] Without this individual action and without the type of terrorist training camps that existed prior to 9/11, these terrorist organizations and movements would risk stagnation and atrophy, similar to sharks, they must continue to move and attack in order to survive.[170]

[166] James Kirchick, ―The Homegrown Terrorist Threat," *commentary magazine*, February 2010. http://www.commentarymagazine.com/viewarticle.cfm/the-homegrown-terrorist-threat-15345 (accessed September 15, 2010).

[167] Ibid.

[168] Paul Eedle, interview by Tony Jones, *Lateline*, Australian Broadcasting Company, March 18, 2004.

[169] Jarret Brachman and James J.F. Forest, ―Exploring the Role of Virtual Camps," 133.

[170] Ibid.

Hamas is one of the first organizations to publish training manuals online with *The Mujahedeen Poisons Handbook* in 1996.[171] The manual had 23 pages of material on how to ―prepare various homemade poisons, poisonous gases, and other deadly materials for use in terror attacks."[172]Al Qa'ida started publishing its first virtual training manual *Al Batter* in 2002, which was improved upon with its bimonthly online edition of *Al Batter Training Camp* beginning in 2004.[173] Recently a US federal jury convened to review evidence against Samir Khan a 24-year-old who ran a militant Islamic website out of his parents' basement in North Carolina. Khan is suspected of being behind the Al Qa'ida magazine *Inspire*. *Inspire*, a 67-page magazine published online in June 2010, ―slapped snappy titles on terrorist advice columns like "Make a Bomb in the Kitchen of Your Mom" and ran items like a packing guide for what to take on a jihad trip."[174]

On the other side of the debate over whether or not the Internet's virtual training camps can replace actual physical camps are two scholars, Anne Stenersen and Petter Nesser. Stenersen argues that ―in order to call the Internet a virtual training camp, it has to represent more than just a place for storing and distributing training material" and concludes that Al Qa'ida is not making an ―organized training effort" to train its followers online.[175] Nesser tends to agree with Stenersen that the concept of virtual training camps is questionable. Nesser concludes in a survey conducted of European Islamic terrorists that ―the Internet indeed functioned as a practical tool for terrorists, both for recruitment and radicalization,

[171] Gabriel Weimann, *Terror on the Internet,* 121.

[172] Ibid., 123.

[173] Ibid., 128.

[174]Dina Temple-Raston, ―Grand Jury Focuses on N.C. man Tied to Jihad," *NPR*, August 22, 2010. http://www.npr.org/templates/story/story.php?storyId=129263809 (accessed September 15, 2010).

[175]A. Stenerson, ―The Internet: A Virtual Training Camp?" *Terrorism and Political Violence* 20 (April 2, 2008): 215-33.

and tactical purposes. However, [his survey] also suggests that the role of the Internet as a ―training camp" might be overstated."[176]

Despite the debate, no one debates that the publication of training videos and manuals is helpful to terrorists and the quality of training cannot replace the quality associated with actual hands-on training. Marc Sageman makes a good point that ―when such expertise acquired in a terrorist training camp is combined with an informal Internet network, the results can be literally devastating."[177] With the current risks associated with possessing actual training camps and the ―leaderless jihad" decentralization of Al Qa'ida and its affiliates, however, we can expect to see virtual training camps and those terrorists studying them online for sometime into the future.

Conclusion

> Al Qa'ida has become the first guerilla movement in history to migrate from physical space to cyberspace. With laptops and DVDs, in secret hideouts and at neighborhood Internet cafes, young code-writing jihadists have sought to replicate the training, communications, planning, and preaching facilities they lost in Afghanistan with countless new locations on the web.[178]
>
> –Steven Coll and Susan B.Glasser

With the limited geographical safe havens available to Al Qa'ida, its current decentralized social movement form, and the global audience and safety associated with the Internet, this author believes that the Internet as a safe haven is more important than geographical safe havens to Al Qa'ida and its affiliates at this time. It was the US military's direct approach strategy against Al Qa'ida's leadership and geographical sanctuaries that defeated Al Qa'ida in Afghanistan in 2002 and again in Iraq during the Surge from 2007-2008, forcing Al Qa'ida to adapt to survive by moving the majority of its operations to

[176] Petter Nesser, ―How did Europe's Global Jihadis Obtain Training for their Militant Causes," *Terrorism and Political Violence* 20 (April 2, 2008): 234-56.

[177] Marc Sageman, *Leaderless Jihad,* 115.

[178] Steven Coll and Susan B. Glasser, ―Terrorists Turn to the Web as base of operations," *Washington Post*, August 7, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138_pf.html (accessed September 15, 2010).

the domain of the Internet. The Internet safe haven sustains Al Qa‘ida as it is a source of both moral and physical strength and enables almost complete freedom of action. It is arguable that the Internet over the last few years, due to its increasing importance to Al Qa‘ida and its affiliates, has now become Al Qa‘ida‘s new operational center of gravity. Despite this, the —USstrategy to date has largely assumed that America‘s contemporary enemies…have a traditional center of gravity and that they can be defeated primarily by targeting bad guys."[179] Despite the initial success with this direct approach strategy in Afghanistan and again during the Surge in Iraq, this approach has also resulted in long bloody counterinsurgencies in both Iraq and Afghanistan primarily against mostly local Sunni and Afghan Taliban insurgents instead of the transnational Al Qa‘ida terrorist organization that served to justify American involvement in the first place. According to Dell Dailey, the State Department‘s counterterrorism chief, —AlQa‘ida and other terrorists‘ center of gravity lies in the information domain, and it is there that we must engage it."[180] While conducting research for this monograph, the consensus amongst numerous sources was that the United States is doing a poor job at engaging Al Qa‘ida and other terrorists within its new center of gravity. Operational centers of gravity tend to change during wars; this war is no different, as Al Qa‘ida has clearly adjusted its operational center of gravity to the Internet while the United States continues to engage Al Qa‘ida‘s 2001 operational center of gravity on the ground. This is perhaps because a geographical place with an enemy existing within it is something that the United States is more comfortable with in challenging. You can find and eliminate this type of threat by traditional military power.

[179] Bruce Hoffman, Foreword for *Influence of Warfare*, ed. James Forest (Westport, CT: Praegar Security International, 2009),28

[180] Eric Schmitt and Thom Shanker, —US Adapts Cold War Idea to Fight Terrorists," *New York Times*, March 18, 2008. http://www.nytimes.com/2008/03/18/washington/18terror.html?_r=1 (accessed September 15, 2010).

The Internet is a much more complex problem to tackle as a terrorist sanctuary. One can shut down an Islamic website only to see it reopen a few hours later at another IP address on another server. It is the ultimate problem that keeps popping up. The Internet as a terrorist safe haven is a wicked, ill-structured complex problem that empowers individuals over nations, involves religion, possesses incredible technologies, neutralizes sovereignty, challenges civil liberties, endangers security, questions laws, and generates violence. Moreover, they are all linked together in a literal world-wide dark web.

Again, most politicians, generals, political pundits, and the American people for that matter justify American presence in Afghanistan, for almost 10 years now, as part of the effort to deny Afghanistan from becoming once again a terrorist sanctuary. Is this justification sufficient if those same terrorists can accomplish their same planning and training requirements online now instead of Afghanistan or some other geographic safe haven? What does this say about the United States entire strategy to disrupt, defeat, and Al Qa‘ida and its affiliates? What does this imply about America‘s strategy in Afghanistan and Pakistan? What safe haven and battlefield is more important, the one against an enemy entity that largely exists within the comfort, freedom, and safety of a ‗virtual‘ safe haven online from a basement in London or Detroit or the geographic ones in Mogadishu, Yemen, Kandahar, or Waziristan? Where is the tipping point between the intelligence value of monitoring Islamic terrorists websites and allowing an online safe haven exploit young Muslims to radicalize and commit acts of terror? These are just some of the questions the US must ask itself while it continues fighting a counterinsurgency and counterterrorism war in Afghanistan and elsewhere.

Meanwhile, despite some cyber-capabilities the US military possesses to disrupt, dismantle, and defeat Al Qa‘ida‘s Internet safe haven, it is currently constrained by US law from doing so. This is in addition to the fact that this virtual conflict is very much outside the scope of traditional military duties and responsibilities. The United States military, however, does understand the threat that hostile nations, hackers, ―hactivists”, and terror organizations pose to the American government and military‘s own Internet dependence. As such, the United States recently established Cyber Command, called CYBERCOM, headed by a four-star general that inherited the Internet Area of Operations. This author hopes CYBERCOM possesses more operational flexibility to aggressively both shut down Islamic websites forums worldwide and manipulate them by actively participating within them anonymously to battle in this ―War of Ideas” in cyberspace.

This United States Government‘s and US military‘s hesitancy to adapt and participate in this new virtual war reminds the author of the hesitancy of the American military to accept and adapt to nation-building stability operations witnessed earlier decade. Although one may say the Internet just makes Al Qa‘ida appear bigger and tougher than it really is. Be reminded that it only took 19 hijackers to execute 9/11 and change the American military and the world environment we all live in. The United States Army, like Al Qa‘ida, must adapt to this new environment if it wants to ever truly ‗disrupt, dismantle, and defeat Al Qa‘ida and its affiliates‘. Many think we are in a War of Ideas against radical Islam, while others think what we are witnessing today is a historical anomaly outside the historical propensity of war that will fade away over time. Either way, one of the fronts in today‘s war against Al Qa‘ida is online and the United States needs more than a defensive firewall there to fight it. Further research and reframing of US military doctrine, US government strategic policy, and United States laws affecting civil liberties on this topic of the Internet as a safe haven is encouraged. Otherwise, the United States may be bound to a persistent conflict that it may never really win. There will be nothing virtual about it.

APPENDIX

Definitions

Cyber-Terrorism-(FBI)- A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and /or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.[181]

Or

Cyber-Terrorism-Cyberterrorism is the convergence of cyberspace and terrorism. It referrers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to quality as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures would be acts of cyberterrorism, depending upon their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[182]

Cyber attack- Cyber attack actions combine computer network attacks with other enabling capabilities (Such as electronic attack, physical attack, and others) to deny or manipulate information and/or infrastructure.[183]

Cyber defense- Cyber defense actions that combine information assurance, computer network defense, to include response actions, and critical infrastructure protection with enabling capabilities (such as electronic protection, critical infrastructure support, and others) to prevent, detect, and ultimately respond to an adversaries ability to deny or manipulate information and/or infrastructure. Cyber defense is integrated with the dynamic defensive aspects of CyberWar to provide defense in depth.[184]

Cyber exploitation- Cyber exploitation is actions combining computer network exploitation with enabling capabilities (such as Signal Intelligence and others) for intelligence collection and other efforts.[185]

Cyber situational awareness- The immediate knowledge of friendly, adversary, and other relevant information regarding activities in and through cyberspace and the electromagnetic spectrum. It is

[181] U.S. Department of Army, DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism*, (Fort Leavenworth, KS, August 15, 2005). Glossary-1.

[182] House Committee on Armed Services, *Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism by Dorothy Denning*, May 23, 2000.

[183] U.S. Department of the Army, *TRADOC Pamphlet 525-7-8 Cyberspace Operations Concept Capability Plan 2016-2028,* 67.

[184] Ibid.

[185] Ibid.

gained from a combination of intelligence and operational activity in cyberspace, the electromagnetic spectrum, and in the other domains, both unilaterally and through collaboration with our unified action and public-private partners.[186]

Cyberspace warfare- The component of cyber operations that extends cyber power beyond the defensive boundaries of the global information grid to detect, deter, deny, and defeat adversaries. CyberWar capabilities target computer and telecommunication networks and embedded processors and controllers in equipment, systems, and infrastructure. Cyberwar uses cyber exploitation, cyber attack, and dynamic cyber defense in a mutually supporting and supported relationship with cyber network operations and cyber support.[187]

Dynamic cyber defense- Dynamic cyber defense actions combine policy, intelligence, sensors, and highly automated processes to identify and analyze malicious activity, simultaneously tip and cue and execute preapproved response actions to defeat attacks before they can do harm. Dynamic cyber defense uses the Army defensive principles of security, defense in depth, and maximum use of offensive action to engage cyber threats. Actions include surveillance and reconnaissance to provide early warnings of pending enemy actions. Dynamic cyber defense is integrated with the defensive aspects of cyber network operations to provide defense in depth.[188]

Safe haven-A place or situation that enables illicit actors to operate while evading detection or capture, including ungoverned, under-governed, misgoverned, or contested physical areas or exploitable non-physical areas (virtual) where illicit actors can organize, plan, raise funds, communicate, recruit, train, and operate in relative security.[189]

Ungoverned Area- A place where the state or the central government is unable or unwilling to extend control, effectively govern, or influence the local population, and where a provincial, local, tribal, or autonomous government does not fully or effectively govern, due to inadequate governance capacity, insufficient political will, gaps in legitimacy, the presence of conflict, or restrictive norms of behavior…In this sense, ungoverned areas are considered *potential* safe havens.[190]

[186] Ibid., 68.

[187] Ibid.

[188] Ibid.

[189] U.S. Department of Defense, *Ungoverned Areas and Threats from Safe Havens* by Robert D. Lamb. Prepared for the Office of the Under Secretary of Defense for Policy. (Washington, DC, 2008) 6.

[190] Ibid.

BIBLIOGRAPHY

al Libi, Abu Yahya. —Shaykh Abu Yahya al-Libi-To the Army of Difficulty in Somalia-Muharram." WorldAnalysis.net. http://worldanalysis.net/postnuke/html/index.php?name=News&file=article&sid=209 (accessed September 15, 2010).

Anti-Defamation League. —Jihad online: Islamic terrorists and the Internet." Anti-Defamation League Web Site. Pdf file, http://www.adl.org/Internet/jihad_online.pdf. (accessed August 19, 2010).

Arquilla, John, and David Ronfeldt. —Cyberwar is coming!" In *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, Calif.: RAND Corporation, 1997.

Bailey, Timothy, and Michael Grimaila. —Running the Blockade: Information Technology, Terrorism, and the Transformation of the Islamic Mass Culture." *Terrorism and Political Violence* 17, no. 3 (Spring/Summer 2005): 523-43.

Baumann, Robert F. —Compound Warfare Case Study: The Soviets in Afghanistan." in *Compound Warfare*: *That Fatal Knot*, edited by Thomas Huber, 285-306. Leavenworth,KS: U.S. Command and General Staff College Press, 2002.

Boucek, Christopher. —The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia." *CTC Sentinel* 1, no. 9 (August 2008): 1-28.

Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity.* New York: Columbia University Press, 2009.

Brachman, Janet, and James J.F. Forest. —Exploring the Role of Virtual Camps." In *Denial of Sanctuary*. Edited by Michael Innes. Westport, CT: Praegar Security International, 2007.

Bruscino, Thomas A. —Out of Bounds-Transnational Sanctuary in Irregular Warfare." in —Global War on Terrorism," Special issue, *Occasional Paper* 17 (2006).

Bunt, Gary R. *iMuslims-Rewiring the House of Islam.* Chapel Hill: The University of North Carolina Press, 2009.

Chen, Hsinchun et al. —Uncovering the Dark Web: A Case Study of Jihad on the Web." *Journal of the American Society for Information Science and Technology* 59, no. 8 (January 4, 2008): 1347-59.

—Citing Al Qa'ida Manual, Rumsfeld Re-Emphasizes Web Security." InsideDefense.com. http://www.insidedefense.com (accessed September 15, 2010).

Cohen, Eliot A., and John Gooch. *Military Misfortunes: The Anatomy of Failure in War*. New York: Free Press, 1990.

Friedman, Thomas. *The World is Flat: A Brief History of the 21st Century.* New York: Picador/Farrar, Straus, and Giroux, 2007.

Gray, David and Albon Head. ―The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven." *European Journal of Scientific Research* 25, no.3 (2009): 396-404.

Hart, B. H. Liddell. *Strategy*. 2nd ed. New York: Signet, 1974.

Hoffman, Bruce. Foreword for *Influence of Warfare*. Edited by James Forest. Westport, CT: Praegar Security International, 2009.

Huntington, Samuel P. *The Clash of Civilizations and the Remaking of the New World Order*. New York: Touchstone, 1996.

Innes, Michael A. ―Cracks in the System: Sanctuary and Terrorism After 9/11." In *Denial of Sanctuary*, edited by. Michael Innes 1-20. Westport CT: Praegar Security International, 2007.

―Internet usage in the Middle East." Internet World States. http://www.Internetworldstats.com/stats5.htm (accessed September 15, 2010).

Johnson, Steven. *Emergence: The Connected Lives of Ants, Brains, Cities, and Software.* New York: Scribner, 2001.

Kaplan, Robert D. *Soldiers of God- With Islamic Warriors in Afghanistan and Pakistan.* New York: Vintage Departures, 2001.

Kittner, Christina C. Brafman. ―The Role of Safe Havens in Islamic Terrorism." *Terrorism and Political Violence* 19, no. 3 (Spring/Summer 2005).

Marion, Russ and Mary Uhl-Bien. ―Complexity Theory and Al-Qaeda: Examining Complex Leadership." Presentation given at Managing the Complex IV: A Conference on Complex Systems and the Management of Organizations, Fort Meyers, FL, December 2002.

Mir, Hamid. ―Interview of Osama Bin Laden." *Daily Pakistan*, March 18, 1997.

Nesser, Petter. ―How did Europe's Global Jihadis Obtain Training for their Militant Causes." *Terrorism and Political Violence* 20 (April 2, 2008): 234-56.

Rabasa, Angel et al. *Ungoverned Territories: Understanding and Reducing Terrorism Risks*. Santa Monica, CA: Rand Corporation, 2007.

Rashid, Ahmed. *Taliban: Militant Islam, Oil & Fundamentalism in Central Asia.* New Haven: Yale University Press, 2001.

Ryan, Alex. ―The Foundation for an Adaptive Approach: Insights from the Science of Complex." *Australian Army Journal* VI, no.3 (Summer 2009): 70-88.

Sageman, Marc. *Leaderless Jihad-Terror Networks in the Twenty-First Century.* Philadelphia: University of Pennsylvania Press, 2008.

Sardar, Ziauddin. —Paper, Printing, and Compact Disks: The Making and Unmaking of Islamic Culture." *Media, Culture, & Society* (January 1993).

Scheffer, Jaap de Hoop. —Public Diplomacy in NATO-led Operations." NATO Secretary General address, Copenhagen, October 8, 2007.

Scheuer, Michael. *Through our Enemies' Eyes-Osama bin Laden, Radical Islam, and the Future of America*. Washington, D.C: Potomac Books, Inc., 2006.

Stenerson, A. –The Internet: A Virtual Training Camp?" *Terrorism and Political Violence* 20 (April 2, 2008): 215-33.

Thomas, Timothy L. —Countering Internet Extremism." *IOsphere* (Winter 2009): 16.

Thomas, Timothy L. —Cyber Mobilization: The Neglected Aspect of Information Operations and Counterinsurgency Doctrine." In *Countering Terrorism and Insurgency in the 21st Century*, edited by James J.F Forest. 3 vols. Santa Barbara: Greenwood Press, 2007.

Thomas, Timothy L. *Cyber Silhouettes: Shadows Over Information Operations*. Fort Leavenworth: Foreign Military Studies Office (FMSO), 2005.

Thomas, Timothy L. —Manipulating the Mass Consciousness: Russian & Chechen —Information War" tactics in the second Chechen-Russian Conflict.*"* in *The Second Chechen War*, edited by Anne Aldis. London: Conflict Studies Research Centre. UK Ministry of Defense, June 2000.

U.S. Congress. House. Committee on Armed Services, Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism by Dorothy Denning, May 23, 2000.

U.S. Department of the Army. *Field Manual 3-0 Operations*. Washington, DC: Government Printing Office, February 27, 2008.

U.S. Department of the Army. *Field Manual 3-05.301 Psychological Operations Process Tactics, Techniques, and Procedures*. Washington DC: Government Printing Office, 30 August 2007.

U.S. Department of the Army. *Field Manual 3-24 Counterinsurgency.* Washington DC: Government Printing Office, December 15, 2006.

U.S. Department of the Army. *Field Manual 6-0 Mission Command-Command and Control of Army Forces*. Washington, DC: Government Printing Office, August 11, 2003.

U.S. Department of the Army. *TRADOC Pamphlet 525-7-8, The U.S. Army Concept Capability Plan for Cyberspace Operations 2016-2028*. Washington, DC: Government Printing Office, February 22, 2010.

U.S. Department of Defense. *Joint Publication 1-02 Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, (As amended through April 2010).

U.S. Government. *National Security Strategy for Combating Terrorism*. Washington DC: Government Printing Press, 2006.

U.S. Department of Defense. *Ungoverned Areas and Threats from Safe Havens* by Robert D. Lamb. Prepared for the Office of the Under Secretary of Defense for Policy. Washington, DC: Government Printing Office, 2008.

U.S. President. *National Security Strategy*. (May, 2010).

Wass de Czege, Huba. ―Warfare by Internet-The Logic of Strategic Deterrence, Defense, and Attack." *Military Review* XC, no. 4 (July-August 2010).

Weimann, Gabriel. ―Terror on Facebook, Twitter, and YouTube." *The Brown Journal of World Affairs*
16, no. 11 (Spring/Summer 2010): 45-54.

Weimann, Gabriel. *Terror on the Internet: The New Arena, The New Challenges*. Washington, DC: United States Institute of Peace Press. 2006.

Winn, Aidan Kirby, and Vera L. Zakem. ―Jihad.com 2.0: The New Social Media and the Changing Dynamics of Mass Persuasion." In *Influence of Warfare*. Edited by James Forest. Westport, CT: Praegar Security International, 2009