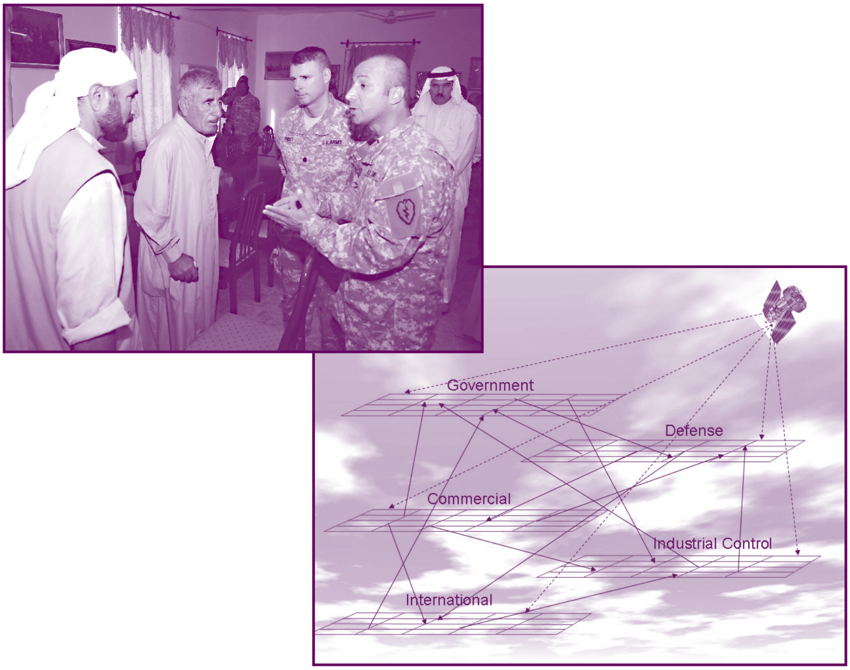

INFORMATION AS POWER

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

VOLUME 5

Edited by
Jeffrey L. Caton, John H. Greenmyer,
Jeffrey L. Groh, and William O. Waddell

INFORMATION IN WARFARE GROUP, U.S. ARMY WAR COLLEGE

US ARMY WAR COLLEGE

INFORMATION AS POWER

VOLUME 5

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

Information as Power is a refereed anthology of United States Army War College (USAWC) student papers related to information as an element of national power. It provides a medium for the articulation of ideas promulgated by independent student research in order to facilitate understanding of the information element of power and to better address related national security issues. The anthology serves as a vehicle for recognizing the analyses of Army War College students and provides a resource for USAWC graduates, senior military officers, and interagency national security practitioners concerned with the information element of national power.

Special thanks to Jerry D. Johnson for his significant editorial and administrative support, to Ritchie Dion for his meticulous layout editing, and to Jennifer Nevil for the cover design.

Information as Power

INFORMATION AS POWER

An Anthology of Selected United States Army War College Student Papers

Volume Five

Editors:

Jeffrey L. Caton, John H. Greenmyer,
Jeffrey L. Groh, William O. Waddell

Information as Power

An Anthology of Selected United States Army War College Student Papers

Volume Five

Executive Agent for the Anthology:
United States Army War College

The views contained in this publication are those expressed by the authors and do not necessarily reflect the official policy or position of the United States Army War College, the Department of Defense, or any other Department or Agency within the United States Government. This publication is cleared for public release; distribution is unlimited.

Published January 2011.

This publication is available on line at the following:

http://www.carlisle.army.mil/dime or,

http://www.csl.army.mil/InfoAsPower.aspx

Cover photograph by Staff Sgt. DeNoris A. Mickle, USAF.
Used by permission.

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

Contents

Preface

The Information in Warfare Working Group (I2WG) of the U.S. Army War College (USAWC) is pleased to present this anthology of selected student work from Academic Year 2010 representing examples of well-written and in-depth analyses on the vital subject of Information as Power. This is the fifth volume of an effort that began in 2006. The I2WG charter calls for it to coordinate and recommend the design, development and integration of content and courses related to the information element of power into the curriculum to prepare students for senior leadership positions. This publication is an important component of that effort.

Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents, to include the 2010 National Framework for Strategic Communication and the current National Security Strategy, allude to different aspects of information but without a holistic, overarching strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power… and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[3] Information as power is wielded in a complex environment consisting of the physical, informational, and cognitive dimensions.

The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and even individuals to cognitively affect strategic outcomes with minimal information infrastructure and little capital expenditure.

Anyone with a camera cell phone and personal digital device with Internet capability understands this. Adversary use of information as an asymmetric strategic means has been extremely effective in Iraq and Afghanistan. On the other hand, the U.S. government and its military exploit the capabilities of cyberspace to communicate effectively, conduct daily business and plan and execute military operations. This capability, however, becomes a vulnerability of dependence that can be targeted by rogue individuals, criminals and adversary nation states. Clearly, managing the message while controlling the necessary technological means represent critical opportunities and challenges.

U.S. strategic thought on these issues has advanced over the past five years as has the research and analysis of our students about these information-related topics. "Information as Power" is reflective of that intellectual evolution. We've moved from a discussion of what defines strategic communication in Volume 1 to the value of narrative to understand and affect culture, and the importance of religion to national security in the current volume. We've shifted from a focus on network centric operations to strategic and operational analysis of cyberspace. As such, the anthology serves not only to showcase the efforts of the College but to inform the broader body of knowledge as the Nation struggles to operate effectively within this environment and to counter current and potentially future adversaries who so effectively exploit it.

Professor Dennis M. Murphy
Chair, Information in Warfare Working Group
United States Army War College

Section One

Information Effects in the Cognitive Dimension

Prudens
Futuri

Introduction

John H. Greenmyer III
Director of Information Operations and C4
Department of Military Strategy, Planning and Operations
U.S. Army War College

This section focuses on information effects in the cognitive dimension that are undertaken to influence a target audience's perceptions and attitudes, ultimately leading to a change in behavior. Despite our need for these effects in today's conflict, Dr. William Rosenau noted that "it is clear to most informed observers that the United States has so far failed to conduct anything approaching an effective counter-ideological campaign against al-Qaida."[1] This section examines several aspects of our information efforts and presents recommendations for how they might be improved.

First, Lieutenant Colonel John Baskerville examines the cultural setting of Hezbollah's information narrative in order to explain the moral and material support the organization enjoys in Lebanon. His paper provides a perspective on how Hezbollah has insinuated itself into the framework of Lebanese society. In light of this, Colonel Baskerville recommends that the United States avoid direct confrontation with Hezbollah, while seeking to gradually co-opt and absorb their state-like operations and organizations into the state framework.

Chaplain (Colonel) Jonathan Shaw discusses the varying ways the Bush and Obama administrations have portrayed religion, the former as a matter of basic freedom and the latter as a unifying force among all the Earth's peoples. Chaplain Shaw moves on to a thorough, objective analysis of Islamic beliefs concerning jihad and support for terrorism which is reason enough to read this paper. In conclusion, Shaw suggests that the administration adopt a policy of portraying "religion as ideology" and provides a discussion of practical issues regarding implementation of his suggestion.

Colonel Thomas D. Mayfield III next contributes an article which discusses how new media fit into the "ends, ways and means" paradigm of strategy. Mayfield uses the 2009 demonstrations in Iran as well as Israel's operations against Hezbollah in 2006 and 2009 to illustrate the effect of new media in operations. Colonel Mayfield then builds on this background to show how a strategy could be developed to employ new media and offers specifics of ends, ways and means defining such a strategy.

Finally, Lieutenant Colonel Thomas A. Davis reviews gaps between structure of the Department of Defense strategic communication enterprise and the nation's requirements for communication strategies. Colonel Davis examines the history and shortfalls of previous strategic communication organizations within DoD, and suggests the creation of a single organization to provide strategic vision and guidance as well as setting priorities and allocating resources. These insights could prove particularly useful in light of the recent creation of the Directorate for Information Operations and Strategic Effects in the Office of the Undersecretary of Defense for Policy.

Together, the perceptive observations and careful analysis in these papers provide valuable insight into the issues surrounding the information element of national power as it is being applied in today's world.

Narratives of Empowerment: A Cultural Analysis of Hezbollah

Lieutenant Colonel John C. Baskerville, Jr.
United States Army

In his opening remarks at the 2010 Arab International Forum for Support of the Resistance, Hassan Nasrallah, the Secretary General of Hezbollah, announced that "Lebanon has abandoned the myth saying 'Lebanon's strength is in its weakness' to adopt the truth saying 'Lebanon's strength is in the solidarity of its army, people, and resistance'."[1] Two themes readily emerge from this brief statement. First, it implies a transformation in the Lebanese outlook – away from embracing 'weakness' by rationalizing it as an asset – toward embracing actual 'strength'.[2] Second, in what almost appears as an adaptation of Clausewitz's remarkable trinity, it presents a concept of three public entities that comprise an empowered Lebanese state – its army, its people, its resistance. This brief statement that re-conceptualizes the strength of the Lebanese state and presents Hezbollah (the key entity of the "resistance") as an integral component of an empowered state, serves as a point of departure for this culture-focused analysis of how Hezbollah situates itself as part of the above trinity. The interaction between Hezbollah's efforts to situate itself in Lebanon and U.S. policy in Lebanon – aimed largely at coaxing the Lebanese government to take control of Hezbollah-dominated territories in the south and disarm the group – forms the basis for this study.

One should understand Hezbollah's efforts to situate itself in the Lebanese state through the framework of sectarian politics, fragmentation, and outsider influence that have characterized the Lebanese state since its inception. In 1920, France carved what is today's Lebanon out of the territories of its post-WWI Syrian mandate by adding the Biqa valley, along with the cities of Tripoli, Beirut, Sidon, and Tyre (and their surrounding environs) to the Christian-dominated district of Mount Lebanon. This entity, designated as Greater Lebanon, comprised numerous communities from 18 religious sects, some with significant histories of political and social strife, often fomented and facilitated by external patrons. Upon becoming an independent state in 1943, Lebanon's leaders adopted a National Pact that endeavored to strike a delicate balance of accepting its Arab identity while limiting its Christian population's propensity toward western orientation, maintaining an independent nature by not letting itself be absorbed or dominated by its Arab neighbors, and fairly distributing political positions among the major sects.[3] However, Lebanon's history is replete with events that betray the frailty of the arrangement. The 1958 civil war exposed the tensions in balancing Lebanon's Arab versus western orientation. The 1975-1990 civil war exposed weaknesses in the fragmented state as the Palestinian Liberation Organization's (PLO) use of Lebanon as a base of operations became a flash point for sectarian strife that drew Syria and Israel into a mix of fierce sectarian violence and a struggle for regional influence.

Hezbollah's roots are in the turmoil of the 1975-1990 civil war. Specifically, the group crystallized in 1982 in the wake of Israel's second invasion into southern Lebanon. Hezbollah represented the amalgamation of numerous internal and external religious and secular resistance entities that found a common cause in repelling the Israeli invasion, but whose genesis and fervor stemmed not only from the invasion, but from causes such as the 1979 Iranian Revolution and decades of movements aimed at mobilizing Lebanon's Shi'a community.[4] There is a vast literature on Hezbollah and its wide array of activities and characterizations that run the gamut from terrorist organization to service-rendering group to political party with armed militias. The intent of this study is not to replicate this literature, but to present a nuanced perspective on the group. This study situates the group within the Lebanese milieu and provides a deeper understanding of its entrenchment within Lebanon through a cultural analysis that reveals the group's pillars of support – empowerment of the Shi'a community and national dignity through resistance to Israel and the West.

Hezbollah's ceremonies, narratives, and institutions communicate to the Shi'a of Lebanon that their community has shed a backward, dispossessed, and uncivilized past and embraced a modern, empowered, and orderly present. Hezbollah embodies this empowered state of being. Hezbollah's narratives and use of images convey to the larger Lebanese population that the "resistance" is an integral part of a modern, alternative landscape in which the "resistance" has led an historic transformation of Lebanese weakness and Arab humiliation into national strength and pan-Arab dignity.[5] This culture-informed understanding of Hezbollah's entrenchment in Lebanese society suggests that U.S. objectives of having the Lebanese government take control of Hezbollah-controlled territory and disarm the group will not occur through direct confrontation or an abrupt uprooting of the group and all that it represents of empowerment and dignity. The process will likely unfold at a slow, measured pace and will entail the United States aiding the Lebanese government to redirect concepts of empowerment and dignity away from the "resistance," while co-opting and absorbing Hezbollah's services and militias into the state framework.

Culture as "Perspective"

Before delving into a cultural analysis of Hezbollah, it is important to establish a basic framework for what culture is and how cultural knowledge benefits the policymaker. The following definition of culture serves as a basis for this analysis:

> …the way humans and societies assign meaning to the world around them and define their place in that world. It is manifested in many ways including languages and words; ideas and ideologies; customs and traditions; beliefs and religions; rituals and ceremonies; settlement patterns; art and music; architecture and furniture; dress and fashion; games; images; in short, anything that is symbolic or representative of the values, norms, perceptions, interests, and biases…[6]

While this definition is just one among dozens, if not hundreds, of potential definitions of culture in various academic, corporate, and military domains, its utility rests in the fact that it captures the key elements of culture that transcend domains: values, norms, perceptions, interests, and biases, and their tangible and intangible manifestations.

These elements coalesce into the notion of perspective, denoting here, very simply, how one interprets and makes larger sense of what one experiences and observes. As regards the formulation of national policy and strategy – addressing issues through applying elements of national power in such a way as to achieve national interests – one can hardly overstate the value of understanding perspective, especially of those affected by policy and whose reaction to it may play a role in its success or failure.[7] This study demonstrates how cultural knowledge serves as a foundation for an informed, nuanced understanding of perspective, including: relevant actors and observers' perspectives on various issues and how they situate themselves in those issues; what individuals and entities tap into various views and why and how they reinforce them, modify them, or turn them on their heads; and what the implications of various perspectives are for the actions and words of key actors.

Through its delineation of cultural manifestations, the base definition provides examples of where one might find clues or key indicators of how others evaluate and interpret the world around them and their place in it. However, a fundamental argument of this study, not explicitly noted in the definition, is that from the strategic standpoint one must look at these manifestations through the lenses of dynamism and negotiation.[8] The introduction of dynamism proposes that the culture that is important to the formulators of national policy is not a static interpretation of texts or a fixed set of rituals or images. For, just as one's own policy and strategy interject words, ideas, and actions into the lives of different groups, historical events have done the same and have been incorporated into or otherwise left their enduring marks on narratives, images and traditions. For instance, the next section demonstrates how the traditions and ceremonies associated with the battle of Karbala (680 A.D.) – an event and narrative essential to a base understanding of Shi'a Islam – have evolved in Lebanon and how understanding the evolution of this cultural tradition is relevant to understanding the range of what Hezbollah represents within various communities in Lebanon.

Negotiation, as it applies to this study, conveys that the reinforcement or remolding of perspective – as seen through adaptations of cultural manifestations – occurs as part of a process whereby actors present viewpoints and interpretations that are subject to levels of acceptance, rejection, and further remolding. Implied here are two key points.

The first is that the dynamism that is vital to analyzing culture at the strategic level is not just due to the occurrence of historical events, but to individual and group interpretations of these events.[9] The second point is that the result of this negotiation is not likely to be one clean, uncontested perspective or view that one can glean from a culture fact sheet. So, this study, for example, does not concern itself with how a particular Shi'a tradition may drive Shi'a community perceptions of Hezbollah as freedom fighters who are on earth to fulfill a mission of righting a historical wrong. Instead, it concerns itself with how historical events, and more importantly Hezbollah's interpretations of these events, through cultural manifestations, influence Shi'a and larger Lebanese perspectives on the group that range along a spectrum from rogue, sectarian, unlawfully-armed group to a legitimate national resistance that is in "harmony with the state"[10] and is an organic element in the Lebanese social landscape.

Of Community Empowerment and National Resistance

As its military rained shells on Beirut and its environs in July and August of 2006, the Israeli political leadership echoed what sounded like a familiar refrain from its 1993 campaign "Operation Accountability" during which Foreign Minister Shimon Peres warned, "The Lebanese government has to decide whether Hezbollah represents it or not ….[If Hezbollah does not represent the government] the Lebanese government will then have to cooperate with us in silencing Hezbollah and ending its activities."[11] Similarly, a large part of Israel's strategy in its 1996 "Operation Grapes of Wrath" campaign was to isolate Hezbollah from the government and the people of Lebanon, thus usurping its support and freedom of action.[12]

The apparent underlying assumption in all three instances is that the Lebanese government and population will somehow rein in this rogue element that has dragged the nation into yet another costly conflict. Since Hezbollah was and remains well entrenched among the Shi'a population of Lebanon and is recognized by the government as a legitimate armed resistance group, all three attempts failed to meet the fundamental objective. At a simplified and very pragmatic level, the Lebanese government and armed forces have not dislodged or disarmed

Hezbollah because they lack the political will and the military means to do so to a group that is at once a political party with 11 parliamentary seats, an occupier of two ministerial posts in the Cabinet, an organized and effective welfare organization, and a heavily-armed, experienced militia with significant outside backing.

However, there is much more complexity to what Hezbollah represents. A look at its use of narratives, ceremonies, images, and institutions adds depth to what the above characterizations imply. What these cultural manifestations portray is a movement that is an integral part of the social landscape and whose "resistance" component embodies the dignity and empowerment of a large portion of the population and the state.

Mobilization of the Shi'a. At the ceremony eulogizing Abbas al Musawi, Hezbollah's secretary general whose motorcade had been devastated by Israeli attack helicopters (February 1992), Hassan Nasrallah (Musawi's successor and current secretary general) stated:

> [Yours is] a death that epitomized the events of Karbala. You were just like al-Hussein, a body without a head.…It is as if your infant son, Hussein is the suckling child of Karbala.…It is as if your spouse and life's companion Um Yasser, as if Zeinab is screaming in revolution…As if your bombed and destroyed cortege were Hussein's tents burning in the desert, as if you were that same Hussein, the commander on the battlefield, Hussein the rebel in the face of oppression and despotism, and Hussein who rejected humiliation and shame.…You, my master, epitomize all that Karbala represented, from resistance to enthusiasm, to the path, to the tragedy.[13]

Any student of Shi'a history will know the story of the battle of Karbala referenced in this passage.[14] Indeed, it is a basic narrative of Shi'a history that at once addresses the historical oppression of the Shi'a, and bravery, martyrdom, sacrifice, and steadfastness in the face of oppression.[15] In the above passage, what one sees is a localization and re-conceptualization of the Karbala narrative, with the slain Hezbollah leader cast as Hussein and his slain wife and son cast as the women and children that accompanied Hussein on his ill-fated journey.

The stage had been set for the recasting of the Karbala narrative nine years earlier, when an Israeli patrol in the Lebanese town of Nabatieh had found itself accidentally wandering through a procession in celebration of the battle. When the Shi'a participants threw stones at the patrolling Israeli troops in protest of their presence, the Israeli soldiers opened fire and killed several of the participants. The incident reinforced the basic Karbala theme of defiance and sacrifice in the face of oppression. However, as opposed to the conventional casting of the Shi'a versus a larger, powerful Muslim dynasty, this incident took on an alternate dimension as it became what Norton describes as "intrinsic to a commonly shared narrative emphasizing Israel's disrespect for Islam and the injustice of the long Israeli occupation."[16]

The reworking of the narrative, incorporating the Nabatieh incident and all that it entailed, built upon groundwork laid in the 1960s and 1970s by Imam Musa al-Sadr. Al-Sadr was an Iranian-born imam who grew wildly popular among the Lebanese Shi'a community during this timeframe and is widely recognized as the spiritual leader who led them from quietism and political withdrawal to empowerment and activism.[17] Part of his legacy rests in his remolding of the narrative of Karbala, first from an event that conjures sorrow, lamentation, and suffering to an event that commemorates defiance, bravery, and sacrifice, then to an event that moves beyond mere bravery in the face of sure death to a calculated, political decision by Hussein to engage the enemy.[18] Ajami's seminal study of al-Sadr succinctly captures the dynamism of the tradition as he describes al-Sadr's activities as taking "a tradition several centuries old" and "grafting onto it new themes of concern and activism."[19]

More striking and enlightening than the progressive remolding of the narrative of Karbala is the visual and aural aesthetic associated with Hezbollah's commemoration of the day of Ashura, the tenth day of the month of Muharram and the actual date of Hussein's death. If one has ever witnessed the ceremonial processions in the streets of Shi'a communities throughout the world, one may recollect images of blood-drenched men and adolescent boys lashing themselves, while women wail hysterically. However, the following description of Hezbollah's rituals during the Ashura celebration poses a striking contrast.

> The masira [procession] was highly organized. It began with four huge portraits of Khomeini, Khamenei, Nasrallah, and Musa al-Sadr. These were followed by many groups of boys, scouts, youth, and men, organized by increasing age. They were either dressed uniformly as scouts or entirely in black, "Husayn" written on their colored arm or headbands. Each group marched in three neat rows behind a microphone-bearing leader, who initiated nudbas [elegies] and chants, and ensured that everyone performed latam [self-flagellation] in perfect unison. This latam did not involve blood Instead, those performing it swung both arms downwards, then up, then out away from their bodies, and finally in to strike their chests with their hands. It was done to a four-count rhythm so that on every fourth beat the sound of hands striking chests resonated loudly, providing a percussive accompaniment….Then the women's part of the masira began, with colored panels of Ashura scenes. These were followed by female scouts and students, again in orderly rows organized by age, all dressed in full abayas. The girls chanted in response to a leader or sang nudbas but did not perform latam…."[20]

Hezbollah's ceremony presents a mesmerizing image of defiance and sacrifice, while at the same time portraying calculation and discipline. The notion of calculation squares with al-Sadr's take on the battle as a calculated decision by Hussein. The notions of order and restraint are salient for the Shi'a community as they appear to speak to an underlying fear that if this 'backward' community were to rise against oppression and become truly empowered, uncivil disorder would likely ensue. Anthropologist Emyrs Peters' 1970 study of a Shi'a village in Lebanon includes descriptions of ceremonial Ashura-affiliated plays that culminate with depictions of chaos and mayhem. Peters' analysis characterizes these plays as part of an order in which oppressive, elite Shi'a families inculcated the idea that while past oppression (among the Shi'a masses) was lamentable, it was not cause for haphazard overturning of the existing social and political order.[21] In this manner, the disorderly culmination of the Ashura ceremonies became what Norton described as "a conservative device for sustaining an existing order, not challenging it."[22] To the contrary, Hezbollah's ceremonies suggest the overthrowing of oppression without resultant mayhem and lack of civility, but with confidence, calculation, and order.

So, what one observes in Hezbollah's Ashura celebrations is the evolution of a basic tradition that at its essence laments Shi'a oppression at the hands of a powerful Muslim dynasty. Hezbollah's adaptations of the narrative and ceremony build on previous adaptations that transform a narrative of Shi'a sorrow and oppression into a narrative of defiance, empowerment, and mobilization. Their adaptations also recast the antagonist as Israel and the protagonist as the "resistance," which now not only represents Shi'a resistance, but places the Shi'a as the vanguard of larger Muslim (and Arab) resistance in the face of Israeli and Western aggression. The striking orderliness of the ceremony appears to counter the belief – previously upheld in the Ashura ceremony itself – that chaos will ensue once this dispossessed and "backward" community confronts and overturns what it views as an oppressive order.

Even though it is not a part of the visual spectacle of Hezbollah's Ashura ceremonies, blood is still an important element of the event. However, as opposed to the haphazard spilling of blood that one may observe in other Ashura ceremonies, Hezbollah promotes the donation of blood among its ceremonies' participants.[23] The notion of donating blood, as opposed to spilling it in what appear as savage rituals, fits the motif of empowerment, modernity, and orderliness as displayed through the Ashura ceremonies and adds another layer – that of community service as activism and empowerment.

In the aftermath of the July 2006 war, Hezbollah paid grants of up to $12,000 to thousands of families that had lost their homes. Likewise, it mobilized planners, medical personnel, and volunteers to design homes for the homeless, care for the infirm, and distribute food to the hungry. [24] In addition to their works in time of tragedy, Hezbollah's services include regular schools, schools for children with special needs, such as Down's syndrome, and summer camps – all enabled by tremendous volunteer support.[25] Hezbollah notes that its charitable organization Jihad al-Bina' (Reconstruction Jihad or Construction for the Sake of the Holy Struggle) had $450 million targeted specifically toward reconstruction of southern Lebanon in November of 2006.[26] More than a decade before the reconstruction efforts following the

2006 war, Hezbollah had made a name for itself by providing the most crucial of services, such as water delivery and waste removal, in the poor, neglected Shi'a sections of Beirut.[27]

While the numbers are impressive, what is important is what Hezbollah's charitable organizations represent to the Shi'a community. Hezbollah does not portray its service organizations as simple patron-client type services. Instead, it presents them as the realization of a shared community struggle (jihad) for self-reliance and prosperity. One may note, for example, the remarkable number of volunteers that Hezbollah's organizations enlist, along with the fact that its services are not simply oriented toward providing services for its constituents, but are also directed toward development. A 2001 Lebanese Ministry of Social Affairs report noted that Hezbollah was the number one non-governmental organization (NGO) within Lebanon for issuing loans to "small institutions" for "small projects."[28] These "small projects" mainly represent small, grass-roots efforts in fields such as agriculture and small-scale construction.[29]

On one level, Hezbollah's institutions represent a group's willingness and capacity to provide essential services to an otherwise deprived community. They represent services that the government, and at times, international organizations failed to provide or simply did not care to provide. However, at another level, they are a tangible manifestation of the narrative of Shi'a empowerment, with the specific connotation of self-reliance through community activism. Norton describes them as "an essential part of the construction of a modern, confident notion of identity," connoting "a spirit of activism and volunteerism" that contrasts with and contests "earlier, rampant acceptance of deprivation among the Shi'a." [30]

The Resistance as Part of the Social Landscape. In her 2006 study of what she deems the "pious modern" in Lebanon, Lara Deeb describes the way in which at times various imagery saturates the streets of the most well-known Shi'a Beiruti neighborhood, claiming it as a space which the Shi'a own and dominate, a marker of "the progress their [Shi'a] community had made within the nation-state."[31] Among these images are martyrs whose photographs Hezbollah's media departments place on lights and poles along the main thoroughfares. Deeb describes them as "head and shoulders of a martyr against a bright pastel background, with the yellow Hizbullah flag flanked by pink at the top and blue at the bottom."[32] She further notes that each contains a caption on the lower edge that reads "The martyred fighter so-and-so" or "The martyred brother so-and-so." [33] Visually, these displays seem to recreate the aesthetic of the "cult of personality" leader whose ubiquitous image greets one at every turn in various countries throughout the region and the world.[34]

Hezbollah's co-opting of space and imagery normally reserved for states and their official leaders may feed accusations that Hezbollah represents a state within a state. However, Hezbollah's narratives tell a different story. They relay the story of an organization that is neither a state within a state nor an alternative to the state, but one that in certain realms complements the state by filling voids, in other realms represents an organic and enduring part of the national landscape, and in other realms embodies the dignity of the state and the people of Lebanon; all of this is portrayed as "in harmony with the state."[35]

As Hezbollah's ceremonies and institutions fill a void of empowering and providing for a large segment of the population, its co-opting of images and space in the conventional domain of the state fills the void of the presence of the state that is absent in large portions of Shi'a Lebanon.[36] With regards to Hezbollah as part of the Lebanese landscape, Nasrallah's narratives of "liberating" Lebanon in May of 2000 and "defeating" Israel in July 2006 portray Hezbollah as an organic and enduring part of the landscape that cannot be extracted or moved. For example, in an August 2006 interview in which he addresses the proposal that the Israeli army withdraw behind the Blue Line (United Nations [UN] demarcation of the Lebanon-Israel border), while Hezbollah withdraws north of the Litani River, Nasrallah questions the logic of the proposal with the following statement:

> …I asked them to tell me how Hezbollah could withdraw from the area south of the river. The people of Ayta were resisting in Ayta, and the people of Bint Jbeil were resisting in Bint Jbeil. The same applies to the people of al-Khiam, al-Tayyibah, Mays, and all towns that fought…all the young men who fought on the front, and even in rear lines in the area south of the river,

> are the people of these areas.…Can I tell the people of Ayta: the Israelis could not force you out of your town, but I will do so because a political agreement has been reached? Can I ask the people of Ayta to live in Nabatieh? The people of Hezbollah are the people of the region. No logic says Hezbollah can get out of the area south of the Litani River." [37]

What Nasrallah presents here are facts on the ground that reinforce the narrative of people and towns that blend into a resistance, that in turn blends into the Lebanese landscape. There is therefore no way to uproot some separate entity known as Hezbollah, because to do so would mean uprooting the Lebanese landscape itself. His message is that the resistance is as enduring and organic as the towns and people of the south, because they are one in the same. For decades, Hezbollah has woven the idea that it is an outgrowth of the people and part of the national landscape into narratives about the very ordinary people that have arisen and thrown off the shackles of oppression. In its original manifesto, the group spoke of "the women with rocks and boiling oil for their weapons, the children with their shouts and their bare fists for their weapons, the old men with their weak bodies and their thick sticks for their weapons…" standing up and "making miracles and… changing…imaginary fates."[38]

The Resistance as Part of an Historic Shift of Power. In her study on post-cold war East Asia, Sheila Jager notes that "While China's history of national humiliation plays a central role in the narrative of shared collective suffering, China's rise as an economic powerhouse is also offered up as a narrative of shared collective redemption."[39] Hezbollah's statements in the aftermath of Israel's May 2000 withdrawal and the July 2006 "war" with Israel construct a narrative of collective Lebanese redemption with the "resistance" having shepherded the nation away from humiliation to redemption and dignity. As it builds and reinforces the narrative of from humiliation to redemption, Hezbollah reinforces the notion that the resistance is "in harmony with the state" and that the victories of the resistance are victories of the state and its people.

Nasrallah's "victory" statement in May of 2000 harps on the importance of Israel's withdrawal to "the dignity of our homeland, and the self-esteem of our nation…"[40] He reminds his "fellow Lebanese" that they "deserve liberation" that was made possible by "harmony between the resistance and the state…"[41] He implores the Lebanese to see the victory as "a victory for all the Lebanese, not only for Hezbollah or for any other movement…"[42] In Hezbollah's second manifesto (November 2009), Nasrallah reinforces the narrative of a resistance group whose struggles culminated in victories that changed history and reversed "imaginary fates." He characterizes the July 2006 war with Israel as "a divine, historical and strategic victory that changed the battle equation entirely, and…crushed the legend of the army that can never be defeated."[43]

Hezbollah also rounds out its narrative of the "resistance" as an organic, history-changing movement for national dignity with the assurance that this national victory does not come at the expense of chaos and disorder. Just as the order of its Ashura ceremonies appears to counter fears of chaos when Shi'a resistance and bravery manifest themselves, its tales of how Lebanon and the resistance conducted themselves in the wake of their victory in 2000 paint a picture of Lebanese order and restraint against Western and Israeli expectations of disorder and savagery. Nasrallah relays that the entire world was expecting "a period of total darkness and endless civil strife" in which "families…would exact vengeance on (one another)…" and in which "one religious group would set upon another." [44] He speaks of expectations that "… blood would be spilled, and massacres would take place." [45] However, Nasrallah reassures the people of Lebanon that fear of savagery and chaos is not an excuse for accepting persecution. He couches their restrained and orderly behavior as proving that "the people, state, resistance, and sects of Lebanon are deserving of the victory they are celebrating…."[46] Nasrallah plays on the idea of western hypocrisy and false fears of chaos with statements such as: "when the Nazi army collapsed in France, the civilized French resistance executed 10,000 French agents without trial. The resistance in Lebanon, and Lebanon itself, is more civilized than France and the whole world."[47]

Implications for U.S. Policy

The opening statement of United Nations Security Council Resolution (UNSCR) 1701 (11 August 2006) welcomes the Lebanese government's efforts to "extend its authority over its territory, through its own legitimate armed forces, such that there will be no weapons without the consent of the Government of Lebanon and no authority other than that of the Government of Lebanon."[48] The resolution, which specifically calls for the cessation of the 2006 Israeli-Hezbollah conflict, also reiterates prior calls for the Lebanese government to exercise authority over its territories. For instance, paragraph 8 calls for the "full implementation of the relevant provisions of the Taif Accords (1989), and of Resolutions 1559 (2004) and 1680 (2006) that require the disarmament of all armed groups in Lebanon…" such that "there will be no weapons or authority in Lebanon other than that of the Lebanese State."[49]

These excerpts help frame U.S. policy objectives for Lebanon and Hezbollah that rest on two broad pillars: coaxing Lebanon to take control of all of its territories; and building the capacity of the Lebanese Armed Forces (LAF) so that they extend state authority over all of its territories and while doing so disarm Hezbollah. However, formulators of U.S. policy and strategy should not expect the Lebanese government to completely uproot Hezbollah without replacing what it represents – varying levels of communal empowerment, national dignity, and civilized resistance. In other words, weakening Hezbollah's grip on Lebanon cannot be seen by the Lebanese as figuratively or literally leading to the Shi'a community or Lebanon's regression to various stages of wretchedness and oppression.[50]

This study's culture-focused analysis of Hezbollah demonstrates that through its service-rendering institutions, Hezbollah invokes a sense of empowerment among the Shi'a that dismantles layers of external and internal oppression. Militarily, the group represents not only an unauthorized militia, but some measure of Shi'a empowerment as well as history-changing Lebanese strength through "resistance." It appears that neither the government, nor the armed forces nor the Lebanese population is likely to quickly uproot and disarm Hezbollah. After an attack on LAF soldiers in September 2008, the Commander, General Jean Qahwaji, recounted the LAF's steadfastness in times of crisis and included as evidence that "the army succeeded, shoulder to shoulder with the people and the resistance, against Israeli attacks in the summer

2006 war…"[51] Likewise, in December 2009, the government reiterated in its Policy Statement that Hezbollah is a legitimate armed resistance movement. The above analysis suggests the following with regards to U.S. policy.

Economic Aid to Loosen Hezbollah's Grip.[52] U.S. economic aid to the Lebanese government should help the government to assist the Shi'a community within a framework of self-reliance and empowerment, as opposed to any number of alternative frameworks for aid (from detached to demeaning). While the amounts matter, what matters more is that aid – while meeting urgent needs first – go toward development projects and include opportunities for participation and community involvement along the lines of Hezbollah's institutions and projects. Government-sponsored economic aid and services must not appear as part of a project to simply replace one patron with another. For, when Hezbollah gives $12,000 to a family that has lost its home after the 2006 'war', it does so against a backdrop of providing what on the surface is aid and services, but beneath the surface is empowerment through community service in a framework of mobilization, volunteerism, and self-reliance. After decades of Hezbollah representing some level of dedicated, non-corrupt self-reliance and activism, there is little reason to believe that a true effort to loosen Hezbollah's grip on parts of Lebanon will come through a mere handout. It will come by way of offering alternate forms of self-reliance.

Disarming Hezbollah and Building the Capacity of the LAF. While for political reasons the United States cannot stop its public calls for Hezbollah to disarm, for Syria and Iran to cease their support for the group, and for Lebanon to adhere to UNSCR 1701 and its antecedents, the perception of overt outside pressure is unlikely to bear significant fruit.[53] Disarming Hezbollah will likely only occur as part of a slow, iterative process within a Lebanese framework in which the government, people, resistance groups, and armed forces negotiate and agree on progressively decreasing roles for the "resistance." U.S. involvement should therefore revolve around a patient behind-the-scenes effort to assist Lebanon in formulating its comprehensive national defense strategy, which will likely entail a gradual relinquishing of Hezbollah's arms and the absorption of some of its militias into the armed forces.[54]

However, a fundamental imperative for removing Hezbollah's legitimacy as an armed presence is that the Lebanese government find a way to redefine national esteem and dignity such that the concepts do not exclusively evoke resistance to Israeli and Western "aggression," but stem from its own capable, non-corrupt, non-sectarian state institutions. It is within this framework that U.S. efforts to build the capacity of the LAF form a key element of policy toward Lebanon and Hezbollah.[55] Numerous studies characterize the LAF as a respected national institution that enjoys support and admiration across Lebanon's numerous sects. For instance, a 2009 Center for Strategic and International Studies (CSIS) report notes that as of early 2009, "the LAF is the only truly cross-sectarian institution – military or otherwise – in Lebanon…[it is a] force that represents the broadest possible swath of Lebanese groups."[56] U.S. policy should aim to strengthen the LAF through equipment and training, so that it is a viable operational force that is able to handle state security and weaken Hezbollah's justification for remaining armed, but the more important objective in building LAF capacity – as it relates to Hezbollah – is educating and professionalizing a respected state institution that serves as one "model" for a capable, non-corrupt, non-sectarian manifestation of national dignity (as an alternatives to the "resistance" to Israel and the West). [57]

Conclusion

When Hasan Nasrallah delivered his opening remarks at the Arab International Forum for the Support of the Resistance, the image projected on the conference hall's massive screen was that of the Hezbollah leader flanked on the right by two flags. To his immediate right was the Lebanese flag, draped such that the national image of the cedar tree was most prominent. To the right of the Lebanese flag was Hezbollah's flag, folded such that Hezbollah's iconic images – a rising fist holding a rifle and the words "Verily, the Party of God (Hezbollah), they are the victors" – converged onto Lebanon's cedar tree. One may ask if this imagery represents Hezbollah "in harmony with the state," on par with the state as an equal actor, or as a rogue element that has taken the state hostage and co-opted its icons.[58] All of the potential responses contain some level of truth, as well as some level of hyperbole or simple falsity. This study suggests that at the level of national policy and strategy what is important is not that one arrive at a definitive truth, but that one understand the array of perspectives, who is negotiating them, and how.

Through its co-opting and manipulation of narratives, images, ceremonies, and institutions, Hezbollah portrays itself as "in harmony with the state" – an integral part of its social, political, and military landscape. Specifically, Hezbollah influences Lebanese perceptions through rooting itself in three broad narratives that have evolved over the past three decades since its inception: the awakening and empowerment of Lebanon's Shi'a community; the evolution of the Lebanese "resistance" to an intrinsic component of the modern national fiber; and the Lebanese "resistance" as the vanguard of an historical movement to reclaim national self-esteem and Pan-Arab dignity.

While not substituting for hard political and military realities, these narratives should inform a nuanced approach to U.S. objectives of having the Lebanese government take control of Hezbollah-controlled territory and disarm the group. While Lebanon may remain vulnerable to the designs of external actors for the foreseeable future, the fundamental change necessary to neutralize Hezbollah is deeply-rooted in perspectives within Lebanon. Analyzing Hezbollah's ceremonies, narratives, images, and institutions suggests that its entrenchment in Lebanese society rests on its having situated itself as the embodiment of Shi'a community empowerment and as an integral element in Lebanon's landscape that represents state dignity.

What this analysis means for U.S. policy (at least policy regarding social services and security cooperation) is that the focus should be on empowering state institutions that address the shortcomings upon which Hezbollah feeds, i.e. institutions that allow the Shi'a community to find true empowerment and self-reliance through non-corrupt, non-sectarian state apparatuses and organizations that steer dignity away from the "resistance" to a non-sectarian, professional state institution. This approach will assist in relegating Hezbollah to a bygone era when Shi'a deprivation, the frailty of the state, and external designs (such as those of Iran and Syria) facilitated the presence of organizations and institutions that pursued communal empowerment and state dignity through “resistance.” Or, it will assist in forcing Hezbollah to temper its actions and fold itself into the political and military framework of the Lebanese state.

The Role of Religion in National Security Policy since 9/11

Chaplain (Colonel) Jonathan Shaw
United States Army

When it comes to formulating national security policy today, religion may be regarded as the elephant in the room – we all know it's there, but nobody really wants to talk about it.[1] On the one hand, some U.S. policy makers and advisers have had concerns about granting religion a place at the table because its subject matter might not be appropriate. On the other hand, those who have been struggling to find a way to integrate religion into the post-9/11 discussion of national security have not yet found a fully satisfactory framework.

For some people, the perceived subjectivity of religion makes it an inappropriate element for national security policy. Some view religion as mere subjective preference, shaping personal choices about God and right and wrong. In contrast, they view national security policy as objective decision making, employing elements of national power against a real adversary. But consider Sun Tzu's strategic dictum: "Know the enemy and know yourself; in a hundred battles you will never be in danger."[2] Here the so-called subjectivity-objectivity polarity collapses in favor of a subject-object distinction: know your enemy and know yourself. But what is such knowledge other than the perception of deeply rooted identity, values, interests, and sources of power – which, more often than not, touch on or even flow from religious traditions?

Others dissent from including religion within national security policy out of concern for compromising what many call "the American separation of church and state." Because religion is spiritual, promoting an inner life springing from God – they argue – wouldn't it be improper for the United States to speak to religion within its national security policy? Carl von Clausewitz's anthropological framework for war suggests otherwise. In his paradoxical trinity, the people supply the emotions and passions of war.[3] Because human emotions and passions are frequently founded on religion, why wouldn't national security policy discuss the motivational power and effects of religion?

Still others judge religion to be too privatistic and idealistic to contribute anything meaningful in the national security world of deadly force and cut-and-thrust maneuvering. We must remember, however, that it is a distinctively liberal, western view that conceives of religion as a private affair divorced from daily life. Most societies see religion as related to individual identity, societal formation, and national values. Religion provides humanity with a framework for understanding the world, human meaning, and human conflict. Religion of necessity speaks to war and its conduct.[4]

In his masterpiece, *The Quest for Holiness*, Adolf Köberle sets forth the trajectories of the various world religions in their attempts to fulfill the human aspiration to overcome the pathos of this world. Köberle identifies this aspiration as humanity's desire for sanctification – for acceptance and holiness before God.[5] His introduction reads like a primer on human need which can drive to violence and perpetuate human conflict, and in that sense, like an introduction to the problem of national security.

> The desire for sanctification is always first aroused in man when he has become conscious, in some painful way, of his lack of peace and the erring restlessness of his life. So the experiences of age and suffering, of sickness and death that surround us… the realization of our moral weakness and uncleanliness, the continually repeated neglect of our duties toward our neighbor awakens a desire for supernatural strength and purity….These are the momentous hours when we have come to the point that secular values can no longer satisfy us; when the need of aspiring to God is recognized and we unite in the longing cry that is the hidden theme of all human history: "Dona nobis pacem." [6]

That religion and national security policy largely share a common base – the experience of human suffering, failed duties toward one's neighbor, the hunger for enduring values, and the desire for peace – suggests an integrative approach for religion within national security policy. But how should religion and national security policy be integrated? If there is a place at the table for religion, where should it sit?

If religion is to enter the discussion, it must not do so in the form of advocacy, promoting one religion over another.[7] Nor may it do so in the form of judgment, ruling on the orthodoxy or heterodoxy of a religion. Rather, religion must enter the discussion in the form of behavior.

Behavior matters – whether it is motivated by religious faith, nationalist commitment, or an empty stomach. And because behavior can support the interests of the United States or attack them, protect innocents or take their lives, our security requires that we understand behavior.

Religion is critically needed now in our national security discussions. We need to understand more clearly the way that religion can shape and motivate behavior. When it comes to our security, the behavior of our friends and our adversaries matters terribly.

Religion – not as a standard of belief, but as a power which drives human behavior – must be at the table if national security policy is to embrace the fullness of the human situation, formulate effective concepts, and yield enduring results. There is room for both a more nuanced consideration and a more comprehensive treatment of religion in U.S. national security policy. We need a workable framework that will provide such nuance and integration.

The struggle to locate that framework has taken the United States down a number of roads since the turn of the millennium, none of which has been totally satisfactory. President George W. Bush viewed freedom as a universal value, with religion as the preeminent freedom characterizing free, robust societies. With these assumptions, he viewed post-9/11 conflict with the Taliban and al-Qaeda as a battle over freedom. He believed that repressed Iraqis and Afghans would welcome the U.S. military as liberators bringing greater freedom, to include freedom of religion. President Bush's assumptions were only partially validated. Part of the problem was the dissonance between a western concept of freedom to choose and worship God over against an Islamic concept to submit to God. "Religion as Freedom" did not offer the optimal framework.

Neither has President Barack H. Obama's "Religion as Unity" framework solved the problem. President Obama has asserted a universal value regarding religion – that all religions are united by a moral law to care for one's fellowman. Based on this assumption, President Obama has labeled terrorists as false Muslims, and also launched initiatives to honor Islam and resolve mutual misunderstandings through dialog with Muslim states. His efforts have succeeded partially, but radical traditionalist Muslims continue to fight, believing they are the pure practitioners of the faith. Also, President Obama's framework has not accounted for the large numbers of Muslims in Muslim-majority countries who find terrorism ever justifiable.[8]

An additional framework is needed, one that understands religion as power which is comprehended in grand strategy, and religion as behavior which is addressed in policy.

This paper proposes to locate that framework by examining the role of religion in national security policy since 9/11, dividing the topic into four parts.[9] Part I helps define the potential scope of the interplay of religion and national security by projecting the question into the future. I examine the work of four recent historiographers, with special attention to their visions of the current and future world, and the role of religion with regard to human conflict.[10]

Because the United States is currently engaged in conflicts in Iraq and Afghanistan – both Islamic countries – part II provides an excursus on the power of Islam. As the religion of the Taliban and al Qaeda, but also of Egypt, Jordan, Saudi Arabia, and many other U.S. allies, Islam is *the* religion under discussion today in matters of national security. In this section I offer a brief investigation into the power of Islam by examining its history, different forms of *jihad*, various approaches to achieving Islamic unity, alignments within radical Islam and terrorist operations, and demographics that bear on Islamic identity and the extent of support for terrorism.

In part III, I examine the role of religion within the national security policies of President George W. Bush and President Barack H. Obama. Based on their approaches, I present and evaluate two paradigms for integrating religion within national security policy – "Religion as Freedom" and "Religion as Unity." I then offer a third paradigm – "Religion as Ideology" – in an attempt to relate a strategic vision which comprehends the power of Islam to a policy which accounts for religious behavior.

Part IV provides a summary and addresses certain practical questions that would need to be answered if the United States moves toward a comprehensive framework for religion, using the paradigm of Religion as Ideology. What changes might occur at the strategic and operational levels of war? What might be the way ahead?

Part I: Historiographical Projections on Human Conflict and Religion

To understand the interplay between religion and national security, one may either look backwards across history to assess past connections, or forward from today to project future connections.[11] I have chosen the latter way, as this allows an anchor point in the current but evolving geopolitical world, with its well-known national security challenges.

The four authors I survey – Alvin Toffler, Francis Fukuyama, Samuel Huntington, and Robert Kaplan – have proposed perhaps the most compelling alternative visions of the future world written in the past thirty years. Each advances his own paradigm, through which he offers a distinctive view of history and projects a future world.[12] To a greater or lesser extent each author discusses his understanding of the causes and projected occurrences of violent conflict, and the attendant role of religion. I include this survey not to critique their works, nor to claim that their works were written to prove a connection between religion and national security interests; I use their works to explore the relationship between religion and human conflict, within a set of possible futures, in order to project back a present-day azimuth for national security policy alternatives which consider the role of religion.

Alvin Toffler[13]

In his 1980 book, *The Third Wave*, Alvin Toffler pictures humanity's struggle as the quest to absorb change and to craft a related ideology that offers meaning for the new reality. For Toffler, humanity has experienced three “waves” of change – first agriculture, second industry, and third super technology – each of which has radically altered civilizational self-understanding, societal practices, and personal meaning. The rise of agriculture ten thousand years ago brought the First Wave. The industrial revolution signaled the Second Wave. Now, a Third Wave has arisen, marked by technological innovation, data systems, decentralized media, renewable energy, invisible economies, chaos theory, fragmented values, and accelerated change.[14]

Toffler locates the seeds of human conflict within his concept of wave confluence. Confluence occurs when a new wave crashes into the previous wave, producing a new situation, a new synthesis, a new civilization. Such new civilizations reflect more than paradigm shifts for ordinary societal labor – from agriculture to industry to technological science. More critically, every new civilization “develops its own ‘super-ideology’ to explain reality and justify its own experience.”[15]

According to Toffler, struggle is the inevitable result of two waves crashing together, each with its own super-ideology. For Toffler, this explains the violent conflict – within states and between states – that occurred at the confluence of the First and Second Waves.[16] Similarly, as the Second and Third Waves collide,

> The decisive struggle today is between those who try to prop up and preserve industrial society [Second Wave] and those who are ready to advance beyond it [Third Wave]. This is the super-struggle for tomorrow.
>
> Other, more traditional conflicts between classes, races, and ideologies will not vanish. They may even – as suggested earlier – grow more violent, especially if we undergo large-scale economic turbulence. But all these conflicts will be absorbed into, and play themselves out within, the super-struggle as it rages through every human activity.[17]

This decisive struggle is intensified because the Third Wave has brought tremendous ideological challenges, including religious challenges. In the Second Wave, the typical citizen retained long-term commitments aligned with the majority. In the Third Wave, civilization now “makes allowances for individual difference, and embraces (rather than suppresses) racial, regional, religious, and subcultural variety." The resultant stress is "tearing our families apart…shattering our values." Toffler notes that this shift in ground rules has led many to pursue fundamentalist religion to find "something – almost anything – to believe in," and to join religious cults in order to locate "community, structure, and meaning."[18]

In short, Toffler treats the subject of religion not as a body of beliefs, but as a manifestation of the confluence of Second and Third Wave ideologies; not as a source of absolute truth, but as a proof of the fragmented values of Third Wave civilization; not as a majority-based morality to guide society, but as a pattern of minority-based power within society.[19]

This reading of Toffler suggests that religion – especially as fleshed out in fragmented, smaller faith communities – will become increasingly vocal and powerful. Effective Third Wave governments will include religious groups as stakeholders, much as they would any minority power base within their ruling coalition.

The policy implication for Toffler seems to be that it is wiser to include religion as a dynamic, societal force, than to omit it and risk irrelevancy or failure. Indeed, his interpretation of the 1979 Iranian Revolution offers a good illustration of how Third Wave national security policy may ignore religion only to its great peril:

> Nurtured by the West, attempting to apply the Second Wave strategy,…[the pre-revolution] Teheran government conceived of development as a basically economic process. Religion, culture, family life, sexual roles – all these would take care of themselves if only the dollar signs were got right….Despite certain unique circumstances – like the combustive mixture of oil and Islam – much of what happened in Iran was common to other countries pursuing the Second Wave strategy.[20]

Francis Fukuyama[21]

In his 1992 book, *The End of History and the Last Man*, Francis Fukuyama embarks on a brave journey to locate "a Universal History of mankind" by determining its evolutionary engines, identifying tensions within the unfolding of the historical process, considering implications for his philosophical construal of anthropology and community, and projecting a provisional end state for humanity.[22] Based on an optimistic philosophy of history and borrowing heavily from Georg Wilhelm Friedrich Hegel,[23] Fukuyama traces the evolution of systems of human governance in the light of the human condition, and tracks a path leading to universal liberal democracy.[24] This would represent "the end of history," that is, its final, rational goal and manifestation.[25]

The historical process that would lead to universal liberal democracy, Fukuyama maintains, runs on the twin engines of economics and the human struggle for recognition. The former represents the simpler case for Fukuyama, given the power of technology and the "universal horizon of economic production possibilities."[26] The latter is more complex. Man's desire to be recognized as possessing dignity and worth – in particular, his desire to be recognized *as desirable*, that is, recognized as greater than his fellowman – has led to an historical chain of slave and master identities, and to war itself.[27] Within this construct, Fukuyama finds religion, and also nationalism and other forms of ideology, to be penultimate fulfillments of the human struggle for recognition.[28] Because religion can end up perpetuating slave and master identities,[29] it presents an obstacle to forming liberal democracies which alone give full expression to the non-negotiable principles of "liberty and equality."[30]

Fukuyama admits his historical method and anthropological assumptions generate analytical problems as humanity nears the final destination of history. If humanity and society separate themselves from their ideological foundations and commitments, how will this affect their ability to sustain themselves internally and engage the world externally? It is to this question we now turn, briefly considering difficulties in the areas of anthropology, sociology, and international relations. This line of inquiry will help sketch a preliminary picture of the role of religion and national security implications in Fukuyama's projected future.

On the anthropological side, Fukuyama believes that the most probable danger is that "the creature who reportedly emerges at the end of history, the *last man*"[31] will lose his passions, his ability to strive, and cease to be a true man. Having been indoctrinated that the birthright of every human is absolute freedom and absolute equality at absolutely no personal cost, the last man will have lost the capacity to make ultimate commitments and, therein, his capacity to be human.[32] Fukuyama also warns of the opposite, less likely, danger – humanity jettisoning the entire project of liberal democracy due to its loss of absolutes. Religion, nationalism, and ideologies would then drive a history which had not ended, and whose demise had been prematurely projected.[33]

On the sociological side, within the United States, those private associations which previously enabled debate and built strength within liberal democracies would be so emptied of religion and other ideological causes that the public good, as the politically-negotiated coherence of privately-held rights, might well collapse.[34] Where tolerance requires being open to all belief systems, it unavoidably attacks the normative character of any one system. Fukuyama's surprising solution is to re-empower personal ideology, to include religion, in order to make liberalism sustainable. He argues:

> No fundamental strengthening of community life will be possible unless individuals give back certain of their rights to communities, and accept the return of certain historical forms of intolerance.
>
> …Men and women who made up American society...were for the most part members of religious communities held together by a common moral code and belief in God…. Liberal principles had a corrosive effect on the values predating liberalism necessary to sustain strong communities, and thereby on a liberal society's ability to be self-sustaining.[35]

Regarding international relations, because societies and states are located at different distances from the end of history[36] – with some still retaining robust religious, nationalist, and cultural ideologies – the United States would still need to practice foreign relations so as to engage the power of religion in those lesser developed societies where it remains the decisive, or at least a not-yet-marginalized, power.[37] Here Fukuyama singles out the Islamic world.

> At the end of history, there are no serious ideological competitors left to liberal democracy….Outside the Islamic world, there appears to be a general consensus that accepts liberal democracy's claims to be the most rational form of government.[38]

For Fukuyama, Islam would seem to merit special attention in national security policy. He represents Islam as an ideology that attracts those who are already "culturally Islamic," that possesses "its own code of morality and doctrine of political and social justice," and that has "defeated liberal democracy in many parts of the Islamic world, posing a grave threat to liberal practices even in countries where it has not achieved political power directly."[39]

To sum up, these difficulties seem to suggest a conclusion that runs counter to the overall direction of Fukuyama's thesis. My reading of Fukuyama is that his projected post-historical United States would of necessity retain religion as a power within society and as a lens for addressing national security issues for that society. Thus, religion would remain a critical component of effective foreign policy in Fukuyama's future world, to meet the challenges of external threats, internal associations, and enduring anthropological distinctions.

Samuel P. Huntington[40]

In his 1996 book, *The Clash of Civilizations and the Remaking of World Order*, Samuel Huntington presents the case that the best paradigm for understanding and addressing current international conflict is "the clash of civilizations." Prior to the fall of the Soviet Union, the alignment of world states was based chiefly on ideology, with states falling into "three blocs."[41] With the collapse of communism, however, Huntington finds that "culture and cultural identities, which at the broadest level are *civilization identities*, are shaping the patterns of cohesion, disintegration, and conflict."[42] Today,

> …the most important distinctions among people are not ideological, political, or economic. They are cultural….People define themselves in terms of ancestry, religion, language, history, values, customs, and institutions. They identify with

> cultural groups: tribes, ethnic groups, religious communities, nations, and, at the broadest level, civilizations.[43]

Identifying seven or eight such civilizations,[44] Huntington concludes that "in the emerging era, clashes of civilizations are the greatest threat to world peace, and an international order based on civilizations is the surest safeguard against world war."[45] Huntington calls such clashes "fault line wars."[46]

Religion plays two key roles within Huntington's paradigm. First, religion largely defines a civilization, and is usually its most important objective element. Huntington quotes English historian Christopher Dawson: "The great religions are the foundations on which the great civilizations rest."[47] Second, because religion is so significant for defining civilizations, religion frequently serves as a critical driver in fault line wars.

Consider the religious components in Huntington's most likely and most dangerous fault line wars. At the "micro level" (localized wars), Huntington sees violent fault lines "between Islam and its Orthodox, Hindu, African, and Western Christian neighbors."[48] At the "macro level" (global wars), Huntington assesses the worst conflicts as occurring "between Muslim and Asian societies on the one hand, and the West on the other." Overall, he projects that "dangerous clashes" (wars of greatest violence between states or entities from different civilizations) will result from the clash of "Western arrogance, Islamic intolerance, and Sinic assertiveness." Religion provides fuel for Huntington's future wars.[49]

Because Huntington explicitly names Islam as a civilization likely to clash in micro, macro, and dangerous wars, a further word is in order. Huntington reviews significant historical, political, cultural, and religious data as he makes his case for the likelihood of continued Islamic civilizational violence. His evidence may be grouped in three, overlapping areas: the Islamic Resurgence,[50] Islamic consciousness without cohesion, and the intercivilizational Islamic-western clash.

First, Huntington documents an Islamic Resurgence wherein multitudes of Muslims have turned to Islam for:

> a source of identity, meaning, stability, legitimacy, development, power, and...hope epitomized in the slogan "Islam is the solution"....It embodies acceptance of modernity, rejection of Western culture, and recommitment to Islam as the guide to life in the modern world.[51]

This Islamic Resurgence he characterizes as a mainstream and pervasive civilizational adjustment vis-à-vis the West, aimed at returning Muslims to "a purer and more demanding form of their religion."[52] Powerful demographic trends such as large Islamic migrations to cities, exploding youth populations, and economic problems have played no small part in this Resurgence. Huntington believes that although this Resurgence will produce many social gains, it will leave unresolved "problems of social injustice, political repression, economic backwardness, and military weakness," thus fueling future conflict.[53]

Second, Huntington considers the implications of a strong transnational Islamic consciousness that exists without cohesive power.[54] Huntington finds that traditional Islamic commitments to "the family, the clan, and the tribe," as well as to "unities of culture, religion, and empire," are producing a strong and widespread Islamic consciousness.[55] What is lacking today, however, is a core or lead state, or transnational power structure, to effect Islamic cohesion. The result has been instability through competition among aspiring Islamic states, sects, and transnational actors, each seeking to gain popular Muslim support to expand its own base and reach of power. For Huntington, this instability and competition increases the potential for conflict within Islamic civilization, and between Islam and other civilizations.

Finally, Huntington addresses what he views as the basic clash of Islamic and western civilizations.[56] Huntington tracks a stormy relationship between these civilizations across 1,400 years of history, with conflict flowing from "the nature of the two religions and the civilizations based on them."[57] He documents that "the argument is made that Islam has from the start been a religion of the sword," that it has expanded by use of force when strong enough to do so, and that it has refused to grant equal protection under the law to adherents of other religions.[58] Beyond such historical and theological concerns, Huntington lists current trends which have contributed to the clash: increases in Islamic population, unemployment, and the number of disaffected youth; greater Islamic confidence over against the West through the Islamic Resurgence; the West's abrasive policies of universalizing its culture and meddling in conflicts in Islamic lands; the fall of communism, against which the West and Islam had made common cause; and increased intercivilizational contacts between Islam and the West, which have magnified intolerances between the two.[59]

Huntington's view of the future is clear: religion as the preeminent cultural factor defining civilization will play a central role in any effective national security policy.[60]

Whatever the normative prejudices of the reader, whether one admits to the possibility of meaningful differences between religions and moral frameworks, or not, the data Huntington cites in order to demonstrate points of friction between civilizations based on religion, must be taken at a minimum as points of data regarding differences in human behavior, flowing from cultural differences between certain state, sub-state, and transnational identities. That such differences in behavior, irrespective of differences in belief, may lead to violence and war implies the criticality of addressing religion as behavior within national security policy.[61]

Robert Kaplan[62]

In his 2000 book, *The Coming Anarchy: Shattering the Dreams of the Post Cold War*, Robert Kaplan advances his vision of the post-Cold War world, with special attention to national security implications for the United States. According to Kaplan, the Cold War brought significant order and stability to a world that was suspended between the polarities of U.S. and Soviet power, tamping down fractious cultural, societal, and religious forces. Such forces, however, gained traction with the fall of the Soviet Union, destabilizing many countries and regions, giving rise to "the coming anarchy." Within this context, Kaplan sees "the environment" as "*the* national-security issue of the early twenty-first century.[63]

In Kaplan's coming anarchy, the population will largely be divided into the "haves" and the "have nots," based on the nature of the devolving world. Kaplan writes that "we are entering a bifurcated world" populated by "Fukuyama's Last Man" and "Hobbes's First Man."[64] The former presents the few – post-modern humanity which is well educated, well fed, dominant in technology, and successfully separated from the brutish world. The latter presents the many – entrapped humanity which is surrounded by anarchy, living in poverty, engulfed in cultural strife, and doomed to failure by environmental privation.[65]

The polarities of Kaplan's future world imply that religion relates to concepts of security and stability in two different ways. First, Hobbes's First Man lives his brutish life in the throes of contradictory cultures, extremist ideologies, and religious constructs. For such a First Man, Kaplan's view is that although religion can sometimes be a positive force – contributing to individual empowerment, cultural identity, and societal order – more often religion is a negative force – undermining stability and fueling conflict.

It is in this context that Kaplan discusses Islamic violence.[66] My reading of Kaplan suggests that although he sometimes interprets violence between Islamic peoples as springing from religious grounds, more frequently he perceives such Islamic violence as rising out of a cultural clash, with religion being subordinated to a specific Muslim culture. So it is that Turks may distrust and clash with Iranians, for example. That said, the cultural differences between Islam and the West are yet greater than the cultural differences within the House of Islam, so that in clashes between Islam and the West, a broader Muslim identity takes precedence.

This is not to suggest that Kaplan agrees with Huntington's thesis of a monolithic Islam clashing with western civilization.[67] Rather, Kaplan's view is that Huntington has oversimplified the matter and misidentified the clash. The clash is not between Islam and the West, but properly within Islam, or more precisely, *within* the patchwork of competing *ethnic groups and cultures* which self-identify as Islamic; and then, only in a derived sense, between Islamic groups and cultures and the West.

But the role of religion in the life of the First Man is yet more complex. This is because Kaplan subordinates all such ethnic and cultural Islamic violence to his thesis of the coming anarchy. Kaplan describes "Islamic extremism [as] a psychological mechanism of many urbanized peasants threatened with the loss of traditions in pseudo modern cities where their values are under attack."[68] He sketches Islam as a religion bringing happiness to "millions of human beings in an increasingly impoverished environment,"[69] but whose "very militancy makes it attractive to the downtrodden. It is the one religion that is prepared to *fight*."[70] Thus for Kaplan foundational militancy within Islam is subordinated to the broader cultural identity, which in turn is subordinated to the environmental struggle of the First Man. From his perspective, the secular government of modern Turkey presents an outstanding success story of an Islamic culture driving toward moderation and modernity, effecting vital order and infrastructure within an Islamic society, "making it much harder for religious extremists to gain a foothold."[71]

Thus, in Kaplan's world of the First Man, religion will play a pivotal role in personal identity, cultural clashes, and the broader environmental struggle. Religion, especially as an enabler of culture, will empower the broader struggle seeking to gain control of critical resources, in hopes of securing a modicum of security and stability.

Second, consider Kaplan's appropriation of Fukuyama's Last Man. Although this suburbanized, well-fed, and self-satisfied man may have no *personal* need of religion, he will still have a *policy* need of religion. If only to achieve the ends of improved international stability and his own security, he will still need to influence the other strife-filled world where religion is valued. Kaplan makes the related policy point that the United States may have to learn to connect with cultures with which it holds little in common. It may sometimes be in the best interests of the United States to support authoritarian regimes in acute need of social stability and economic development, though not yet ready for democratic elections and still perpetuating systems of injustice.[72] Borrowing from James Madison in *The Federalist*, Kaplan suggests that American global engagement will likely best promote stability in fragile societies and governments by focusing on their "regional, religious, and communal self-concern."[73] Thus the Last Man's foreign policy will still need to address the priorities of the First Man, to include his religion.

Toffler, Fukuyama, Huntington, and Kaplan all articulate different visions of the current and future world, with varying views of national security challenges. Each author, however, includes religion as a critical component in policy that would address those challenges effectively, and highlights Islam within that process. Specifically how religion might be treated within national security policy – as a mark of freedom, a symbol of unity, or an expression of ideology – I address in part III.

Part II: The Power of Islam

First, however, it is important to give some direct attention to the religion of Islam. This would seem to be necessary for at least three reasons. One, Islamic terrorists attacked the United States on 9/11. Two, the Taliban and al Qaeda continue to use the religion of Islam as a rallying cry against the United States and the West. Three, Pakistan, Egypt, Jordan, Saudi Arabia, and many other U.S. allies are Islamic countries.

These data points raise a particularly challenging question. How are Americans to comprehend the influence and the nature of a faith that is held by some of our most aggressive adversaries, but also by some of our closest friends? This is the confusion that many Americans feel about Islam, and it is a confusion that cannot be clarified until we are willing to look more closely at the faith and its divisions.

That religions have divisions within them is not unusual. Judaism may be divided into Orthodox, Conservative, and Reformed. Christianity may be divided into Orthodox, Roman Catholic, Lutheran, Episcopal, Baptist, Methodist, Presbyterian, and many other denominations. What is unusual about Islam is that the divisions are extraordinarily complex and represent fundamentally different visions of how the faith is to achieve its universalization.

Yet we must understand Islam with its various divisions if we are to understand Islam as a power which motivates behavior. We must understand the faith dimension to derive the policy implication.[74]

Authoritative Documents[75]

There are many approaches to studying Islam, but one helpful way is to begin with a review of its authoritative documents and then move to its history.

Unlike Christianity, Islam emphasizes practice over belief, law over proclamation.[76] Accordingly, Islam considers its authoritative source documents as supremely important. The primary authority in Islam is the *Qur'an*, revealed from 610 to 632 of the Common Era (CE) and considered to be "the eternal, uncreated, literal word of God, revealed one final time to the Prophet Muhammad as a guide for humankind."[77] The *Qur'an* reveals information about Allah as the radically transcendent, divinely omnipotent and omniscient God, who alone is God, who in himself is Unity; however, the *Qur'an* does not reveal God, for God is beyond all grasp and comprehension. Rather, the *Qur'an* reveals God's universal will or law for all humanity.[78]

Stylistically the *surahs*, or chapters, of the *Qur'an* are composed of dramatic and shifting forms, and not chronological narrative.[79] *Surahs* may be divided based on where the revelation was received – in Mecca or in Medina.[80]

The secondary authority in Islam is the *Sunnah*, composed of the words, deeds, and judgments of Mohammad, to include community practice flowing from the Prophet's example.[81] This form of customary law was written down by Muhammad's Companions, with the written documents themselves called *hadith*.[82] The *sirah*, or biographical accounts of Muhammad's life, also lie within the category of *Sunnah*.[83]

Together the *Qur'an* and *Sunnah* form the basis of divine law, called *Shari' ah*.[84] Meaning "straight path," *Shari' ah* is that law in Islam that effects the rule of God and governs life – individual, community, and state. *Shari' ah* fuses the religious and civil worlds into one. *Shari' ah* is particularly instructive for the *ummah*, the one community of Islamic believers worldwide. *Shari'ah* tells the *ummah* what it means to be a Muslim.

A document of lesser, but still significant, authority in Islam is the *fatwa*, a formal restatement, or new application, of Islamic law. *Fatwas* are the result of difficulties both in understanding certain texts of the *Qur'an* and the *Sunnah*, and in applying those texts to new situations. Islamic legal scholars issue *fatwas* to address aspects of life ranging from prayer and discipline, to marriage and family, to war and politics. The perceived authority of a *fatwa* can depend on the faith community's respect for the scholar and his reasoning in matters of casuistry.

To enable resolution of interpretive difficulties, the Islamic legal tradition mushroomed. Principles of Islamic jurisprudence, or *usul al-fiqh*, established rules of interpretation, reasoning, precedence, and custom, to guide legal decisions.[85] *Siyar*, the Islamic law of nations, also developed, detailing the Islamic law of war. Five legal traditions crystallized. Based on texts from the *Qur'an* and *Sunnah* and the extensive legal system, *fatwas* became a standardized way for leading legal scholars to shape and apply Islamic law.[86]

Brief Overview of Islam

The *Qur'an* documents a series of revelations to the Prophet Muhammad, beginning in 610 CE.[87] After remaining silent for about three years, Muhammad went public and declared his revelations to the residents of Mecca. Decrying their polytheism and vices, he called for them to repent and submit fully to Allah, the one, supreme Being. Following years of difficult preaching and persecution, Muhammad and a small band of followers migrated to Medina in 622. There Muhammad consolidated his religious and political power into one office, which he occupied as the singular spokesman and Prophet of God.

At Medina, Muhammad showed himself to be a wise and talented leader of the Medina community and his nascent *ummah*. The continuing revelations he received in Medina proved especially important for his religious and military future. Certain Medinan revelations to Muhammad established Islamic rites and practices as part of a universal religion. Other revelations authorized offensive military operations in order to achieve that vision. From Medina, Muhammad undertook a number of raids and battles, against neighboring tribes, caravans, Jews, and a force of thousands from Mecca. The trend line multiplied Muhammad's power and wealth, and increased the number of those who submitted to Allah. The peaceful surrender of Mecca in 630 CE gave Muhammad undisputed control of the Arabian Peninsula and religious hegemony based on his earlier order to expel all Christians and Jews. Before enacting a more expansive campaign to spread Islam through conquest, Muhammad fell ill and died in 632.

Following the death of Muhammad, the faithful demonstrated their resolve to realize their Prophet's universal vision of Islam. Islam experienced extensive growth by military conquest in the seventh and eight centuries. Even through the twelfth century, Islam continued to expand its rule, but it achieved this growth in an ebb-and-flow manner as European Christian powers began to achieve dominance. Still, at the height of its power Islam could claim Spain, parts of France and Italy, all of northern Africa, and large portions of Eurasia. That said, internal Islamic struggles for leadership, an ethos constrained by regimented commitment to the past, and the external European dynamism of the Renaissance projected a final wall which Islam would not breech. Islam's defeat at the gates of Vienna on September 11-12, 1683 marked the end of Islam's linear, contiguous warfare to achieve universality. The vestiges of the great Ottoman Empire, launched in 1291, finally faded away through defeat in World War I. A new era for Islam had begun.

Before more thoroughly examining the claim that Islam initially expanded by military conquest in order to achieve its vision of universality, we must first note alternative views. Liberal scholarship and postmodern perspectives in the last century have articulated a trans-historical understanding of Islam's universality in exclusively internal, spiritual terms.[88] Other commentators have suggested that prudence precludes discussing a possible historical occurrence of Islamic militancy, to avoid aiding adversary recruitment or undercutting coalition building. Ibn Warraq sounds a cautionary note on bypassing history to satisfy ideology, especially ones own. Warraq quotes Isaiah Berlin, arguing that from the latent desire to "suppress what [one] suspects to be true....has flowed much of the evil of this and other centuries."[89] From this perspective, the hard investigation of history provides the surest way to the flourishing of humanity.

Jihad

The multiple interpretations of *jihad* that exist within Islam today contend both for legitimacy and for adherents. The struggle over the definition of *jihad* is nothing less than the struggle over the defining character of Islam. Is the peace which Islam represents realized through external struggle, internal struggle, or a combination of the two? The original concept of *jihad* prioritized the meaning of *jihad* as external struggle or warfare, but included shadings of an internal or spiritual struggle. Changes in Islam's external operational environment led to an evolving concept of *jihad*.

In this section I document the initial concept of *jihad* in Islam, its interpretation through the authoritative principles of Islamic jurisprudence, and its application within the Islamic war of nations. In the following section of this paper, I trace modern interpretations of *jihad* that have arisen from reformed Islamic positions.

My reading of Islam's history, *usul al-fiqh* (principles of Islamic jurisprudence), *siyar* (the Islamic law of nations), and teaching on *jihad* (struggle or war) suggests that classical Islamic jurisprudence clearly accepted the proposition that Islam expanded by military conquest in order to achieve its goal of universality, as envisioned by the Prophet.[90] To this one may add that the early emphasis on militaristic or external *jihad* was joined by a rising accent on spiritual or internal *jihad*, as the initial and stunning military advances of Islam slowed.

Shaybani, born 750 CE, wrote Islam's most famous *siyar*, detailing the authoritative understanding of the Islamic law of nations and classical Muslim notions of *jus ad bellum* and *jus in bello*. Shaybani's *siyar* demonstrates the historical and theological connection of *jihad* to the goal of achieving a universal Islamic state. Majid Khadduri, arguably the foremost authority on Shaybani, comments:

> The Islamic faith, born among a single people and spreading to others, used the state as an instrument for achieving a doctrinal or an ultimate religious objective, the proselytization of mankind. The Islamic state became necessarily an imperial and an expansionist state striving to win other peoples by conversion.[91]

Because the vision of a worldwide Islamic empire could not be achieved immediately, Islam needed to generate new law to govern the continued prosecution of war, the distribution of the spoils of war, and the relations of Islam with those states who had not yet been conquered. These necessities gave birth to *siyar* and defined its scope.

Based on this scope, *siyar* assumed a state of hostility between the Islamic and non-Islamic world. The world was divided into two – *dar al-Islam* (the territory of Islam) and *dar al-harb* (the territory of war).[92] *Dar al-Islam* was that part of the world ruled by *Shari'ah*, and *dar al-harb* was the military objective.

> The territory of war was the object, not the subject, of the Islamic legal system, and it was the duty of Muslim rulers to bring it under Islamic sovereignty whenever the strength was theirs to do so.[93]

This does not mean that *siyar* required continuous warfare against the *dar al-harb*. Although "the ultimate objective of Islam was the whole world," expediency or temporary Islamic weakness might justify the halting of hostilities and a temporary peace.[94] When opportunity arose, however, the Muslim ruler was expected to return to offensive operations and, by conquest, achieve a universalization of Islam.

These offensive operations were by definition *jihad*. Khadurri notes:

> The instrument which would transform the *dar al-harb* into the *dar al-Islam* was the *jihad*. The *jihad* was not merely a duty to be fulfilled by each individual; it was also above all a political obligation imposed collectively upon the subjects of the state so as to achieve Islam's ultimate aim – the universalization of the faith and establishment of God's sovereignty over the world.[95]

Hamidullah clarifies an important point. *Jihad* was not to be considered an individual duty in an absolute sense, but only in a derived sense, for *jihad* belonged to the state:

> *Jihad* is not considered as a personal duty to be observed by each and every individual, but only a general duty which, if accomplished by a sufficient number, the rest will no more be condemned for the neglect of that duty – this fact renders the administration of *jihad* entirely in the hands of the government. The practice of the Prophet also shows the same thing.[96]

Such an understanding of *jihad* as state-sponsored, chiefly offensive military operations raises eyebrows today. Liberal and postmodern reformed accounts of Islam largely bypass documentary and historical evidence from the initial centuries of Islam in favor of emphasizing Islam as a religion that has expanded through the attraction of its inherently peaceful, spiritual discipline.

There is some evidence for each side, but most *Qur'anic* verses on *jihad* refer to actual fighting. Consider the following:

> Indeed, Allah has purchased from the believers their lives and their properties [in exchange] for that they will have Paradise. They fight in the cause of Allah, so they kill and are killed. [It is] a true promise [binding] upon Him.…Rejoice in your transaction.[97]
>
> When the sacred months have passed, then kill the polytheists wherever you find them and capture them and besiege them and sit in wait for them at every place of ambush. But if they should repent, establish prayer, and give *zakah* [alms], let them [go] on their way. Indeed, Allah is Forgiving and Merciful.[98]
>
> Fight those who do not believe in Allah or in the Last Day and who do not consider unlawful what Allah and His Messenger have made unlawful and who [Jews and Christians] do not adopt the religion of truth…- [fight] until they give the *jizyah* [annual tax] willingly while they are humbled.[99]
>
> Not equal are those believers remaining [at home]…[compared to] the *mujahideen*, [who strive and fight] in the cause of Allah with their wealth and their lives. Allah has preferred the *mujahideen* through their wealth and their lives over those who remain [behind].…Allah has preferred the *mujahideen* over those who remain [behind] with a great reward.[100]
>
> And fight them until there is no *fitnah* [sedition or idolatry] and [until] the religion, all of it, is for Allah. And if they cease - then indeed, Allah is Seeing of what they do.[101]

To the above verses we must add the authoritative example of the Prophet, in support of understanding *jihad* as war. From the time he arrived at Medina until his death, Muhammad was a warrior. When words and other actions could not convince or coerce non-Muslims to submit to him as the Prophet of Allah, he regularly used warfare to advance Islam. Sometimes such warfare was brutal. Muhammad's role in ratifying the 627 CE beheading of between six and eight hundred captured Jewish men is well documented in the *hadith*.[102] His farewell address in March of 632 reflected a similar understanding of *jihad*: "I was ordered to fight all men until they say 'There is no god but Allah.'"[103]

On the other side, there are *Qur'anic* verses, although significantly fewer, which emphasize *jihad* as a spiritual, inner struggle or striving. Examples include the following:

> And strive for Allah with the striving due to Him. He has chosen you and has not placed upon you in the religion any difficulty. [It is] the religion of your father, Abraham. Allah named you "Muslims" before [in former scriptures] and in this [revelation] that the Messenger may be a witness over you and you may be witnesses over the people. So establish prayer and give *zakah* [alms] and hold fast to Allah. He is your protector; and excellent is the protector, and excellent is the helper.[104]
>
> Those who remained behind rejoiced in their staying [at home] after [the departure of] the Messenger of Allah and disliked to strive with their wealth and their lives in the cause of Allah and said, 'Do not go forth in the heat." Say, "The fire of Hell is more intensive in heat."[105]
>
> There shall be no compulsion in [acceptance of] the religion. The right course has become clear from the wrong. So whoever disbelieves in *Taghut* and believes in Allah has grasped the most trustworthy handhold with no break in it. And Allah is Hearing and Knowing.[106]

To these verses we must add the later distinction of the "greater *jihad*" and the "lesser *jihad*." In the ninth century, ascetic impulses within Islam began to merge into a mystical interpretation – Sufism – generating some documentation of a new distinction between a greater and lesser *jihad*. Although such documentation is absent from the authoritative *hadith*, ninth century wisdom literature provides examples:

> A number of fighters came to the Messenger of Allah, and he said: "You have done well in coming from the 'lesser *jihad*' to the 'greater *jihad*.'" They said: "What is the 'greater *jihad*'?" He said: "For the servant [of God] to fight his passions."[107]

We must note that there need not be a contradiction, strictly speaking, between the belligerent and irenic passages of the *Qur'an*; *jihad* may entail both.[108] That said, there is undeniable dissonance between the *Qur'anic* passages which portray *jihad* as state-sponsored, offensive warfare used to expand Islam and achieve universality, on the one hand, and *jihad* as inner, spiritual striving used to build Islam through peaceful, spiritual discipline. The Islamic legal tradition of *usul al-fiqh* helps in part to resolve this dissonance.

Within *usul al-fiqh*, the principle of *naskh* (abrogation) allows certain later passages of the *Qur'an* and elements of *Shari'ah* to take precedence over earlier passages or elements.[109] This resolution rules out contradiction. Instead, based on the relative time of the revelations, the latter takes precedence over the former. In this way *naskh* has been used by some commentators to argue that the later, Medinan exhortations to wage war against infidels take precedence over and abrogate the earlier Meccan requirements to pursue only peaceful means.[110] Terrorist Muslims continue to use *naskh* in this way as the basis in S*hari'ah* for their terrorist *fatwas*.[111] Other modern commentators reject *naskh* to embrace earlier Islamic admonitions of peace.

The Central Question for Islam: How Islam Is to Achieve its Universalization

This brief study of Islam, pivoting on historical periods of peace and war, and on alternative understandings of *jihad*, suggests that the problem of Islam is the problem of unity.[112] Islamic unity begins and ends within Allah, who is uniquely and radically one in himself, transcendent beyond humanity and the world. Through the *Qur'an* and the testimony of the Prophet, God has given his divine law – *Shari'ah* – as the means for establishing his rule among humanity. Only in full submission to Allah, through obedience to his *Shari'ah*, can there be peace.[113] Although the *ummah* and their *dar al-Islam* know this peace, *dar al-harb* does not. This presents a problem, for it is the will of the transcendent God who himself is Unity that all submit to him. Within the classical construction, only when *dar al-Islam* overcomes *dar al-harb* and places it under *Shari'ah* will God's command be met and permanent peace realized.

In the initial stages of Islam, militant *jihad* was a critical component of life under *Shari'ah*. *Dar al-Islam* conquered large portions of *dar al-harb*, bringing *Shari'ah* to an ever-widening kingdom. But as the expansionist victories of Islam subsided, the realization of the Islamic vision of universality became problematic. A new approach to Islamic unity – other than military conquest to establish worldwide *Shari'ah* – seemed necessary. An evolving reality brought modifications to the previous *jihad* construct and to relations between Islamic and other states.

Below I identify six partially overlapping positions, or schools of thought, within Islam today, each of which attempts to address the problem of Islamic unity. These positions are found among both U.S. adversaries and partners in current overseas contingency operations. Understanding these positions is a vital starting point for resolving related conflict and national security issues.

My study of Islam suggests that Islam's historic vision of its own universalization assumed that *Shari'ah* would one day rule all lands, that *usul al-fiqh* would remain authoritative for regulating the analysis of the legal sources and deducing the content of Islamic law, and that *jihad* as warfare would remain a legitimate mechanism to universalize Islam.[114] Relative to this enduring sixfold distinction, I identify six positions within Islam today.[115] Those groups which retain this vision, albeit with some conditions and concessions to reality, I call traditionalists. I find three categories of traditionalists – radical, conservative, and neotraditionalist Muslims. Those groups which have left the traditionalist understanding, yet articulate another principle of Islamic unity that they apply to public and political life, I label reformists. I denominate two categories of reformists – postmodern and liberal. Finally, those groups which have retained allegiance to Islam as authoritative for personal faith and practice, yet reject any role of Islam in the political sphere, I refer to as secular-state Muslims. See Table 1 (next page) for a summary of the related nomenclature.[116]

Full Name of Islamic Position	Shortened Name of Position	Name of Adherents
Radical Traditionalist Islam	Radical Islam	Radical Muslims
Conservative Traditionalist Islam	Conservative Islam	Conservative Muslims
Neotraditionalist Islam	N/A	Neotraditionalist Muslims
Postmodern Reformed Islam	Postmodern Islam	Postmodern Muslims
Liberal Reformed Islam	Liberal Islam	Liberal Muslims
Secular-State Islam	N/A	Secular-State Muslims

Table 1. Islamic Positions

Radical traditionalist Islam generally sees no need to change from Islam's historic assumptions regarding the universalization of the faith. Radical Islamic groups desire a return to Islam as it was practiced in its first centuries, seeking the expansion of Islam through *Shari'ah*, applying *usul al-fiqh*, and leaving open the possibility of militant *jihad*.

The roots of radical Islam as a revivalist movement were sown by the 18th century work of Muhammad ibn abd al-Wahhab, the 1979 Islamic Revolution in Iran led by *Shi'i* Ayatollah Ruhollah Khomeni, and the 20th century evolution of Salafism as a movement containing increasing numbers of radical Muslims.[117] Today, radical Muslims are present around the world and affiliated with scores of Islamic groups and countries, to include *Shi'is* from Hezbbollah and Iran; and *Sunnis* from Hamas, Fatah al-Islam, the Taliban, al-Qaeda, and other Wahhabist derivatives, to name but a very few.[118] Radical Muslims frequently demonstrate hostility not only toward the West, but also toward those Muslims whom they judge to be apostate or corrupted.[119]

It is important to distinguish radical Islam from terrorism. As a defined group, radical Muslims are not all terrorists. That said, many within this group are terrorists.[120] By terrorists, I mean those who aim violence against innocents, in order to create fear and advance their political ends.

The use of terror as a tactic is highly problematic within the Islamic tradition. *Qur*'an 2:195 and 4:29 are often quoted as proof that terrorist suicide operations are forbidden in Islam.[121] David Cook, however, cites a number of Islamic legal rulings and *Qur'anic* verses used by terrorists to argue just the opposite. Terrorist radical Muslims distinguish between "suicide operations" and "martyrdom operations," and view martyrdom as a way to leverage minimal resources to achieve both maximum damage against the enemy, and eternal reward for the martyr.[122]

Conservative traditionalist Islam shares with radical Islam similar commitments to *Shari'ah*, *usul al-fiqh*, and *jihad*, but makes greater concessions to geopolitical realities. Here one finds a realist perspective on traditionalism. Khadduri is in many ways representative of such conservative Muslims. He seeks no reevaluation of the *Qur'an* and *Sunnah*, and no reformulation of *Shari'ah*, for he is content with the traditionally deduced law. He does, however, make concessions for Islamic nations vis-à-vis the international community and the power of the West. He argues that just as *jihad* evolved from imperialist expansion to defensive war due to the growing strength of adversaries, even so the Islamic principle of unity has had to evolve.[123] Khadduri tracks an accompanying change from the goal of a universal Islamic state, to a system of Islamic nations no longer at permanent war with the West, to the goal of an Islamic bloc of nations in common cause cooperating within the community of nations.[124] Here we find a conservative vision of unity founded not in Westphalian nationalism, but in the *ummah* living under *Shari'ah*, and united with fellow-Muslims of other Islamic nation states. Conservative Muslim approaches to unity may be found in Pakistan, Afghanistan, and many other Islamic nation states.

Neotraditionalist Islam also values *Shari'ah*, *usul al-fiqh*, and *jihad* within the historic Islamic tradition, but seeks to readjudicate the goals and objectives of Shari'ah, in order to better integrate Islam in the present. Like conservatives, neotraditionalists frequently envision the unity of Islam in terms of an Islamic bloc of nations together addressing the community of nations. But going beyond this, neotraditionalist Muslims seek an updated integration of Islamic tradition within their respective societies.

Mohammad Hashim Kamali well represents the neotraditionalist Muslim position. His assessment is that over time *usul al-fiqh* became "a retrospective construct," and "a theoretical, rather than empirical, discipline."[125] As a result, *usul al-fiqh* became literalistic, wooden, and incapable of bringing forward into present Islamic culture and society the original dynamism of the *Qur'an* and the *Sunnah*. Kamali calls for a reevaluation of these sacred texts to capture anew

> *...their emphasis on justice, equality and truth, on commanding good and forbidding evil, on the promotion of benefit and prevention of harm, on charity and compassion, on fraternity and co-operation among the tribes and nations of the world, on consultation and government under the rule of law.*[126]

Many Islamic movements may be described as neotraditionalist. These include the Muslim Brotherhood organizations found in many Islamic states, the Renaissance Party of Tunisia, the Islamic Salvation Front of Algeria, the Jamaat-i-Islami found in Pakistan and Bangladesh, and others.[127] It is significant that although such organizations may be designated as neotraditionalist, their "neo" status does not preclude their potential support for militant *jihad*.[128]

Reformed positions within Islam conceive of a different approach to the unity of the faith. While retaining a high view of the *Qur'an* and *Sunnah*, reformed Islam distinguishes between sacred traditions which may be anchored in historical conditions and enduring principles and values which may be projected across time into the present. On account of this, reformed Islam accepts only non-violent concepts of *jihad* and seeks fuller integration within a globalized, western world.

Postmodern reformed Islam finds clear expression in the work of Tariq Ramadan.[129] Many proponents of postmodern Islam focus on the Muslim experience in the West, and Ramadan is a good example. Ramadan's goal is to articulate and apply universal principles for Islam which both respect pluralism, and enable Muslims to live out their faith in modern, secular societies.[130] Based on his interpretation of Islamic sources and sciences, Ramadan identifies "three fundamentals of the universal at the heart of Islamic civilization," namely, "the encounter with the Only One, the 'full and natural faith' of the created universe, [and] the 'need of Him' as the essence of being human."[131] These fundamentals bring changed conceptions of *Shari'ah* and *jihad*, and shift the concept of Islam unity from the external to the internal.[132] This unity occurs first within the individual Muslim. First, "to be with God…all of us are required to return to ourselves and to rediscover the original breath, to revive it and confirm it."[133] From here, this unity is projected into society, because "one's *duty* before God is to respond to the *right* of human beings."[134] This solidarity with society propels postmodern Muslims into a program of engagement for: the right to life and the minimum necessary to sustain it, the right to family, the right to housing, the right to education, the right to work, the right to justice, and the right to solidarity itself.[135] From the postmodern Muslim perspective, this oneness, founded in the individual and projected into society, forms the basis of the universalized Islamic civilization.[136]

Liberal reformed Islam provides a vision similar to that of postmodern Islam, valuing the *Qur'an* and *Sunnah*, seeking enduing Islamic principles and values, and pursuing reform in the context of an increasingly modernized world. But beyond this, liberal Islam interprets the whole of the faith within the overarching categories of religious process and religious continuity. We will briefly examine both of these categories from the perspective of John L. Esposito, an ardent and articulate proponent of reformed Islam.[137]

Esposito locates Islam within the category of religious process in such a way that the historical underpinnings of the faith give way to deeper meanings which extend both backward and forward in time.[138] Islam at its emergence was "a return to a forgotten faith."[139] As such, Islam was "not a new faith but the restoration of the true faith (*iman*), a *process* that required the reformation of an ignorant, deviant society."[140] Part of this reformation entailed *jihad*, a "struggle against oppression and unbelief," which provides Muslims today "with a model and ideology for protest, resistance, and revolutionary change."[141] In short, Islam possesses a "trans-historical significance…rooted in the belief that the Book and the Prophet provide eternal principles and norms on which Muslim life, both individual and collective, is to be patterned."[142]

Esposito also portrays Islam as participating in a great phenomenological continuity of world religion. Esposito praises what he perceives

Islam, Judaism, and Christianity to hold in common – a heritage of monotheism, spiritual values, and peaceful proclamation.[143]

One might ask: what kind of reform will liberal Islam bring, being formed by religious process and continuity, and normed by enduring Islamic principles and values? The answers will vary, based on the realities of each Muslim society, but the process of contextualizing Islam within a globalized world will finally expand justice for Muslims across the domains of gender, economy, law, and politics, as Esposito sees it. As might be expected, western governments laud this vision and cheer the process.

Finally, secular-state Islam reflects that position which retains allegiance to Islam as authoritative for personal faith and practice, but rejects the role of religion in the political sphere. Egypt and Turkey are two such secular states, which have attempted to travel the difficult road to modernity while honoring Islamic piety. Significant challenges continue today.[144] Their societies view *Shari'ah* as applicable for the private and community practice of Islam, and as decisive for the true unity of Islam across the *ummah*. That said, *Shari'ah* remains officially excluded from the power relationships of government. In other words, although Islamic principles may permeate law, *Shari'ah* itself is not state law, and is not determinative for state relations. Based on this understanding of private faith practice and secular political power, Egypt and Turkey have found common cause with the United States and other western nations, and are vital partners within the community of nations.

To summarize, the above six schools of thought represent varying approaches to the practice of Islam today. Most significantly, each position holds its own view on how the Islamic faith is to achieve its universalization. Understanding these positions is a prerequisite for policy makers who would address national security issues in the Islamic world. But to this understanding we must also add an awareness of the changing nature of coalitions within traditionalist Islam.

Alignments within Traditionalist Islam

Common wisdom in the West previously assumed that the chief divide within Islam was between *Sunnis* and *Shi'is*. Whereas this may well remain true theologically, this is not necessarily the case regarding national security. As we have seen, positions within traditionalist Islam – radical, conservative, and neotraditionalist – remain open to the potential legitimacy of *jihad* as warfare, whereas reformed Islam rejects violent *jihad*. This would suggest that the most significant divide within Islam is between the traditionalist and reformed positions, but the situation is yet more complex. Recent research shows that some traditionalist *Sunnis* and *Shi'is* align themselves together against the West, while other *Sunnis* and *Shi'is* find common cause against other *Sunnis*, notwithstanding the enduring differences in motivation and strategy which obtain between *Sunnis* and *Shi'is*.

Thomas F. Lynch III notes important differences in motivation and strategy that continue to surface when *Sunni* and *Shi'ah* groups each wage militant *jihad* on their own terms.[145] He makes the case that *Shi'ah* terrorism emanates from the policy objectives of the state of Iran, and is executed as a campaign under the leadership of affiliates such as Hezbollah and the Islamic Jihad Organization. This differs in form and substance from *Sunni* terrorism, which Lynch describes as being motivated by a "theologically-driven…grandiose, ideological framework" that is executed as a wave.[146]

Samuel Helfont would not disagree with Lynch's thesis as far as it goes, but would add significantly to it. Helfont argues that if the task is "to assess the loyalties or predict the actions of various regional actors," then at least in the Middle East the dividing line in Islam lies *within* traditionalist *Sunni* Islam, with groups siding either with Wahhabism or with the Muslim Brotherhood. As evidence, he points out that in both the 2006 Israeli-Hezbollah conflict in Lebanon, and in the 2008 Israeli-Hamas conflict in Gaza, regional politics did not divide along *Sunni-Shi'i* lines. Instead,

> …*Shias* from Hezbollah and Iran sided with *Sunni* Islamists from Hamas and other Muslim Brotherhood associated organizations. On the other side of the regional divide were

> *Sunni* Arab Nationalists, traditional *Sunni* monarchs, and *Sunni* Islamists with Wahhabist tendencies.[147]

For Helfont, these represent the enduring alignments of Middle East Islamic power.

Helfont shows that these two streams of *Sunni* Islam differ greatly today. Wahhabism and their affiliated groups, such as al-Qaeda, hold to radical traditionalist Islam. They are motivated chiefly by theology, desiring to purify Islamic faith and practice by restoring radical traditionalist concepts of *Shari'ah*. Toward that end, radical Wahhabist organizations have endorsed *jihad* as offensive warfare against both the West and those Muslims deemed to be impure or corrupt.[148]

By way of contrast, Helfont characterizes Muslim Brotherhood organizations as chiefly political.[149] Willing to work with *Shi'i* and even non-Islamic groups if necessary, Muslim Brotherhood organizations seek to consolidate adequate power locally and regionally to build modern political systems that respect human rights while retaining an Islamic identity. Falling far short of the theological commitments of radical and even conservative Islam, the neotraditionalist Muslim Brotherhood is dedicated to political reform, concerned with western perception, and committed to building viable, modern Islamic states.

Just how different the Brotherhood can be from Wahhabism is shown in their approaches to *jihad*.[150] Given justifiable circumstances, the Brotherhood will employ any tactic of terrorist *jihad*, from suicide bombings to children as human shields, but only so long as the tactic may be construed as defensive. Their concerns for western perception and political settlement remain high. Wahhabists will also employ any terrorist tactic, but are willing to include *jihad* as offensive warfare because they see their warfare as divinely ordained. Not surprisingly, they accuse the Brotherhood of abandoning religious purity for political compromise. For the Brotherhood's part, they decry what they consider to be the Wahhabists' needless offenses against the West and their archaic and unworkable conceptions of the Islamic state. The strategic tension between Wahhabism and the Muslim Brotherhood is yet further magnified by Iran's drive for regional hegemony.[151]

In short, the need for nuance in understanding the Islamic world has never been greater. National security policy needs to address overlapping and competing alignments grounded in six Islamic positions, accounting for the division between traditionalist and reformed Islam, divisions within traditionalist Islam, the division within *Sunni* Islam between Wahhabism and the Brotherhood, Iran's drive for regional hegemony, and the power of other national and transnational Islamic organizations.[152]

Demographic Surveys

Having surveyed a variety of Islamic positions, can we find demographic surveys which shed light on how various Muslims view the relationship of Islam to politics, the rule of *Shari'ah*, and the use of violent *jihad* and terrorist tactics? There have been relatively few scientific studies of the demographics of those who support radical Islam or terrorism.[153] John Esposito and Dali Mogahed have published their views based on certain polling data, but did not include the data.[154] The Pew Research Center's surveys provide arguably the most dependable, comprehensive data; their initial applicable survey is the December 4, 2002 report of the Pew Global Attitudes Project (henceforth, 2002 Pew Report).[155]

Christine Fair and Bryan Shepherd have conducted rigorous analysis of the demographic variables represented in the 2002 Pew Report, yielding insights into Muslims who support terrorist tactics. Among the conclusions reached in their research are the following: (1) those who believe that Islam is under threat are much more likely to support terrorism, (2) those who believe that religious leaders should play a larger role in politics are substantially more likely to support terrorism, and (3) those who have a lower socioeconomic status are less likely to support terrorist acts.[156]

I will focus on the most recent data, from the July 14, 2005 updated report of the Pew Global Attitudes Project (henceforth, 2005 Pew Report), and the 2007 Pew Research Study, *Muslim Americans: Middle Class and Mostly Mainstream* (henceforth, 2007 Pew Study).[157]

I have selected data that focus on three areas: (1) the importance of Islam for Muslim identity and political life (Tables 2, 3, and 4); (2)

the Muslim perception of the meaning, and associated threats, of Islamic extremism (Tables 5 and 6);[158] and (3) the level of support of Muslims for terrorist actions (Tables 7, 8, and 9).[159] Values in the tables represent the percentage of responders for each specific answer to a survey question.

The 2005 Pew Report establishes the primary importance of Islam for Muslim identity and political life. When Muslims were asked how they viewed themselves – as either a citizen or resident of their country first, or as a Muslim first – respondents generally answered that they were Muslims first (See Table 2).[160]

Country	Muslim First	Person of Country First	Both Identities Equal/VR*	DK/RA**
Turkey	43	29	27	1=100
Pakistan	79	7	13	1=100
Lebanon	30	30	39	1=100
Jordan	63	23	13	0=99
Morocco	70	7	23	0=100
Indonesia	39	35	26	0=100

Table 2. Self Identity of Muslim or Citizen (Muslim respondents only)
*** VR = “Voluntary response to question” (here and in following tables).**
**** DK/RA = “Don’t know, or refused to answer question” (here and in following tables).**

This predominant religious identity carries over into the perceived role of Islam in political life (See Table 3).[161] When asked how much of a role they thought Islam played in the political life of their country, most Muslims saw Islam playing a very large or fairly large role. Comparing the 2002 data to the 2005 data does not suggest an overall trend.

Although no overall trend may exist between the 2002 to the 2005 data in Table 3, Muslims themselves believe that the religion of Islam is playing a generally greater or equal role in their countries, compared to a few years ago (See Table 4).[162]

Country (Year of Data)	Very Large Role	Fairly Large Role	Fairly Small Role	Very Small Role	DK/RA
Turkey **2005**	**30**	**32**	**16**	**14**	8=100
2002	21	25	19	24	11=100
Pakistan **2005**	**38**	**24**	**12**	**9**	17=100
2002	35	21	11	16	17=100
Lebanon **2005**	**22**	**32**	**35**	**5**	6=100
2002	33	38	15	8	6=100
Jordan **2005**	10	**20**	**49**	**19**	2=100
2002	25	25	27	22	0=99
Morocco **2005**	**57**	**18**	**9**	**9**	7=100
Indonesia **2005**	33	52	11	**2**	2=100
2002	39	47	10	2	2=100

Table 3. Role of Islam in Political Life (2002 data corrected March 3, 2007)

Country	Greater Role	Lesser Role	No Change/VR	DK/RA
Turkey	47	32	14	7=100
Pakistan	48	23	12	16=99
Lebanon	35	17	25	23=100
Jordan	18	43	38	1=100
Morocco	57	28	4	11=100
Indonesia	73	15	9	2=99

Table 4. Greater or Lesser Role of Islam in Politics, Compared to a Few Years Ago

The 2005 Pew Report shows the difficulty in trying to define Muslim extremism. The survey asked Muslims to define what Islamic extremism means to them by choosing between two options: (1) advocating the legal imposition of strict *Shari’ah* on all Muslims, or (2) using violence to get rid of non-Muslim influences in their country (See Table 5).[163] Because the two options are both marks of the position of traditionalist Islam, adding the two together would likely yield the minimum number of traditionalist Muslims in each country. Strict *Shari'ah* and the potential use of militant *jihad* are marks of the position of traditionalist Islam.

Country	Impose Strict *Shari'ah* on All Muslims	Use Violence to Remove All Non-Muslim Influences	DK/RA
Turkey	48	16	36=100
Pakistan	36	22	42=100
Lebanon	35	46	19=100
Jordan	36	60	4=100
Morocco	20	53	27=100
Indonesia	50	30	20=100

Table 5. What Islamic Extremism Means

After noting support for possible meanings of Islamic extremism, the 2005 Pew Report turns to the more significant question of the nature of the perceived threats of Islamic extremism. Individuals were asked what concerned them most about Islamic extremism in their own country. Options included: it is violent, it will lead to people having fewer personal freedoms and choices, it will divide the country, and it will set back economic development (See Table 6).[164]

Country	Is Violent	Leads to Fewer Freedoms	Divides the Country	Sets Back Development	None VR	DK/RA
Turkey	25	28	29	9	2	6=99
Pakistan	17	15	24	28	5	12=101
Lebanon	24	36	29	9	3	1=102
Jordan	21	37	26	15	1	0=100
Morocco	37	20	24	14	1	4=100
Indonesia	41	20	19	15	2	3=100

Table 6. Perceived Threats of Islamic Extremism in One's Country

It is interesting that in Table 6 the mean scores for violence (27.5), loss of freedom (26.0), and division of country (25.2) are so close to each other. In these Islamic countries the concern over violent Islamic extremism – or, more precisely, violence from Islamic traditionalism and terrorism – is essentially as intense as the concern over having fewer personal freedoms or having a country with greater divisions, as a result of Islamic extremism. This suggests a level of acceptance regarding violence and terrorism within Islamic societies that is fundamentally higher than is usually found in western societies, at least by comparison with the other accompanying threats.

Additional data from the 2007 Pew Study survey seems to bear this out. Individuals were posed the following question, with responses summarized in Table 7:

> Some people think that suicide bombing and other forms of violence against civilian targets are justified in order to defend Islam from its enemies. Other people believe that, no matter what the reason, this kind of violence is never justified. Do you personally feel that this kind of violence is often justified to defend Islam, sometimes justified, rarely justified, or never justified?[165]

		Muslims in Europe April 2006 Data				Muslims only in Muslim Countries, April 2006 Data					
Justified	U.S. *	Britain	France	Germany	Spain	Egypt	Turkey	Indonesia	Pakistan	Jordan	Nigeria
Often	1	3	6	1	6	8	3	2	7	5	8
Sometimes	7	12	10	6	10	20	14	8	7	24	38
Rarely	5	9	19	6	9	25	9	18	8	28	23
Never	78	70	64	83	69	45	61	71	69	43	28
DK/RA	9	6	1	3	7	3	14	1	8	0	3
Total	100	100	100	99	101	101	101	100	99	100	100

Table7. How Often Terrorist Acts against Civilians Justified (Muslim respondents only)
*** = U.S. Muslim respondent only data from May 2007.**

Based on Table 7 data, the number of Muslims who view terrorist acts against civilians as justified often or sometimes is quite high, ranging to over 20 percent in Egypt and Jordan, and over 40 percent in Nigeria.[166] To grasp the full extent of the acceptance of terrorist acts among Muslims surveyed, one must add all three categories of those who see terrorism as ever justified – often, sometimes, and rarely. I have done this below in Table 8.

As an example, data from Table 8 show that in the United States 13 percent of all Muslims believe that some terrorist acts against civilians can be justified. If one extrapolates this sample to the 2007 Pew Study estimate of 2.35 million Muslims in America, this could translate into as many as 300,000 American Muslims who find certain terrorist acts justified.[167] By comparison, the percentages of Muslims in Egypt, Jordan, and Nigeria who responded that certain acts of terror can be justified exceeded 50 percent.

Aggregated Data		Muslims in Europe April 2006 Data				Muslims only in Muslim Countries, April 2006 Data					
Justified	U.S. *	Britain	France	Germany	Spain	Egypt	Turkey	Indonesia	Pakistan	Jordan	Nigeria
Ever**	13	24	35	13	25	53	26	28	22	57	69
Never	78	70	64	83	69	45	61	71	69	43	28
DK/RA	9	6	1	3	7	3	14	1	8	0	3
Total	100	100	100	99	101	101	101	100	99	100	100

Table 8. How Often Terrorist Acts against Civilians Justified (Muslim respondents only)
*** = U.S. Muslim respondent only data from May 2007.**
**** = Aggregated data from respondents, the sum of all responses that said that terrorist acts can ever be justified—often, sometimes, and rarely.**

This data does not appear to be anomalous. The 2005 Pew Report followed the above general question, about Muslim perception of terrorist acts being justified, with a specific question about the use of suicide bombing against Americans and other Westerners in Iraq: Were such terrorist actions justifiable or not? See Table 9.[168]

Country	Justifiable	Not Justifiable	DK/RA
Turkey	24	62	14=100
Pakistan	29	56	15=100
Lebanon	49	41	10=100
Jordan	49	43	8=100
Morocco	56	40	4=100
Indonesia	26	67	7=100

Table 9. Are Suicide Bombings against Americans and Westerners in Iraq Justifiable?

The approximately one quarter to one half of surveyed Muslims who responded that terrorist acts in Iraq against Americans and other Westerners were justifiable corresponds roughly to the data in Table 8 for Muslims within Muslim countries and their rates of ever finding terrorist acts justified. By country, there is apparent agreement between these data sets.

We cannot say how many of these Muslims who justify terrorist acts would self-identify with radical, conservative, or neotraditionalist Islamic positions, all of which leave open the possibility of legitimate, violent *jihad*. However, it is important to note that the survey question used to gather the data for Tables 7 and 8 specifically asked about violence being justified "to defend Islam." This is the language of *jihad* and, because of this, we may reasonably infer that Muslim respondents' personal acceptance of violent *jihad* was reflected in their rates of finding acts of terror justified.

Part III: Religion as Paradigm in National Security Policy

We have seen that religion will continue to play a powerful role in influencing matters of conflict and security, and that nuance will be needed to address the varying positions within Islam. We now turn to consider alternative paradigms for integrating religion within national security policy. We begin with national security policy of President George W. Bush, the President of the United States from 2001-2009.

Religion in the National Security Policy of President George W. Bush

Because President Bush was quite open about his religious faith, it is important to briefly consider the relationship of his faith to his national security policy. President Bush's evangelical Christian faith undoubtedly provided motivation and guidance for him in his private and public life.[169] His faith also affected his construal of the adversary in the global war on terrorism.[170] That said, it appears that President Bush set policy based on his view of universal values, not his religion. For example, President Bush saw freedom and human kindness as universal values, created by God – not by the United States – for the benefit of all.[171] A critical component of that freedom was religious freedom. Because of this, it made sense to President Bush to use national security policy to encourage growth of religious freedom in problematic societies, irrespective of whether their religion was fundamentally different from his own.[172]

This view of religion as an expression of the universal value of freedom was reflected in President Bush's 2002 and 2006 National Security Strategies (henceforth, 2002 NSS and 2006 NSS).[173] I will use these documents as representative of his national security policy.

President Bush's 2002 NSS was a wartime document released just one year after 9/11. It framed the global war on terrorism as a war in defense of freedom and human dignity. The broader purpose of the 2002 NSS – "to create a balance of power that favors human freedom" – aligned with its foundational assumption – that "freedom is the non-negotiable demand of human dignity; the birthright of every person – in every civilization."[174]

Toward the end of defending freedom within the homeland and abroad, the 2002 NSS expressed eight strategic imperatives. The first and arguably primary imperative focused on growing freedom by championing the non-negotiable components of a free society, which included "freedom of worship" and "religious tolerance."[175] Moreover, the 2002 NSS articulated policy ways to achieve these freedoms: speak out clearly about violations of these freedoms, use foreign aid to support those who struggle non-violently for these freedoms, develop these freedoms through bilateral relations, and "take special efforts to promote freedom of religion and conscience and defend it from encroachment by repressive governments."[176] If my reading of the 2002 NSS is correct, this promotion of religious freedom was also intended to buttress the "war of ideas" against international terrorism. By supporting moderate Muslim governments in their efforts to build freer and more robust societies, the United States would make it harder for terrorists to plant their violent ideologies.[177]

President Bush's 2006 NSS similarly emphasized freedom as a universal desire, but it went further by elevating religious freedom to the status of "First Freedom":

> Against a terrorist enemy that is defined by religious intolerance, we defend the First Freedom: the right of people to believe and worship according to the dictates of their own conscience, free from the coercion of the state, the coercion of the majority, or the coercion of a minority that wants to dictate what other must believe.[178]

The 2006 NSS also offered additional policy ways to promote freedom of religion.[179]

Beyond these incremental changes, the 2006 NSS did advance a substantive addition to the role of religion in national security policy. It offered a strategic message that Islam was a "proud religion" that was being "twisted and made to serve an evil end." It characterized terrorists as turning the concept of *jihad* into a "call for murder," eliminating any religious freedom to disagree, even among Muslims. To meet this threat, the 2006 NSS offered both long-term and short-term strategies.[180]

Religion in the National Security Policy of President Barack H. Obama

Less than one month after his inauguration, during remarks at the first National Prayer Breakfast of his administration, President Barack Obama grounded his understanding of the role of religion in world affairs in his personal faith experience. Connected to a religiously diverse family and raised by a mother skeptical of organized religion, he came to view his mother as the most spiritual person he had ever known. She taught him "to love, and to understand, and to do unto others as I would want done." This understanding later became decisive for his own faith, which germinated in the context of community organizing in Chicago:

> I didn't become a Christian until many years later, when I moved to the South Side of Chicago after college. It happened not because of indoctrination or a sudden revelation, but because I spent month after month working with church folks who simply wanted to help neighbors who were down on their luck – no matter what they looked like, or where they came from, or who they prayed to.[181]

This personal faith perspective has led President Obama to articulate a positive view of religion as a force for unity. For President Obama, belief systems may vary, but all Christians, Jews, Muslims, Buddhists, Hindus, Confucians, and secular humanists stand united: "There is one law that binds all great religions together….the Golden Rule – the call to love one another; to understand one another; to treat with dignity and respect those with whom we share a brief moment on this Earth."[182] Based on this understanding of the essential nature of religion, President Obama has rejected as false any religion that would preach hate or condone the taking of innocent life.[183]

This view of religion as a force for unity is reflected in President Obama's national security policy. To examine this view, I have used as sources the following major speeches which bear on the role of religion in his national security policy – President Obama's January 20, 2009 Inaugural Address in Washington, DC (henceforth, Inaugural Address); his April 6, 2009 remarks to the Turkish Parliament in Ankara, Turkey (henceforth, Ankara); his June 4, 2009 "On a New Beginning" speech at Cairo University, Cairo, Egypt (henceforth, Cairo); his July 11, 2009 "New Moment of Promise" speech to the Ghanaian Parliament in Accra, Ghana (henceforth, Accra); his November 10, 2009 remarks at the memorial service at Fort Hood, TX (henceforth, Fort Hood); and his December 1, 2009 "On the Way Forward in Afghanistan and Pakistan" speech at West Point, NY (henceforth, West Point).[184]

In his Inaugural Address, President Obama announced the beginning of a new policy of rapprochement with the Muslim world based on "mutual interest and mutual respect." In Ankara, he began to unfold this policy by identifying three main objectives bearing on religion. The United States would work with the Muslim world to (1) "[roll] back violent ideologies that people of all faiths reject"; (2) listen respectfully, conquer misunderstandings, and seek common ground; and (3) "convey our deep appreciation for the Islamic faith."[185] Here President Obama began to edge past President Bush's 2006 NSS position by calling on the United States to praise the religion of Islam and by implying that Muslim terrorists were not true Muslims. In a side note, President Obama also encouraged diversity of religious expression as important for building strong and vibrant societies.[186]

In Cairo President Obama retained his three-fold emphases from Ankara, but expanded them in his bid to make "a new beginning" with Islam. Going beyond the language of common interests with the Muslim world, President Obama spoke of a "partnership between America and Islam [that] must be based on what Islam is, not what it isn't. And I consider it part of my responsibility as President of the United States to fight against negative stereotypes of Islam wherever they appear." Toward that end, the President argued that the actions of terrorists placed them outside the religion of Islam.[187] Moreover, he maintained that Islam participated in a fundamental unity with all religions: "There's one rule that lies at the heart of every religion – that we do unto others as we would have them do unto us….It's a faith in other people, and it's what brought me here today." Based on this concept of shared faith, the President challenged his Muslim audience: "We have the power to make the world we seek, but only if we have the courage to make a new beginning."[188] Retaining his previous side note, the President also encouraged his audience to embrace religious diversity to enable all people to live together.

At Accra, Fort Hood, and West Point President Obama continued to portray religion as a force for unity in matters of national security. At Accra, President Obama rejected as false any religion that would define itself over against another faith: "Defining oneself in opposition to someone…who worships a different prophet, has no place in the 21st century.…We are all God's children."[189] At Fort Hood, during the memorial service that followed the shooting that left 13 dead and

30 injured, the President reasoned that all true religions were united against such acts of violence: “No faith justifies these murderous and craven acts; no just and loving God looks upon them with favor.”[190] At West Point, President Obama judged al-Qaeda terrorists to be beyond the pale of true religion, having “distorted and defiled Islam, one of the world’s great religions, to justify the slaughter of innocents.” Returning to the language of mutual interests between America and the Muslim world, the President called for partnership in “breaking a cycle of conflict” and in “[isolating] those who kill innocents.”[191]

Three Paradigms for the Role of Religion in National Security Policy

Religion as Freedom. The role of religion in the national security of policy of President George W. Bush suggests a paradigm of Religion as Freedom.[192] The narrative of this paradigm runs as follows: Freedom is a universal value. All people everywhere desire to live in free societies securely, with equal rights under the law. Chief among these rights is the freedom to choose one’s religion and worship according to one’s conscience. Current adversaries such as the Taliban and al-Qaeda wield power defined by religious intolerance, intending to establish repressive rule that would deny inhabitants their freedoms. To defeat these adversaries, the long-term solution requires working within the Muslim world to build and strengthen democratic institutions, in order to protect the rule of law and individual freedoms, including the freedom of religion.[193]

This paradigm suggests certain national security policy options that leverage Religion as Freedom: Support moderate Muslim governments and isolate radical Muslim terrorists, to help build freer societies and to make it harder for terrorists to plant their violent ideologies of religious intolerance. Champion religious freedom and speak out clearly against religious oppression. Praise the actions of, and award foreign aid to, moderate Islamic governments that work to promote freedom of religion. Build religious freedom through linkage with other policies across all elements of national power. Work multilaterally to encourage Islamic governments to support freedom of religion and to discourage terrorists who repress such freedoms. Show religious sensitivity.

Analysis of the paradigm of Religion as Freedom follows: The pros of this paradigm are that it resonates with the enduring American value of freedom; is fully transparent to the American public; enables a slightly nuanced understanding of various Islamic positions, distinguishing between those which support freedom of religion and those which do not; and takes the long view of growing peace in the Muslim world by growing institutions of freedom. The cons of this paradigm are that it emphasizes a western concept of freedom to choose and worship God over an Islamic concept to submit to God, omits any discussion of the decisive nature of Islamic unity,[194] fails to promote understanding of evolving alignments within traditionalist Islam,[195] and locks itself into a monolithic "freedom" framework for addressing the role of religion in future conflicts. These problems suggest that this paradigm will not find traction in the Muslim world, at least in the short run.

Religion as Unity. The role of religion in the national security of policy of President Barack H. Obama suggests a paradigm of Religion as Unity.[196] The narrative of this paradigm runs as follows: All religions are bound together by a universal moral law to love one another and to treat each other with dignity and respect. Religion is finally faith in humanity. Because of this, the religions of the world are a powerful force for unity, properly used to encourage people to work to understand each other and to resolve conflict. Any "religion" that preaches otherwise – propagating hate, violence, or opposition toward another religion – is no true religion, but only a fraud and defilement. Islam is a religion which embraces peace and rejects violence. Current adversaries such as the Taliban and al-Qaeda represent no religion, but only hate and violence. To defeat these adversaries, the long-term solution requires forming an enduring partnership with the Muslim world, seeking opportunities to honor the Muslim faith, address mutual misunderstandings, and locate and pursue mutual interests.

This paradigm suggests certain national security policy options that leverage Religion as Unity: Enter into dialog with all Muslim governments with the intent of showing honor to Islam, resolving mutual misunderstandings, and pursuing mutual interests – especially to isolate violent terrorists. Integrate the strategic communication that all true religions are a powerful force for unity through their common commitment to love humanity, spread peace, and reject violence. Champion Islam as a religion of peace, and fight negative stereotypes. Praise the actions of, and award foreign aid to, moderate Muslim governments which work to resolve disagreements through dialog and non-violent means. Work multilaterally to encourage Islamic governments to marginalize violent ideologies and to enact policies that show dignity and respect to people of all faiths. Show religious sensitivity.

Analysis of the paradigm of Religion as Unity follows: The pros of this paradigm are that it resonates with many Muslims through its praise of Islam, undercuts certain terrorist recruitment arguments which vilify the West, leverages religion as a force for unity, takes an immediate view of growing peace in the Muslim world through open dialog with all Muslim governments, and promotes some understanding of evolving alignments within traditionalist Islam through open dialog. The cons of this paradigm are that it employs a concept of religious unity that assesses a moral equivalence between world religions, which traditionalist Muslims do not accept; generalizes Islam into a caricature of peace, failing to provide a nuanced understanding of varying Islamic faith positions or to address data that show support for terrorist tactics between 22 percent and 69 percent in certain Muslim countries;[197] appears to lack full transparency to Americans who are aware of rates of Muslim support for terrorism; omits any discussion of the decisive nature of Islamic unity;[198] and locks itself into a monolithic "unity" framework for addressing the role of religion in future conflicts. These problems suggest that this paradigm will run headlong into serious difficulties in the long run.

Religion as Ideology. The preceding discussion of the paradigms of Religion as Freedom and Religion as Unity shows how hard it is to locate an adequate framework for integrating religion within national security policy today. Each paradigm has its own strengths and weaknesses, but neither rises to the level where its discussion of religion contributes robustly to the promotion of national security.

We must certainly value the strengths of these paradigms. Each paradigm brings an important truth to the table. We should understand freedom of religion as a necessary component of free and robust societies, and work to plant and nourish that freedom. It is also true that religions often share a moral commitment to care for one's neighbor, and that cooperative ventures to meet human needs can build human trust. Each paradigm rightly encourages respect for religious expression and commitment.

That said, we must also account for the weaknesses of these paradigms. Taking a step back and looking at the entire policy formulation process, the reason for the weaknesses becomes clear. Although each paradigm brings an important perspective to the table, each does so apart from a prior assessment of Islamic power within the strategic environment. It is all well and good to begin with the enduring values of the United States (as the Religion as Freedom paradigm does), or liberal democratic values (as the Religion as Unity paradigm does), and then to frame national interests in terms of those values. But policy rests not only on national interests, but also on a grand strategy and strategic vision that comprehend strategic power and threat. Operationally the adversary always gets a vote. To frame the adversary in terms of our enduring national values or liberal democratic values – which is essentially what each of these two paradigms does – will ensure that our strategic vision and policy, although partially correct, are fundamentally flawed. The adversary must be known in terms of his values, his center of gravity, and his objectives. Effective policy rests on the creative interplay of our values which beget our national interests, with our strategic vision which comprehends the nature of the power of an adversary.

This means that there can be no adequate determination of the role of religion in national security policy apart from a logically prior and accurate assessment of an adversary and his power. In the case of our current adversaries, this means that we must first understand radical Muslims and terrorists by way of their values, their center of gravity, and their objectives. To the extent that these are based in religion, we must understand their view of, and participation in, Islam as power. Only then can policy makers bring our values-generated interests to bear on the adversary's power as it actually exists.

This suggests a new paradigm for the role of religion in national security policy. If at the level of grand strategy and strategic vision religion matters as a source of power, then at the level of policy religion matters as a source of behavior. Religion motivates, enables and directs behavior which can have consequences for national security. In this sense we are not discussing religion in its capacity as divine path, but religion in its capacity as ideology, i.e., as a moral framework of ideas that drives actions, values, and objectives. This is what I mean by the paradigm of Religion as Ideology.

This paradigm is particularly important because the federal government of the United States is religion-neutral.[199] There is no place in United States national security policy for religion in the capacity of advocate for one faith or judge of another, but only for religion in its capacity as empowerment of human behavior. The focus must not be on belief, but on behavior. Such empowered behavior must be in view as national security policy frames its options to influence behavior toward the ends of our grand strategy in support of our national interests. This is especially critical because religious behavior frequently reflects the fullness of human aspiration in light of the breadth and depth of the human condition.

Part II of this paper attempted to provide the underpinnings of an estimate for a grand strategy and strategic vision that comprehends Islam as power. The paradigm of Religion as Ideology would argue the necessity of contextualizing this understanding of Islam as power before generating related national security policy options. First distinguish Islamic actors at the transnational, national, regional, and local levels by their behaviors. Identify their actions which demonstrate their understanding of *jihad*, their concept of universalizing Islam, their position relative to alignments within traditionalist Islam, and their support of terrorist violence. Second, for analytical purposes, aggregate those actors which demonstrate similar actions, values, and objectives. Only then formulate policy options, in light of our values-generated interests.

Examples of policy options might include: Integrate the strategic communication that the United States is committed to enhanced freedom, peace, and prosperity for its Muslim friends, but will oppose all those who use violence to achieve their political ends. Informed by the above critical distinctions regarding Islam as power, issue statements that articulate ideological differences between Islamic actors in terms of behaviors and objectives, taking care to neither praise nor judge the religion of Islam. In these statements identify positive actions such as participating in peaceful dialog and consensus building, committing publicly to peaceful coexistence with those of different faiths, protecting broader freedoms, honoring the value of every human life, showing respect for religious diversity, and meeting critical human needs. Also identify negative actions such as violence and repression against innocents, against women, and against those of other faiths; support for terrorism; and destruction of infrastructure. Enact a diversified policy of engagement with a continuum of rewards and support for actors with positive behavior, and consequences for actors with negative behavior. Use this diversified policy to move Islamic groups and governments incrementally toward the positive end of the spectrum. Work multilaterally wherever possible to support moderate Muslim governments and isolate radical Muslim terrorists by revealing the full costs of their actions. Use available elements of national power, both soft and hard, to support our national interests and the mutual interests we hold with the Muslim world. Synchronize policy actions across the interagency. Show religious sensitivity. Encourage respect for religious commitments.

The advantages of the paradigm of Religion as Ideology are numerous. First, this paradigm is based on a strategic vision that comprehends the power of Islam understood in terms of varying concepts of universalizing Islam, different forms of *jihad*, evolving alignments within traditionalist Islam, and various levels of support for terrorist violence. Second, it promotes a more nuanced understanding of different Islamic groups based on their behavior. Third, it allows a diversified continuum of "carrot and stick" responses based on the relative behaviors of actors. Fourth, it brings the fullness of American values to bear through articulated national interests vis-à-vis national security issues, without the limitations inherent in monolithic paradigms such as Religion as Freedom, or Religion as Unity. Fifth, it should appeal to moderate Muslim governments as the United States works multilaterally to pursue mutual interests and isolate terrorists. Sixth, it conforms to the traditions of the religiously neutral federal U.S. government, neither advocating nor judging any religion, but only focusing on behaviors in light of national security concerns. Finally, the paradigm of Religion as Ideology should appeal to the American public as fully transparent.

There are at least two risks associated with implementing this paradigm. First, changing from the paradigm of Religion as Unity to the paradigm of Religion as Ideology might appear to some western and moderate Islamic audiences to signal a new, negative orientation toward Islam. Second, terrorist recruiters might seize on the changed rhetoric of a United States which was no longer praising Islam as yet further justification for fighting the West.

Part IV: The Way Ahead

Part I of this paper has shown that religion matters and will continue to matter in national security challenges for the foreseeable future. Toffler, Fukuyama, Huntington, and Kaplan may point to different root causes of future conflict, but all emphasize religion as a critical component in policy that would address those challenges. This is all the more true because religion frequently reflects the fullness of human aspiration against the sobering reality of the human condition.

The study of the power of Islam in part II of this paper has revealed an Islam that is far from monolithic. Islam today is manifested in many forms, reflecting multiple perspectives on how the faith is to achieve its universalization, on what *jihad* means, and on when, if ever, terrorist tactics are justifiable in defense of Islam. Traditionalist conceptions of Islam maintain the continuing applicability of *Shari'ah* as state law, and the potentiality for *jihad* as warfare, with an average of over 20 percent of Muslims in Muslim-majority nations finding terrorist acts ever justifiable in defense of Islam. Liberal and post-modern reformists, on the other hand, generally condemn violent *jihad* and seek peaceful relations with the West. An accurate assessment of Islam as power will inform that grand strategy and strategic vision on which effective national security policy rests.

A review of the national security policies of President George W. Bush and President Barack H. Obama in part III has demonstrated the incredible difficulty of bringing religion to bear within national security policy. Weighing the alternative paradigms of Religion as Freedom, Religion as Unity, and Religion as Ideology, I have suggested that the last paradigm offers the greatest utility. It calls for a strategic vision that comprehends the power of Islam, it enables a nuanced understanding of Islamic groups based on their behavior, it facilitates a diversified continuum of policy rewards and consequences based on that behavior, and it refrains from violating the American tradition of the federal government neither advocating for nor judging a religion.

Certain practical matters will need to be addressed if religion is to gain currency within national security policy. If we move closer to the paradigm of Religion as Ideology, it will be important to head off any erroneous public perception that the United States is shifting to a negative strategy toward Islam. U.S. officials will need to state emphatically that America has no policy for or against any religion, that we promote full freedom of worship, and that we seek partnership based on mutual interests and mutual respect with people of all religions. Actions will need to follow these words. The United States will need to reach out with renewed vigor through diplomatic summits and multilateral engagements with the Muslim world to build consensus wherever possible. Certainly this would include partnership in the continued defense and support of peaceful Islamic governments against terrorist violence.

To support a more robust role of religion in national security policy, United States combatant commands should consider ways to include religion in all campaign design and planning. Campaign design activities include framing and reframing the operational environment, problem, and operational approach. Designing with religion in mind will help combatant commanders better understand their actual environment, grasp the deep roots of complex problems, and create opportunities to provide enduring solutions.

Campaign planning should also include vigorous consideration of religion. In current overseas contingency operations, religion contributes directly to stakeholder identity, power, strategic alignment, and operational outcome. To strength planning, one option would be to integrate religion as a phased line of effort (LOE) in addition to current LOEs defined by political, military, economic, social, infrastructure, and informational (PMESII) systems.[200] This would raise religion's operational significance, but might risk reducing its human significance if religion were to become merely a manipulated element of power. Another option would be to add religion as a supporting objective under both the political and social LOEs. This would again raise religion's operational significance, but might additionally elucidate its human significance within political and social systems. Religion must be understood as a power directing, guiding, and living through the behavioral choices of its adherents across formal and informal political, social, and cultural systems.

An issue of supreme importance will involve calculating the strategic room needed for various conceptions of achieving the universalization of Islam. As part II of this paper has argued, the critical issue for Islam today is determining how the faith will achieve its final vision of unity. Various positions within Islam answer this question differently – radical Muslims through the mechanism of militant *jihad*, conservative Muslims through the vision of a united *ummah* living under *Shari'ah*, neotraditionalist Muslims through an updated integration of Islamic tradition within their respective societies, reformed Muslims through a determination and application of enduring Islamic principles to enable Muslim life in modern societies, and secular-state Muslims through a private and community practice of *Shari'ah* that excludes the power relations of government. In all cases, policy makers will need to understand the conceptions of universalization to which various Islamic positions aspire. Even more, policy makers will need to determine how much active support or passive space the national interests of the United States can afford or allow toward the fulfillment of those aspirations. Knowing the parameters could amount to a national security imperative.

Finally, that religion will continue to matter, and matter a lot, in the national security challenges of the United States may be a bitter pill for secularist western liberals to swallow. Certain political advisers, academics, and senior leaders of the professions of arms may find it difficult to believe that many 21st century people are still motivated by religion, and that some are even willing to fight and die for their beliefs. Their incredulity is easy to document. National security policy statements, academic texts on cultural frameworks, and even military manuals on counterinsurgency doctrine can discuss their subject matter without examining religion as a power which motivates human behavior. I encourage all to rethink their assumptions and reengage in these critical arenas.

A Commander's Strategy for Social Media*

Colonel Thomas P. Mayfield III
United States Army

> *We must hold our minds alert and receptive to the application of unglimpsed methods and weapons. The next war will be won in the future, not the past. We must go on, or we will go under.*
>
> —General of the Army Douglas MacArthur, 1931

In 1931, General MacArthur could not have imagined many of the forms of warfare that would be used just a few years later during World War II. He understood, however that changes in methods and weapons can alter the nature of conflict. Just as machine guns, tanks and aircraft changed the nature of conflicts, so did the telegraph, radio, television, and eventually the internet. The advances today in the information world, specifically with the advent of social media, or new media, may prove to be as profound as any of these inventions. We must therefore observe and adjust our information strategies in order to not "go under."

One of the challenges commanders now face is to develop strategies that recognize the shifts in the nature of warfare resulting from social media. There are already examples of militaries that have ignored the realities and have suffered. The effective use of social media may have the potential to help the U.S. military better understand the environment in which it operates. Social media may allow more agile use of information in support of operations. Finally, it may be harnessed to help achieve unity of effort with partners in conflict. Finding clever and innovative ways to help achieve the desired ends may be the key to success in a continuously evolving social media environment.

The social media phenomenon is changing the way information is passed across societies and around the world. The rapid spread of blogs, social networking sites, and media sharing technology (such as

* This paper was originally published by "Joint Force Quarterly," (Issue 60, 1st Quarter, January 2011) and is republished here with their permission.

YouTube), aided by the rapid spread of mobile technology, are also changing the conditions in which the United States conducts military operations. The speed and transparency of information has increased dramatically. Events that only a few years ago could remain state secrets indefinitely are being reported around the world in minutes. The traditional roles of the media are changing with the ubiquitous nature of data transmitting technology. Citizens with simple cell phone cameras can transmit unfiltered damning images to the world in the time it takes to make a phone call. People can use social networking to mobilize groups in support of a cause without having to expose themselves to the risks and costs formerly associated with activism. In response, governments and institutions can do little to effectively stop it. The aftermath of the June 2009 elections in Iran provides an example of how social media may be changing the nature of political discourse and conflict in the world.

Tehran, June 20, 2009

Neda Agha-Soltan was sitting in her Peugeot 206 in traffic on Kargar Avenue. She was accompanied by her music teacher and close friend, Hamid Panahi, and two others. The four were on their way to participate in the protests against the outcome of the 2009 Iranian presidential election. The car's air conditioner was not working well, so she stopped her car some distance from the main protests and got out on foot to escape the heat. She was standing and observing the sporadic protests in the area when she was shot in the chest (reportedly by a member of the Basij, the pro-government Iranian militia). As captured on amateur video, she collapsed to the ground and was tended to by a doctor and others from the crowd. Someone in the crowd around her shouted, "She has been shot! Someone, come and take her!" The videos spread across the internet virally, quickly gaining the attention of international media and viewers. Discussions about the incident on Twitter, a popular micro-blogging site, became one of the most viewed topics worldwide by the end of the day on June 20, 2009.[1]

What happened next reveals the potential power of social media. Within hours, several versions of the video were posted on YouTube and linked to various other websites. Millions saw the gruesome photos of Neda's death when they were posted on blogs, websites, Facebook pages and internet news sites. The images of Neda's death highlighted the harsh response from the Iranian government and added fuel to the next ten days of violent protests in Tehran. Many people around the world began posting editorials about the protests and the Iranian government's oppressive reactions. Twitter reported millions of "Tweets," or 140 character long comments, most condemning the Iranian government and its supporters. Iranian students began using Twitter and Facebook, as well as Flickr, the social site that allows users to post and share photos, to communicate to the Iranian audience information about when and where the next protest would take place, and which streets to avoid because of police or militia checkpoints.[2]

The case of Neda demonstrates that social media is not easily contained. Even with all the measures taken by the Iranian government, the images of the protests and the reports of the government's abuses continued to somehow make it to the web. The protestors quickly devised ways to get around the government efforts to impose blocks on their networking. The Iranian government eventually managed to control much of the online traffic, but it was too late to stop the effects of the social media. The Iranian government received massive diplomatic pressure from governments and condemnation from media around the world to put an end to the post-election violence.

Around the world, social media is becoming a commonplace tool for political and social activism. If military leaders do not fully understand these social networking tools, they may miss the significant impact of the social media on the nature of future conflicts. America's potential enemies are using these technologies now to enhance their efforts. The U.S. military can either engage in the social media environment seriously or cede this ground to the enemy.[3] The development of strategies to account for the impact of social media will be one of the keys to success in future operations.

The germane question to answer is: How can an effective social media strategy have an impact on the outcomes of military operations? A recent *Military Review* article described the use of new media tools in the Second Lebanon War involving Israeli forces and Hezbollah in the summer of 2006. The article then contrasted that with Operation

Cast Lead, when the Israeli forces attacked into the Gaza strip in December 2008 and January 2009. The contrasting approaches taken by the Israeli forces in the two operations highlight how an effective new media strategy can impact the strategic outcomes.[4]

In 2006, during the Second Lebanon War, Hezbollah effectively integrated information operations, including social media, into their tactical operations to fight the Israelis. Hezbollah embedded photos and videos into blogs and YouTube to promote their image and to highlight negative perceptions of Israeli operations. Hezbollah used information very effectively to limit Israel's strategic options. After 33 days of fighting, a cease fire was declared and Hezbollah claimed victory. Hezbollah was able to create a perception of failure for the Israeli forces. During the 2006 war, Israel ignored the realities of the new media and relied instead on traditional information policies. They were less agile than Hezbollah and were unable to match them in the information war. In contrast, by 2008-09 in Operation Cast Lead, the Israeli forces devised a more effective strategy for the use of new media. The Israelis developed a proactive information strategy, incorporating social media tools, YouTube and Twitter, along with enlisting the support of the Israeli online communities, the Israeli forces were better able to set the agendas in the media and control the perceptions of the fighting. The result was the Israelis used information effectively to preserve strategic options enabling them to achieve their objectives.[5]

A Strategy

The strategic framework used by the U.S. Army War College defines a strategy as the relationship between ends, ways, and means. In order to develop a strategy, you must first have objectives or "ends" in mind. The "ends" are the objectives or the goals sought by the commander devising the strategy.[6] With respect to social media, what are some of the ends a commander might have in mind?

Perhaps the first end commanders should have in mind when determining their strategy for social media is to develop a better understanding of the environment, or better situational awareness, through an effective use of social media. By systematically observing the online community in the area of responsibility (AOR), commanders may be able to develop an ongoing understanding of the society, their concerns and interests, and they may be able to identify emerging trends and patterns. Blogs and social networking sites may be able to provide insight to any society where there is a significant online community, particularly in societies with a relatively young population. The Department of State (DOS) has effectively used social networking sites to gauge the sentiments within societies. The U.S. embassies in many nations are effectively using Facebook and other social media tools in places like Podgorica, Damascus, Phnom Penh, and Panama to maintain relationships with the local cultures, particularly with the youth who are more likely to engage using social media.[7]

Maintaining a social media presence in deployed locations will also allow commanders to better understand potential threats and emerging trends within their AORs. The online community can in many ways provide a good indicator of the prevailing mood and emerging issues within a society. Many of the vocal opposition groups will likely use social media to air grievances publicly. In *Military Review* in the fall of 2008, General David Petraeus wrote an article entitled Multi-National Force – Iraq Commander's Counterinsurgency Guidance. In the article, he lists key tasks for his commanders in Iraq. While the tasks listed in the article are intended for fighting the insurgency in Iraq, many of them are universally applicable. For example, he says it is important for commanders to "Understand the neighborhood" and "Live among the people."[8] An online social media presence can be an integral part of understanding the issues and attitudes in a neighborhood or community. An online presence can play a significant role in "living among the people" in a society that has a significant online community. Social media will certainly not be the only tool used by commanders, however it may enable the commander to better understand his environment and allow him to have better situational awareness of his environment.

A second desired "end" for social media in a theater of operations may be to assist the command in providing better, more agile, and credible public information in the AOR (both Strategic Communication and local/tactical information). As demonstrated in the example above of the Israeli defense forces, aggressive engagement in the social media environment can aid a commander in winning the information fight. General Petraeus' guidance emphasizes the importance of several related tasks. He says in his guidance to "fight the information war relentlessly" and to "be first with the truth."[9] Clearly a social media program can play a key role in accomplishing these tasks. Understanding that social media has altered the way news is reported and the speed with which it is reported, commanders will be best served if they are actively engaged in the environment. With an aggressive online presence, commanders can be better prepared to counter false and negative reporting as events occur. They can better interdict and react to bad news if they are already engaged and understand the way reporting in the AOR is likely to proceed as events occur. Finally, by being proactive, commanders can avoid letting the enemy elements set the agenda, by being first with the truth. As demonstrated in Operation Cast Lead in Gaza, commanders can use social media to help set the agenda in a strategically beneficial way.

The third and final "end" for commanders using social media in an AOR is enhanced unity of effort. General Petraeus in his guidance says that commanders should strive for unity of effort with the embassy, the interagency partners, local governmental leaders and non-governmental organizations (NGOs) to make sure all are working to achieve a common purpose.[10] The characteristics discussed earlier relating to the ability of social media to aid in organizing can be used to enhance unity of effort with partner organizations in the theater of operations. The Israeli Defense Forces used new media methods to enlist the support of the Israeli "blogosphere" to help achieve a common purpose during Operation Cast Lead. A proactive and innovative social media strategy, using social networking, blogs, and Twitter-like capabilities can aid commanders in ensuring all concerned entities in the theater of operations are sharing the necessary information to work towards a common goal.

The Ways

The second element in developing a strategy is to identify the "ways" or how one organizes and applies the resources.[11] What are the organizational schemes and methods required to achieve the ends the commander has stated?

The first of the ways to enable social media to achieve the commander's desired ends is the concept that the social media use must be in the form of a Commander's Social Media Program. That is to say, the social media should have the support and interest of the commander and key members of his staff, and should be formalized into a program with responsibilities assigned to members of the commander's staff. The commander should view social media as an asset rather than a threat. Social media planning should be incorporated across the spectrum of conflict. The commander should state his intent for information effects explicitly, noting the role social media will play. That will allow his staff to generate options much the same way as for other combat multipliers. A proactive engagement with social media incorporated into the commander's operational planning will likely provide the best results.

There will certainly be skeptics about the need for a command social media program. In an article linked to the Department of State's Social Media Hub, entitled *Eight Ways to Ruin your Social Media Strategy*, mistake number one is: "Pretend you can do without it."[12] As seen in the case of the Israeli Defense Forces' experience, ignoring new media is done at your own peril.

A second way to take advantage of social media is to organize the social media program for success. The U.S. military has experimented with ways of organizing for success in strategic communication (SC) for the last few years. The experience gained in organizing for SC may provide some insight to organizing for social media success as well. The Joint Warfighting Center's *Commander's Handbook for Strategic Communication* lays out five models that have been used for organizing SC.

The options include:

1. Increased Command Emphasis (Least Costly)
2. Tasking an Existing Staff Leader
3. Direct Planning Team Integration
4. Centralized Control of all Strategic Communication-Related Activities under a Separate Directorate (Most Costly)

5. Strategic Communication Director with a small coordinating staff and supporting Strategic Communication Working Group.

The final option has gained the most traction in the field, with several combatant commands adopting a similar structure.[13] That option provides the commander the ability to incorporate the best attributes of the other options and maintain an appropriate level of command emphasis on the SC program. While commanders may choose to employ a similar methodology for social media, integration of social media planning into an already existing SC structure may also be an effective way to ensure success. There may be synergy created by integrating the social media program into the SC program. Commanders will have to evaluate the costs with the potential benefits in their particular situation.

The natural reaction of many commanders may be to assign one staff section as the proponent for the social media, (option 2 above) leaving the responsibility for integration to them. While that approach may be easier to implement than some of the other options, the risk is the social media program will become viewed as a niche program and will not get the attention it might deserve. Further, the social media program would assume the natural biases of the assigned staff element, decreasing its broad effectiveness. For example, if the J6 (Command, Control, Communications, & Computer Systems staff section) were the proponent, they might input a technical bias, and likewise the Public Affairs (PA) section might tend to approach social media as a media outreach tool only. Thus broad integration may provide the best opportunity to achieve the results desired.

The third way to benefit from social media is the creation of a Social Media Monitoring Team. This team is to be the eyes and ears of the strategy team. They may be viewed as "Social Media Scouts," observing, monitoring and collecting information on the state of the online community in the AOR. The monitoring team represents a systematic way to take advantage of the content and trends ongoing in the social media. Without a systematic approach, there may be little chance of making accurate observations and drawing the correct conclusions from the online traffic in the AOR. If every staff section were to independently monitor Facebook, Twitter, YouTube, or the local language versions of social networks and blogs, without lateral coordination within the staff, there will likely be significant gaps in the monitoring of the social media environment.

The monitoring team should contain broad staff representation in order to be effective. The team will require members with local language skills, cultural understanding and a high degree of familiarity with the social media tools and protocols. In order to be effective they will need to conduct field research in the AOR. They will need to observe the internet cafes and local habits in the AOR and become familiar with the social media platforms popular in the culture. The team will become the experts in the command on the social media activity within the AOR.

The fourth way to ensure success in a social media strategy is to find a balance between security and sharing. The information security concerns over experimentation of social software on DoD computers are not trivial. Security officers will be inclined to say "No" to extensive use of social media on networks that are used for official purposes.[14] There is considerable discussion within the DoD on this issue. The services have significant disagreement on the right level of access to allow, balanced against the need for security. The DoD policy released on February 25, 2010 directs that "all NIPRNET [unclassified networks] shall be configured to provide access to Internet-based capabilities across all DoD Components."[15] The policy goes on, however, to give the components significant latitude to take actions to limit access to defend against malicious activity when needed. There may be ways using firewalls or separated networks to ensure security of information while still benefiting from the use of social media. Each command will have to weigh this balance and make the decision based on their needs.

Since speed and agility are key elements of successful social media strategy, the fifth way to enhance success in a strategy is to enact policies to allow the social media campaign to be agile. Restrictive and cumbersome approval chains may inhibit the ability of the operators to achieve results. Perhaps the best approach is to allow for centralized planning and decentralized execution.[16] The enemy will not be constrained by cumbersome approval process for posting information to the Internet, and has the ability to act very quickly. Operation Valhalla in Iraq in 2006 provides an illustrative example.

During a successful firefight against the Jaish al Mahdi (JAM) forces, U.S. Special Forces and Iraqi forces killed a number of enemy fighters, rescued a hostage, and destroyed a weapons cache; by all measures, a very successful operation. By the time the U.S. and Iraqi forces returned to their base, someone repositioned the bodies and removed the weapons of the JAM fighters so that it looked like they were murdered while at prayer. They photographed the bodies in these new poses and uploaded the images onto the internet, along with a press release explaining that American soldiers killed the men while they were praying in a mosque. All this took the enemy less than an hour. The public reaction was predictably negative. The U.S. forces had a combat camera crew with them during the operation, and some of the soldiers wore helmet cameras. The U.S. forces were in possession of the evidence to disprove the claims, but a cumbersome and highly centralized process for releasing information prevented the correct story from reaching the media for nearly three days. By the time the U.S. forces released the correct version of Operation Valhalla, the strategic damage was done.[17] The inability to react immediately to the enemy claims in the previous example was largely for policy reasons. To promote agility the U.S. military's policies must allow for decentralized execution of operations involving new media.

Decentralization of execution will, however, force commanders to accept levels of risk with which they may not be comfortable. The commander will essentially delegate the control of information releasing authority to uncomfortably low levels. Clear rules of engagement (ROE) distributed to all the potential social media operators may be able to mitigate the risks. The need for agility will often conflict with the need to carefully control the strategic message.[18]

One of the key elements for commanders to enhance agility in their social media program is to allow and encourage social media operations to be executed even at the lowest unit level. Many of the closest relationships established in an AOR are done so at battalion level and below. The local government leaders, the tribal leaders, the local police and militias are all developing relationships at the very lowest levels. The leaders at these units will know how best to interface with the local population. Local websites and blogs, and links to Facebook pages can be used for local activities. In Africa, there are examples of local groups reporting tactical information like roadblocks and ambushes to websites set up by DOS teams. The website then consolidates them on a map for locals to check when they are travelling.[19] Commanders may be able to enhance local relationships with the positive use of social media at the unit level.

The sixth and final way in which a commander can take advantage of social media is to set up social networking sites as an outreach tool to enhance unity of effort. As General Petraeus mentioned in his guidance, there are a number of key partners in theater with whom units must cooperate. Seemingly simple efforts like establishing a Facebook page can allow partner organizations to better understand the commander's intent. Joint Task Force (JTF) Haiti, supporting relief operations in the aftermath of the January 2010 earthquake, has effectively used social media as a tool for outreach to other organizations engaged in the effort.

There are numerous key relationships in the AOR relative to the social media strategy. The obvious ones are the local governments, the NGOs operating in the area, the local press, local civic organizations, and the local populace in general. Commanders should also consider outreach to the local blogger community (if there is one), local businesses, the internet service provider, and the cellular network providers. These relationships will better enable the social media program to be effective and adaptable to changes.

The Means

The final component in the development of a strategy is the identification of the "means." The means are the resources available to pursue the objectives. Fortunately in the U.S. military today the means to conduct an effective social media strategy are readily available. The skills and resources already contained in the U.S. armed forces today are the ones needed to be successful in the social media environment. To employ the strategy listed above, there may be a requirement to reorganize and re-prioritize resources within deployed headquarters as described in the discussion of the "ways," but there will be no wholly new skills or equipment required.

Some of the key means or resources required will be the individual talents and skills of our service members. Skilled information operators, public affairs specialists, and intelligence collectors and analysts are already conducting operations at all levels and in all services of the DoD. Language and cultural skills will continue to be a critical factor in our ability to conduct operations around the world. When engaging with social media, operators who are trained to function effectively in the cultures in which we are operating will be key assets. The "digital natives" will be critical to success in the social media environment as well. In a report following the *New Media and the Warfighter* workshop, the authors defined digital natives as "those young service members who are savvy in the use of new media devices, platforms, networks, and possibilities – and are underexploited assets in the information-led wars against new adversaries."[20] Employing these younger and more tech savvy operators in roles that will have strategic impact will require some change to the traditional hierarchical mindset. The bright and talented personnel will continue to be the foundation for success.

These digital natives however, may lack the strategic insight and understanding of more senior strategists and planners. Strategic thinkers will have to provide clear guidance and oversight to ensure the actions of the digital natives match the strategic intent of the commander. In order for the relationship between the leaders and the operators to work, the senior leaders must have an understanding of the capabilities and limitations of social media. Social media may be one case where the senior leaders must be trained to have an understanding wof hat the soldiers and junior officers already know. Inclusion of an introduction to social media into commanders' courses may be an appropriate initiative.

Finally, the military's ties with academia and industry will be more important than ever. These relationships have already been established. The DoD has some very effective ties with the blogger community and with many companies who are engaged throughout the social media community. The relationships currently enjoyed by the DoD today will have to continue to grow in order to ensure the success of any social media strategy.

Conclusion

Social media or new media is changing the way information moves around the world. Speed and transparency of information have increased, the roles of traditional and new media are changing, and the social networking tools allow collaboration as never seen before. There will no doubt be changes to the nature of conflicts as a result. A key to successfully adapting to the changes will be the ability of commanders to develop strategies that take advantage of the changes, and deny the enemy exclusive rights to the same. The U.S. military has the tools available to perform the tasks inherent in a strategy that will allow it to take advantage of the emerging trends in information. An innovative strategy that takes advantage of the lessons already learned in the social media environment will allow the U.S. military to improve its ability to understand the environment, communicate more effectively and generate unity of effort throughout the battlefield.

Prudens Futuri

Strategic Communication: A Departmental Transformation

Lieutenant Colonel Thomas A. Davis
United States Army

> *Strategic communication is a dynamic process with responsibility held by those at the highest levels of government-the President and senior government leaders…But to do so requires a commitment not yet seen, though some steps have been taken to improve the nation's capability. What is needed is a transformation supported by resources and strength of purpose that matches the nation's commitment to defense, intelligence, law enforcement, and homeland security.*
>
> —Defense Science Board
> Task Force on Strategic Communication[1]

The ability to communicate U.S. government and U.S. military policy and purpose is vital in today's information environment. We are at a precipice in the battle of the information environment. Since 2002, when U.S. military forces have been actively engaged in multiple regions of the world, the worldwide perception of U.S. image has consistently declined. According to the January 2008 Defense Science Board (DSB) *Report on Strategic Communication*, "The United States faces continuing decay in support for U.S. policy and rising anti-Americanism, which challenges national interests."[2] Additionally, according to the 2009 Pew Research Center's *Global Attitudes Project*, since the election of President Obama, "it reveals the Muslim world remains largely immune to Obamamania. In predominantly Muslim nations, widespread concerns about American policy and American power linger."[3] More than a year into the current administration, there are still extensive anti-American feelings throughout the world.

This paper reviews the capabilities gap between existing organizational structure of the DoD Strategic Communication enterprise, and the nation's requirements for communication strategies. Its premise is that effective strategic communication strategies can influence the nation's effectiveness in today's military operations/activities, and that the nation cannot execute strategies appropriate to national goals without a transformed resourcing of the SC enterprise.

Strategic Communication activities are vital to achieving America's strategic goals and interests. Effective use of the national elements of power synchronizes diplomatic, informational, military and economic tools in such a way that actions and words work together to achieve the nation's goal and advance its interests. Currently within the DoD, there is no effective single advocate or department with the responsibility, capability, and the authority to ensure this. Admiral Michael Mullen, the Chairman of the Joint Chiefs of Staff (CJCS), has noted, "We hurt ourselves more when our words don't align with our actions. Our enemies regularly monitor the news to discern coalition and American intent as weighed against the efforts of our forces. When they find a "say-do" gap – such as Abu Ghraib – they drive a truck right through it. So should we, quite frankly."[4]

In his article about Strategic Communication, the CJCS identified that SC is needed not only to communicate about current and future policies and activities, but to influence development of those policies and activities with a realistic consideration of how they are to be communicated. "In fact, I would argue that most strategic communication problems are not communication problems at all. They are policy and execution problems," wrote Mullen.[5] The capabilities gap is not just a DoD problem; it is an issue that permeates the U.S. Government (USG) as well. U.S. Representatives Adam Smith and Mac Thornberry echoed this view in early March 2010 when they invited other members of the U.S. House of Representatives to join the newly created Strategic Communications and Public Diplomacy Caucus [6] to tackle the issue at the USG level: "The caucus seeks to raise awareness of the challenges facing strategic communication and public diplomacy and provide multiple perspectives on proposed solutions."[7]

In January 2008, the Defense Science Board Task Force on Strategic Communication called for a level of change and commitment that has yet to been seen.[8] That view was reinforced by Mr. Price Floyd, the acting Assistant Secretary of Defense for Public Affairs, ASD (PA) when he said, “When it comes to SC capability, we are weak, the Department of State is weak, and the National Security Staff is weak. None of us can adequately get the job done.”[9]

Strategic Communication and DoD Objectives

Only recently has SC been officially defined. The October 2009 update of Joint Publication (JP) 1-02, the Department of Defense Dictionary of Military and Associated Terms, defines SC as “focused United States Government processes and efforts to understand and engage key audiences to create, strengthen or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power.”[10]

A December 2009 DoD report to Congress further details that the SC process is designed to synchronize efforts to achieve one or more of the following:

- Improve U.S. credibility and legitimacy;
- Weaken an adversary’s credibility and legitimacy;
- Convince selected audiences to take specific actions that support U.S. or international objectives;
- Cause a competitor or adversary to take (or refrain from taking) specific actions.[11]

Within DoD, SC supports USG and DoD policy goals. DoD agencies, Geographic Combatant Commanders and the Services find guidance for SC in the National Security Strategy, National Defense Strategy, and the National Military Strategy. These documents are augmented with additional policy guidance from the Office of the Under Secretary of Defense for Policy to develop Theater Campaign Plans that describe how the Combatant Commander intends to conduct operations and activities – including shaping and influence programs – in support of national and DoD objectives , and DoD Guidance for Employment of the Force.[12]

The significant role of SC in the 21st century is related as much to the global information environment, characterized by many voices competing for the attention of virtually-connected publics worldwide, as it is to the increase in U.S. military activities worldwide. Within DoD, senior leaders recognize the importance and the mandate to integrate strategic communication with military strategies; experience shows that the DoD will not win our current conflict, or any future conflicts characterized within the irregular warfare umbrella, by kinetic means alone. In his Afghanistan assessment, General Stanley McChrystal, Commander, International Security Assistance Force and Commander U.S. Forces Afghanistan stated: "Many describe the conflict in Afghanistan as a war of ideas, which I believe to be true. However, this is a 'deeds-based' information environment where perceptions derive from actions. We will win by matching our actions with our words."[13]

Secretary of Defense Robert Gates, as well, believes a non-kinetic solution is vital. "Over the long term, we cannot kill or capture our way to victory….Non-military efforts – these tools of persuasion and inspiration – were indispensable to the outcome of the defining ideological struggle of the 20th century," he said. "I believe that they are just as indispensable in the 21st century – and maybe more so."[14]

The Defense Department must, additionally, synchronize its actions and communication with other members of the interagency community to support national objectives throughout the world, not just in our combat zones. The 2008 DSB Report on SC articulates this point:

> Strategic communication is essential to the successful use of all persuasive, cooperative, and coercive instruments of national power. It can amplify or diminish their effects. It is necessary long before, during, and after armed conflict. It can help prevent or limit conflict. It is central to the formulation and implementation of strategies, and it must be treated accordingly.[15]

Strategic Communication and DoD Organization and Responsibilities

Effective SC activities within DoD require an effective organizational structure that is capable of providing the needed vision, guidance, resources and leadership. Three major related areas comprise the SC organization within DoD today: Public Affairs (PA), Information Operations (IO), and Defense Support to Public Diplomacy (DSPD).[16]

Three different departmental directors within DoD have exclusive oversight of each these related functional responsibilities: Assistant Secretary of Defense for Public Affairs, Under Secretary of Defense for Policy, and the Under Secretary of Defense for Intelligence, USD (I). While each has a unique set of responsibilities and lines of coordination, those roles have evolved within and between the SC organizations in recent years.

The Assistant Secretary of Defense for Public Affairs, the ASD (PA), is the principal advisor to the Secretary of Defense for all communication activities including but not exclusively, public liaison, media relations, and public affairs. The department is the public face of DoD, and plans, coordinates, and executes media engagements, speeches, talking points, and other messaging for the Secretary, Deputy Secretary, and Office of the Secretary of Defense principals. Its staff plans, coordinates and approves DoD public affairs guidance for the services, combatant commands, and other DoD components.[17] The ASD (PA) also oversees the Office of the Deputy Assistant Secretary of Defense for Joint Communication. That office is primarily responsible for long-range SC communication planning and communication proponency within the joint force.[18]

The Under Secretary of Defense for Policy, the USD (P), is the principal advisor to the Secretary of Defense for all matters on the formulation of national security and defense policy and the integration and oversight of DoD policy and plans. In that role, the USD (P) is responsible for ensuring that strategic communication is integrated into policy decisions, and that the SC process is integrated into DoD long-term policy planning. This integration occurs through documents such as the National Defense Strategy, Guidance for Employment of the Force (GEF), and Combatant Command contingency plans.[19]

Within the Office of the USD (P) there was, until recently, a Deputy Assistant Secretary of Defense for Defense Support to Public Diplomacy. The Obama administration's new USD (P), Michele A.

Flournoy, disbanded the office due to reports indicating the office was providing guidance that did not meet DoD standards for accuracy and transparency.[20] The responsibilities for public diplomacy were transferred to regional offices with OUSD(P).[21] Similarly, oversight of psychological operations (PSYOP) activities was transferred to the Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities.[22]

Subsequently Ms. Flournoy created a new entity, the Global Strategic Engagement Team, to coordinate SC activities within USD (P). The December 2009 DoD Report on Strategic Communication to Congress explained the change:

> Experience proved, however, that a DASD-level office was not an effective means for ensuring high-level attention to improving policy-driven strategic communication, and in March 2009 that office was disestablished. Recognizing that effective strategic communication requires high-level advice and coordination, USD(P) appointed a senior advisor with responsibility for global strategic engagement within the OUSD(P) front office in April 2009, and shortly thereafter established the OUSD(P) Global Strategic Engagement Team (GSET). This team reports directly to USD(P) and is tasked with facilitating the strategic communication process within OUSD(P) and liaising with other DoD components as appropriate.[23]

The GSET, led by senior advisor Rosa Brooks, coordinates all SC activities within the OUSD (P). She also is the primary SC liaison between the OUSD (P) and the rest of the DoD SC enterprise. Additionally, she represents the OUSD (P) at SC interagency meetings, along with representatives from OASD (PA) and OUSD (I), and other elements as required.

The Under Secretary of Defense for Intelligence, or USD (I), is the principal advisor to the Secretary of Defense for Information Operations (IO). Information Operations is "the integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own.[24] The USD (I) exercises authority for IO (minus policy implications of the employment of PSYOP) in coordination with USD (P) and other OSD offices.[25]

Though not on the "policy" side of the DoD SC enterprise, and not part of the three key drivers of the DoD SC enterprise, the Joint Staff (JS) is still an important element. The JS coordinates SC related products and advises senior leaders on SC matters from a military perspective as well as providing guidance to the combatant commands and services. Key players include: the J-3 (Current Operations Directorate) with IO and PSYOP experts; the J-5 (Plans and Policy Directorate), with responsibility to coordinate and plan strategic guidance and participation in the DoD and interagency SC process; and the CJCS Public Affairs Office, which coordinates with OASD (PA) and communicates policy guidance to the Services and Combatant Commands.[26]

The three separate DoD departments that are key drivers within the SC enterprise lack a single vision and unity of effort. There is no overarching strategic leadership that sets strategic vision, sets priorities, allocates resources, or provides strategic guidance to ensure that DoD goals and objectives are achieved. As pointed out in the 2008 DSB Report on SC, "Strategic communication requires sustained senior leadership….These leaders must have authority as well as responsibility – authorities to establish priorities, assign operational responsibilities, transfer funds, and concur in senior personnel appointments."[27]

The 2009 DoD Report on SC communicates a contrasting position, however, championing coordination across disparate DoD organizations engaged in SC processes.

After struggling to define SC and develop effective coordination processes for much of the past decade, there is now substantial consensus within DoD about the value of viewing SC fundamentally as a process, rather than a collection of capabilities and activities. Conceptualizing SC as a process has allowed DoD to focus on ensuring effective coordination among DoD components, and to identify needed supporting capabilities, instead of designing and resourcing elaborate new structures and organizations.[28]

Strategic Communication Evolution in DoD

The past decade has indeed been a struggle to create and maintain the position that SC is a "process" across a large organization like the DoD. Developing an effective SC coordination process has been characterized by attempts to create an SC process, yet without true commitment and resources from senior DoD leadership. Nonetheless, DoD maintains the view that SC is a process that requires no changes, organizational or leadership, at this time.[29] Despite the emphasis on SC in the last decade, DOD has not produced an official directive or instruction on SC nor is there SC doctrine to educate and guide the DoD SC enterprise.[30]

In 2005, Rear Admiral Frank Thorp was assigned duties as the first Deputy Assistant Secretary of Defense for Joint Communication, DASD (JC), in an effort to shape department-wide communications doctrine, organization, and training for the joint force.[31] The DASD (JC) had two missions: to integrate communication including future communication planning within the DoD, and to act as the joint strategic communication proponent, helping to ensure that DoD communicators are properly organized, trained, and equipped to support the joint war fighter.[32] Soon after, the 2006 Quadrennial Defense Review (QDR) reflected the office's challenge:

> The QDR identified capability gaps in each of the primary supporting capabilities of Public Affairs, Defense Support to Public Diplomacy, Military Diplomacy and Information Operations, including Psychological Operations. To close those gaps, the Department will focus on properly organizing, training, equipping and resourcing the key communication capabilities.[33]

As a direct result of the QDR, the Strategic Communications Roadmap was developed to institutionalize SC across the Department. The first objective was to institutionalize a DoD process by which principles of SC are incorporated in the development of policy formulation, planning and execution. A second was to define roles, responsibilities and relationships, and develop doctrine for SC and its primary communication supporting capabilities: Public Affairs, aspects of Information Operations (principally PSYOP), Visual Information, and the DoD activities of Military Diplomacy and Defense Support to Public Diplomacy. A third priority was to properly resource Military Departments and combatant commands to organize, train, and equip DoD's primary communication supporting capabilities.[34]

On August 25, 2006, the Deputy Secretary of Defense established a Strategic Communication Integration Group (SCIG) and SC Secretariat under the DASD (JC).[35] These offices were tasked with ensuring that communication plans and concepts from the Office of the Secretary of Defense, the Joint Staff, the Combatant Commanders, and the Military Departments were coordinated and synchronized. A SCIG Executive Committee, or EXCOM, provided senior leadership for the Department's strategic communication initiatives, and direction and oversight of the SCIG. The EXCOM was co-chaired by the USD (P), ASD (PA), and the Director of the Joint Staff, but membership included senior representatives from the services and some of the combatant commands.[36]

The results of these efforts were by far the most aggressive that DoD had undertaken. Yet, they ultimately failed due to internal disputes and ultimately a lack of leadership. When the SCIG's charter was about to be renewed, the CJCS, Admiral Mullen, defended the renewal of the SCIG in a memorandum to the Deputy Secretary of Defense. Although the Chairman suggested renewal, he recommended midcourse corrections: Appoint an accountable leader, repurpose the SCIG, and restructure the EXCOM.[37]

Admiral Mullen clearly expressed the need for a single element to lead the SC effort and be central point of contact for SC within DoD. He clearly vocalized his frustrations with the SCIG and the EXCOM, and their inability to get the job done.[38] Certainly this was not lost on the Deputy and the Secretary of Defense when they deliberated and decided not to renew the charter, thus allowing the SCIG, and associated efforts – EXCOM, Secretariat, SC Roadmap, etc. – to expire on March 1, 2008.[39]

Assessing Effectiveness

For years, interested parties in and out of government have assessed the organization, processes and effectiveness of the DoD attempt to synchronize communication and gain ground in the information environment in order to help its war fighters win the nation's wars and support U.S. national goals. Those who recognize the significant role of SC have registered deep concern.

Ambassador Brian Carlson, the Department of State Liaison to DoD from 2006-2009, offered a unique "outsider" perspective on the current DoD SC structure, noting, "that an SC organizational transformation is necessary, that someone should be put in charge, that all elements of SC – DSPD, PA, IO minus the technical aspects of IO – should fall under an Under Secretary of Defense for Strategic Communication." That Under Secretary would then provide the strategic vision, guidance and specifically – the leadership that the DoD SC enterprise is currently lacking.[40]

The years of the George W. Bush Administration were marked by instances where departmental allegiance overrode the furthering of DoD SC capabilities. According to various sources, instances of turf battles between the departments occurred as new initiatives were coordinated or instituted, and attempts to slow down staffing actions to disrupt or directly halt initiatives occurred.[41] The disbandment of the Office of Strategic Influence (OSI) could be considered a clear example. Indications were that the ASD (PA) felt its territory was being infringed upon by the OSI, consequently, the ASD (PA) was alleged to have leaked information to the press with the intention of having the OSI disbanded. The Secretary of Defense felt intense pressure from the media, and ultimately dissolved the OSI.[42]

DoD's SC enterprise is still vulnerable to gridlock. Mr. Floyd described the current organizational arrangement as, "better than it ever has been, but still ineffective and personality-based without adequate leadership and direction." Floyd continued, "The way to long- term stability is an organizational transformation, with all elements of Strategic Communication falling under a single department and leader, an Under Secretary. We are all just playing nice; ultimately, someone has to be put in charge."[43] Ambassador Carlson echoed the assessment when he said, "Counting on everyone's goodwill is not a prescription for the long-term…you need to have someone who is in charge."[44]

Recently Mr. James Swartout, a political appointee, was selected as the Director of Joint Communication and runs the ODASD (JC). His office with a small staff of planners is the single area within DoD that does long-range SC planning, and is the joint SC proponent. The office has also has taken a more active role in the coordination of SC plans within the combatant commands, OSD, and the interagency community. The Afghanistan Strategic Communication Plan is a good example of effective DoD-wide SC planning. But issues remain.

Every Combatant Command has some sort of SC office or cell – all are staffed and operate differently. Some commands send SC plans to OSD through their J-5 Plans and Policy offices and some send them through their SC offices. The plans then reach either OUSD (P) or the ODASD (JC) for coordination. This then creates a situation where some plans may be coordinated in a timely manner, some may not. But ultimately they should be brought to the newly established Global Engagement Strategy Coordination Committee (GESCC) for departmental and possibly interagency coordination.[45]

The GESCC was established in June 2009 when the OUSD (P) and OASD (PA) re-missioned an informal information sharing body known as the Information Coordinating Committee (ICC). It expanded its membership and is evolving into the central body for facilitating the SC integrating process. This informal body meets bi-weekly to identify emerging issues, exchanges information on key issues, and facilitates information sharing and de-confliction of DoD communication activities.[46] The 2009 DOD Report to Congress states:

> The GESCC brings a more robust audience to coordinate DoD SC issues. The GESCC is co-chaired by OUSD(P) and OASD(PA), and brings together all of the key DoD offices mentioned above (OUSD(P), OASD(PA), OUSD(I), Joint Staff). Other regular GESCC attendees include representatives from the Office of the Assistant Secretary of Defense for Legislative Affairs and the Office of the Under Secretary of

> Defense for Acquisition, Technology & Logistics. Other DoD offices, including Combatant Command representatives, are invited to participate in GESCC meetings as appropriate, as are representatives of other USG agencies, such as the State Department, Open Source Center, the National Security Staff, and the National Counterterrorism Center. GESCC representatives participate in the NSC's regular interagency policy committee meetings on strategic communication and global engagement, and also work closely with the State Department's Global Strategic Engagement Center.[47]

Comparing the GESCC and the now-defunct SCIG, Mr. Floyd articulated the same crucial issue that Admiral Mullen had identified when recommending the renewal of the SCIG. "You need to appoint a leader."[48] When discussing how effectively GSECC conducts business, Mr. Floyd said:

> Though you have now have all the players around the table, business is still based on personalities, usually in an informal ad-hoc way…it's all personality-based and that, national security should not be based on some PDASD knowing some guy at State or a COCOM. It should be based on a formal process that is codified and with an organization chart that works and is not purely based on personalities…but, fully knowing that one of the best ways to get things done is through relationships that have been developed through common interests, training or exercises.[49]

Redundant, stove-piped representation from DoD departments and agencies with no singular leadership element complicates effective coordination between DoD and other federal agencies. Despite all the players at the table with the GESCC,[50] DoD tends to be over-represented in interagency coordination, since there is no single point of contact for all DoD SC-related issues. When an interagency SC meeting is held, all the major departments within DoD are present at the meeting as well. As Mr. James Swartout, Director of Joint Communication, commented, "At an SC interagency meeting, it is not uncommon for DoD to have twelve or so people in attendance." He believes this is because each department wants to know what is going on. He contends, "Other departments or agencies may have only one or two representatives each, and DoD is over represented."[51] Additionally, he states, "Because we have no single point of entry, and our informal process is based on personalities, it's frustrating sometimes because the National Security Council or DoS will go straight to certain people or the COCOMs, leaving us out, and we find out information after the fact."[52]

Strategic Communication and External Assessment of DoD Capabilities

The USG's and DOD's inability to communicate effectively with regard to Strategic Communication has been noted in numerous studies and reports. Dr. Christopher Paul, a social scientist and expert in SC at the RAND Corporation, produced a report titled, *Whither Strategic Communications? A survey of Current Proposals and Recommendations*. The survey reviews the recommendations and suggested improvements for SC and public diplomacy compiled from 36 selected documents and more than a dozen interviews with stakeholders and subject-matter experts on SC.[53]

The four common key themes were these: a call for leadership; demand for increased resources for SC and public diplomacy; a call for a clear definition of an overall strategy; and the need for better coordination and organizational changes (or additions).[54] These four common key themes apply as much to DoD as to the USG.

The 2006 and the 2010 QDRs both discuss the need to improve and strengthen the SC capabilities within DoD.[55] The 2006 QDR clearly states that, "Victory in the long war ultimately depends on strategic communication by the United States and its international partners."[56]

The DSB has also studied the subject of SC quite extensively; three major reports were released: 2001, 2004 and 2008. Their key lingering issues, some of which have been discussed already, are articulated in the DSB 2008 report:

> Nevertheless, the task force finds reasons for continued concern. Positive changes within organizations are real, but they depend to a considerable extent on the skills and imagination of current

> leaders. These changes must be evaluated, and those that work should be institutionalized. Resistance from traditional organizational cultures continues. Resources for strategic communication have increased, but they fall substantially short of national needs.
>
> This task force's primary concern is that fundamental transformation in strategic communication has not occurred at the strategic and interagency level.[57]

In the last few years, the realization that SC should be playing a pivotal role in bolstering U.S. image abroad, as well as being a key element to winning our current conflicts in Afghanistan and Iraq has become clear to Congress. In the National Defense Authorization Acts (NDAA) for fiscal years 2009 and 2010, Congress voiced concerns about current efforts, and have required the President as well as the DoD to compile reports on their SC efforts. For example, in section 1055 of the Duncan Hunter NDAA for FY 2009, PL110-417, Congress required the President of the United States to produce by December 31, 2009, a comprehensive interagency strategy for public diplomacy and SC with priority communication support to foreign policy objectives.[58]

This report, released in March 2010, broadly describes USG SC efforts as essential to sustaining global legitimacy and supporting our policy aims, that it's a shared responsibility across the USG, and how it has initiated an effort to review military programs that would be better conducted by other agencies and departments.[59] The report also reflects a significant change in responsibilities; the National Security Staff (NSS) is now described as having 'lead' for the interagency community for the "guiding and coordinating interagency deliberate communication and engagement efforts.[60] It reflects a new responsibility for the NSS – whereas the DoS had held that responsibility previously.

Another example of Congressional oversight of the DoD SC enterprise is in the NDAA for fiscal year 2010, PL 111-166. It states:

> Furthermore, the committee is concerned that the disestablishment of the office of the Deputy Assistant Secretary of Defense for Support to Public Diplomacy has left the Department of Defense without the necessary management

> structure to coordinate and guide effectively the myriad activities that comprise military public diplomacy. In order to craft an effective engagement strategy, the Department of Defense should understand all of the instruments at its disposal. The committee directs the Secretary of Defense to submit a report on the planning for, and execution of, military public diplomacy to the congressional defense committees within 120 days after the date of enactment of this Act.[61]

These Congressional requirements articulate that Congress is serious about their congressional oversight role of DoD, and the importance of SC. They obviously feel that a direction is needed and want the USG and DoD to move forward in developing an SC capacity. One could infer that Congress believes that USG and DoD efforts are either very superficial or, at the very least, ineffective.

Conclusion

The key issue is the absence of clear leadership and organizational harmony within the DoD SC enterprise. Leadership provides unity of effort and strategic vision, develops strategy, and fights for and allocates resources to the SC enterprise. SC efforts, both past and present, are a direct reflection of leadership and organizational ineffectiveness. Past efforts suffered from it, as evidenced by Admiral Mullen's recommendation to appoint an SC leader within DoD, and by DoD's report to Congress, noted above, that policy-driven SC requires high-level advice and coordination. Both acting Assistant Secretary Floyd and Ambassador Carlson draw on extensive experience in Strategic Communication when they recommended appointment of an Under Secretary of Defense for Strategic Communication to transform the organization. Further, Carlson further noted that there is no SC leader in DoD of a level equivalent to the Under Secretary of State for Public Diplomacy and Public Affairs, able to execute effective interagency coordination.[62]

In the fiscal year 2010 NDAA, referenced above, Congress expressed concern that DoD's management structure offers inadequate leadership to guide SC. Almost every major report and study on SC has four common themes: a call for leadership, demand for increased resources for strategic communication and public diplomacy, a call for a clear definition of an overall strategy, and the need for better coordination and organizational changes (or additions).

Recommendations for DoD Strategic Communication

Create a new Under Secretary of Defense for Strategic Communication – USD (SC). As an Under Secretary, USD (SC) would be of equal status with his/her SC/Public Diplomacy peers within the interagency community. The Under Secretary would provide the vital leadership needed, and represent and fight for DoD equities among federal agencies, as well as the National Security Council, on an equal footing.

Transform the DoD SC Enterprise so that all SC Elements Fall Under the Newly Established USD (SC). To be an effective organization, all elements of SC must be placed under the newly established USD (SC). That organization then would be led, resourced and staffed by an organization equal to its importance within DoD. The Under Secretary would have a Deputy Under Secretary and three Assistant Secretaries of Defense (ASD). Each ASD would each lead one of the three pillars of SC (PA, IO, and DSPD). There would be a few caveats: the USD (I) would keep all technical elements of IO; and the ASD (PA) would maintain his access and position as advisor to the Secretary of Defense for all matters relating to the media.

Consolidation of all elements would create a unity-of-effort organization. This organization would have a leader who would provide strategic vision and guidance, set goals and priorities, and would be able to fight for and then allocate resources to its elements. In essence, this SC organization would be a true hierarchical organization with leadership responsible for and authorized to direct and control all elements of SC in support of DoD and USG national interests. This would also end the participation of numerous DoD representatives in interagency SC related meetings; the OUSD (SC) would then have a single point of contact for interagency coordination.

When asked if he were king for a day and how he would fix the DoD SC problem, Mr. Floyd stated "Do what we discussed, create an Under Secretary, but being king for a day implies that it's not reality and looking at reality and ultimately the political will, the most you could hope for is having one element being put in charge as the lead."[63]

Adequate political will has not existed within the DoD, to date, to create an effective SC enterprise. That position is maintained in DoD's recent report to Congress recommending against any organizational change and the articulation that they continue to view SC as a process.

With all the Congressional interest being generated, Congress may gain enough momentum to act on its own and require a dramatic transformation to an effective DoD SC enterprise within DoD. Congress has exercised its influence before, when it created the United States Special Operations Command after DoD ignored numerous recommendations to do so. Only time will tell if Congress will be the proponent for more effective Strategic Communication enterprise within DoD and in support of the USG.

Section Two

Information Effects in the Cyberspace Domain

INTRODUCTION

Cynthia E. Ayers
NSA Visiting Professor of Information Superiority
Center for Strategic Leadership
U.S. Army War College

As nations of the world experience cyber threat and resort to high-technology weaponry at ever increasing levels, the U.S. military and intelligence community attempt to delve into theory, strategy, and lessons learned, while also wrestling with national policy, international law, and belligerents who fully understand U.S. limitations (to include moral and ethical limits placed on our forces). How do we engage? How do we respond? Do we act now and consider the consequences later? These are just a few of the plethora of questions raised in the continuing debate on regulating and planning cyber and other high-tech operations.

Colonel Richard G. Zoller's monograph (winner of the 2010 Secretary of Defense National Security Essay Competition) takes a hard look at the potential for cyberwar from the perspective of strategic cyberattack to the strategic planning needed by U.S. entities to counter a major cyber offensive. Recognizing that Russia may have already garnered success in cyberwarfare with the alleged attacks against Estonia and Georgia, he examines what this means to the United States and especially to the United States Military, given the subsequent kinetic attack by Russian forces against Georgia. What strategies (protect, defend, engage, etc.) should be considered? Where is the line drawn between being on the receiving end of a cyberevent that merely causes "inconvenience" and one that under other circumstances might be considered an act of war? Should cyberoffense always be met with cyberdefense, or are non-cyber kinetic and/or non-kinetic efforts preferable? What are the responsibilities of the United States to our allies in the onset of a cyberwar against them (singularly or collectively)? How would intermediaries act? Colonel Zoller further considers the anonymity that cyberattackers can maintain, as well as the potentially infinite nature of a cyberwar – especially one consisting of multiple "small" attacks and counterattacks. Defining the act of "winning" a war in cyberspace could be an extremely complicated – if not impossible – task. For that reason, Colonel Zoller raises the possibility of responding to cyberattacks with a non-cyber response such as sanctions, diplomacy, or even with conventional weapons. Regardless, Colonel Zoller ultimately argues that Russia's apparent incorporation of cyberattack into their strategic military planning indicates a need for the United States and allies to develop similar planning – as partners – to counter future adversarial cyber first-strikes such as those employed in the attacks on Estonia and Georgia.

Colonel Mary-Kate Leahy, in her own award-winning essay, looks at traditional "just war theory" and its application to the new high-tech battlefield. She considers whether unmanned systems (drones) linked to remote operators by virtue of cyberspace (and potentially incorporating artificial intelligence) challenge the assumption that war can continue to be waged on the same moral and ethical stance as the conventional wars of old. She takes into account differences inherent in current operations with regard to concepts of target discrimination, proportionality, responsibility, and legitimacy, concentrating on *jus in bello* or justice *in* war, as opposed to pre- (*jus ad bellum*) and post-war (*jus post bellum*). When one considers the outcry over the possibility of performing assassinations via drone attacks, as well as the insistence of legal and human rights organizations that these decisions are matters for international courts, this truly is a matter worthy of research and debate. Colonel Leahy makes an important case against "a scenario in which 'virtueless' war becomes the norm." Still, in a world where the non-state actors can access and utilize weaponry similar or equal to that of a nation-state, the rules are bound to change. Colonel Leahy argues that responsible nations should begin the process of rewriting them.

Colonel John R. Mahoney notes in his monograph that relevant legal authorities and policies are insufficient for effective computer network operations. He concentrates, however, on the lack of a unifying vision which provides for an efficient use of cyber operations within the defense arena. Colonel Mahoney explains that visualization begins with the establishment of what can and cannot be done within the bounds of a cyberwar. Additionally, a thorough understanding of enemy intent and capabilities is necessary to achieve successful engagement.

He concludes that the current focus is on strategic cyberwar – to the detriment of the actual operations. Colonel Mahoney further maintains that U.S. entities have concentrated on cyber defense and deterrence, leaving forces ill-equipped and ill-advised in the conduct of cyber response. He sees hope, however, in the establishment of United States Cyber Command (USCYBERCOM), including the expansion of the role of Signals Intelligence (SIGINT) within cyberspace operations; yet Colonel Mahoney warns against a continuing focus on the strategic while leaving the operational aspects of cyberwar to flounder.

Mr. Paul Matus, in his award-winning paper (winner of the 2010 Commandant's Award for Distinction in Research) takes the need for consideration of cyberwarfare further, examining the strategic impact of cyberwarfare rules, laws, and regulations on the conduct of counterattack and conventional response. Mr. Matus notes that there are differences of opinion as to the damage that a cyberwar could do, but acknowledges that vast economic as well as destructive damage could result from a well-planned and executed attack by a nation-state such as North Korea, Iran, China and/or Russia. Indeed, he comments that China's cyber doctrine of "global electronic dominance" states the need to take down critical infrastructure (to include communications and the electric grid) prior to the application of conventional force. But applying definitions prescribed by law for a more conventional force-on-force application to the often ambiguous circumstances that usually surround a cyberattack seems only to end in confusion. Although such laws may legitimately prevent large-scale war stemming from a cyber attack waged by a single teenage hacker, they may also prevent a response to non-state belligerents acting in concert and performing substantial offensive maneuvers – especially considering that there may be no cyber equivalent of "use-of-force" or "invasion of territory" in play. Discussions regarding the establishment of international laws or rules of engagement in the cyber realm have only added to the confusion and increased the number of seemingly unanswerable questions. Mr. Matus, however, clearly explains the implications to United States national security, and recommends multilateral participation in the development of rules to prevent cyber belligerents and adversarial nations from engaging in cyberwarfare – even if in the end, clarification through dialogue is the only outcome.

These four authors question the readiness of the United States to conduct cyber and high-tech operations because the theoretical, legal, and regulatory groundwork is not yet sufficient to support success in the cyberspace arena. They present leadership with recommendations and opportunities to excel – to create the means necessary to engage the enemy on any battlefield, any time. In the cyber realm, to a large extent, the United States is already behind the curve. Due to new high-tech capabilities, we may be floundering in regard to ethics and human rights issues. If answers to the questions raised in these papers are not found soon, the people of our nation may pay a heavy price.

Russian Cyberspace Strategy and a Proposed U.S. Response

Colonel Richard G. Zoller
United States Army

> *The numerous cyber attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyberspace high on the list of novel security threats. The acknowledgment that such attacks pose a threat to international security reached new heights in 2007 owing to the first-ever coordinated cyber attack against an entire country – Estonia – and also because of large-scale cyber attacks against information systems in many other countries as well.*
>
> —Estonian Cyber Security Strategy[1]

As inferred from the statement above, cyberattacks[2] have become a part of military strategy. Countries such as China have been exploiting cyberspace for years to engage in computer espionage and have exfiltrated enormous amounts of sensitive information. Going a giant step further, Russia has made cyberspace attack a major factor in its military strategy to coerce "near abroad"[3] nations to align with Russian national interests. As recently as January 2009, Kyrgyzstan, one of the Russian "near abroad" nations, was the latest to suffer from cyberattacks by computers located in Russia.[4] This paper analyzes two cases of Russian cyberattacks and recommends a United States strategy to counter the Russian strategy.

Background

To understand and develop a United States' strategy to counter Russian cyberstrategy, the author must define terms regarding cyberspace. Cyberspace has been defined in many different ways. For the sake of consistency, this paper uses the Department of Defense (DoD) definition. A Deputy Secretary of Defense memorandum defines 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."[5] A later DoD memorandum further defines cyberspace as "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in and through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[6] DoD subdivided cyberspace operations into two main components, Computer Network Operations (CNO) and Network Operations (NETOPS). CNO is further subdivided into Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defense (CND). Joint Publication 1-02 (JP 1-02) defines CNA as, "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[7] JP 1-02 defines CNE as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[8] CNE is fundamentally different from CNA. CNE is more comparable to spying, whereas CNA focuses on disruption or corruption of an adversary's systems or networks.[9] JP 1-02 defines CND as, "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks."[10]

Two other terms which are extremely relevant to any discussion of cyberstrategy are deterrence, in general, and cyberdeterrence, in particular. JP 1-02 defines deterrence as "the prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[11] In RAND's monograph, "Cyberdeterrence and Cyberwar," the author chose to define cyberdeterrence as "deterrence in kind to test the proposition that the United States…needs to develop a capability in cyberspace to do unto others what others may want to do unto us."[12]

The Estonia Case

In April 2007, the small Baltic state of Estonia received an unprecedented cyberattack. The Estonians relocated a Russian war memorial, the Bronze Soldier, from Tallinn to a military cemetery, which outraged Estonia's Russian-speaking citizens, leading to two days of rioting.[13] Throughout April and early May 2007, Estonia was the victim of clearly coordinated cyberattacks against its social, political and financial institutions.[14] Key Estonian web sites were flooded with Distributed Denial of Service attacks (DDOS) that effectively shut them down. Additionally, hackers attacked key government web pages using botnets (short for Internet Robot Networks) to take control of computers.[15] Estonia is a small country but it is extremely Internet dependent and conducts much of its business in cyberspace. Also, hundreds of thousands of Estonians work outside the country and use cyberspace to wire money back to their families.[16] Estonia conducts an astonishing 98 percent of its banking online and when the DDOS attacks disconnected its two largest banks for hours, the impact was nearly paralyzing.[17] Many argued that the source of the attacks cannot be conclusively traced to the Russian government or military but Estonia has insisted that the attacks represented the culmination of Russia's year long plan to attack the Estonian government for their anti-Russian policies.[18]

Because the attacks used botnets, the cyberattacks cannot be conclusively attributed to the Russian government. Hackers use botnets to control computers remotely by loading them with rogue software, usually without the knowledge of the computer owner. The computers, once hijacked using botnets, sent thousands of messages per minute to Estonian servers, causing them to crash.[19] One such attack against an Estonian Internet Service Provider disrupted Estonian "government communications for at least a 'short' period of time."[20] Because it is difficult to trace the origination of the botnets, it proves neither Russian guilt nor innocence. As will be discussed later, attribution is one of most difficult aspects of cyberwar. It is possible that Russia could have used government agents to "incite patriotic Russian hackers, of which, there are plenty, as well as cybercriminals to attack Estonian targets."[21] Because the hackers coordinated the cyberattacks with organized violent demonstrations in Tallinn among Russians and in Moscow against the Estonian embassy, it seems evident that Moscow sanctioned the computer attacks "and reflected a coordinated strategy devised in advance of the removal of the Bronze Soldier from its original pedestal."[22]

Because of Estonia's dependence on cyberspace in all facets of life, they were particularly vulnerable to a cyberattack but also better prepared to respond. In the immediate aftermath of the attacks, Estonia took the matter to the North Atlantic Treaty Organization (NATO) of which it has been a member since 2004.[23] Estonian's Defense Minister Jaak Aaviksoo said, "the cyberattacks were a threat to Estonia's national security and likened their effect to a blockade of a country's sea ports."[24] Although Estonia asked for NATO's help in responding, a senior civilian NATO official said, "Estonia's response…was so effective as to preclude the need for drastic NATO action" and "NATO experts summoned by Estonia during the weeks of the attacks had learned at least as much as they had contributed in terms of advice."[25] In fact because of Estonia's leadership in cyberspace, seven NATO nations signed the documents to establish a Cooperative Cyber Defence (CCD) Centre of Excellence (COE) in Tallinn, Estonia.[26]

The Georgia Case

As with Estonia, Georgia suffered a similar cyberattack during its conflict with Russia in 2008. On August 8, 2008, just as Russian troops were moving into South Ossetia to defend the so called Russian compatriots, "a multi-faceted cyber-attack began against the Georgian infrastructure and key government web sites."[27] Again, the attacks included web defacement, and DDOS attacks but also included "Web-based Psychological Operations" and a "fierce propaganda campaign."[28] In addition to hacking hundreds of Georgian government and news sites, the attackers hacked the Georgian parliament site and replaced content with images comparing Georgian President Saakashvili to Adolf Hitler. The attackers were able to disrupt President Saakashvili's telephonic interview with CNN.[29] In their report, the United States Cyber Consequences Unit (U.S. CCU) stated that "signs of advance preparation and planning, suggests that cyber attacks against Georgia had been on the Russian agenda for some time."[30] According to the Benton Foundation, "the leading suspect behind the attacks, which disabled key government Web sites, is a cybercriminal organization known as the Russian Business Network."[31] As Marcus H. Sachs, Director of the SANS Internet Storm center states, "RBN is a virtual safe house for Russian criminals responsible for malicious code attacks, phishing attacks, child pornography and other illicit operations."[32] Though it is not clear what precisely is the nature of the interaction between the Russian government and those who executed the attacks, it does seem that it is likely to become part of Russia's standard operating procedure henceforth to use cyberspace as part of an integrated strategy to coerce its "near abroad" nations.[33]

Again, because of the ability to remain anonymous in cyberspace it is difficult to attribute the attacks directly back to the Russian government. However, according to "Internet technical experts, it was the first time a known cyberattack had coincided with a shooting war,"[34] leading to the possible conclusion that the Russian government was behind the attacks. Of course, the Georgians accused the Russians who in turn denied any responsibility.[35] A metaphor "wilderness of mirrors" describing intelligence agencies is appropriate for cyberwar and depicts what happened in Georgia during the attack.[36] Because Georgia does not rely as heavily on cyberspace, the attacks had far less immediate impact than it did in Estonia "where vital services like transportation, power and banking are tied to the Internet."[37]

Russia's Cyberspace Strategy

The two cases described above should lead one to believe that Russia has integrated cyberspace as part of an overall military strategy. Although there is an absence of any formal charges within the international community against Russia, their complicity in the cyberattacks remains uncertain. Russia first used the term cyber in April 2008 when the Deputy Director of the Department of Information Society Strategy, Vladimir Vasilyev, used the term several times in charts explaining President Vladimir Putin's document, "The Strategy of Information Society Development in Russia."[38] In fact, Russia, like China prefers to use the term "informationization" and recognizes that “informationization” highly influences the means and methods of conducting war.[39]

When one analyzes the cyberattacks against both Estonia and Georgia, it is easy to recognize that the cyberattacks were not an end in themselves but part of an integrated strategy. As Kenneth Geers, the United States representative to the Cooperative Cyber Defense, Center of Excellence states in his article, *Cyberspace and the changing nature of warfare*, “practically everything that happens in the real world is mirrored in cyberspace”[40] and that “strategists must be aware that part of every political and military conflict will take place on the internet.”[41] More than any other nation-state, Russia uses the cognitive domain of cyber as much as the technical domain.[42] Where Western definitions of cyberspace focus on technical aspects of information technology, “informationization” takes on a much broader definition. “Informationization” can be broadly defined as, applying modern information technologies into all fields of both social and economic development, including intensive exploitation and a broad use of information resources.[43] What this means is that Russia uses cyberspace more to disrupt an adversary’s information than to steal or destroy it. The cases above described the disruption of information flow. While attackers defaced web pages and temporarily shut down cyberspace services in both Estonia and Georgia, there was no permanent damage. The attacks, especially against Georgia, demonstrate a key component of the Russian’s cyberspace strategy of coercion. As John Bumgarner, a former cyber security expert for the CIA and other U.S. intelligence agencies told reporter Steve LeVine, “they [the attackers] didn’t attempt to cripple sites that could have caused chaos or injury, such as those linked to power stations or oil-delivery facilities, but merely those that could trigger comparative ‘inconvenience.’”[44]

Timothy L. Thomas, a senior analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas explains in his chapter, “Nation-state Cyber Strategies from China and Russia,” the “targets of disorganization are not only weapons and decision-makers on the field of battle but also in the mind of average citizens.”[45]

Possible Cyber Strategies

In the December 2008 report, "Securing Cyberspace for the 44th Presidency," the Center for Strategic and International Studies commission spelled out three major findings. First, "cyberspace is now a national security problem for the United States."[46] Second, "decisions and actions must protect privacy and civil liberties."[47] Finally, and most importantly, "only a comprehensive national security strategy that embraces both the domestic and *international* (emphasis added) aspects of cybersecurity will make us more secure."[48] In the 2009-2010 Chairman of the Joint Chief of Staff's guidance, Admiral Michael Mullen states that "we must put more resources – intellectual, money and people – into accelerating development of our cyber capabilities and integrating them into our daily operations."[49] In dealing with Russia in cyberspace, the U.S. must not only protect and defend American interests but also those of our allies, which include Russian "near abroad" nations. In the case of Estonia, international interest was high when that country asked for a reinterpretation of NATO's Article 5, which states that "an armed attack against one (member)… shall be considered an attack against them all."[50] Although not invoked after the attacks on Estonia, NATO could deem future cyberattacks damaging enough to U.S. and NATO security interests to result in invocation of Article 5.

The United States has multiple strategic options in dealing with cyberattack by Russia either directed against the United States or its allies. First, the United States can continue to rely on a reactive defensive posture using routers, firewalls, intrusion detection systems (IDS) and anti-virus programs to defend cyberspace and not engage in cyberattack or exploitation. This strategy would require the United States not only to defend its own cyberspace but to assist other nations in defending theirs. The second option is to continue cyberdefense but also engage in a strategy of cyberdeterrence using both cyber exploitation and active cyberattack. A third option is a strategy to continue to conduct cyberdefense and cyber exploitation but use non-cyberattack (kinetic and non-kinetic) deterrence options. The strategy selected should be one that best postures the United States to prevent, reduce vulnerability to, and minimize damage and recovery time from, cyberattacks against its own national interests and Russian "near abroad" states.

A policy of "defense only" sends a strategic message to the Russians that a cyberattack on a particular portion of cyberspace that is a national interest to the United States is an act of war. This, in and of itself, creates disincentives for Russia to start hostile action in cyberspace, i.e., it provides deterrence. Any "defense only" posture must anticipate future attacks.[51] To rely on a "defense only" policy, the U.S. Government (USG) would have to protect critical cyber infrastructure and "become adept at predicting the type, time and location of the next"[52] inevitable cyberattack. To accomplish the latter, the United States and its allies would have to establish national and international watch-and-warning networks to detect and prevent cyberattacks as they emerge. Then the United States could successfully respond to an attack and minimize damage and significantly reduce recovery time.

The option to continue cyberdefense but also engage in a policy of cyberdeterrence using both cyber exploitation and active cyberattack certainly legitimizes cyberattack and sends a strategic message to Russia and other potential adversaries that cyberattack is an acceptable act. There are two strong arguments against engaging in cyberattack. First, cyberattacks travel over civilian networks. Second, the owners/operators of those networks can, at least at some point, identify data as cyberattack traffic, as opposed to the normal traffic they usually carry. Therefore, the civilians who own and operate the constituent networks that create cyberspace can, in effect, exercise a veto over cyberspace operations.[53] The owners and operators of civilian networks could exercise their ability to prevent the attacked state from launching retaliatory cyberattacks and to stop the attacking state from launching further offensive cyberattacks. In this scenario, the cyberspace owners and operators are essentially neutral.[54] There is another, more dangerous scenario; the private owners of the network could choose to intervene. They could allow the traffic of the attacking state's cyberattacks and prevent the defending state from counterattacking. [55]

There is another strong argument against using cyberattack. True "conventional" warfare poses two adversaries head-to-head to achieve decisive battle, but attacks in cyberspace are essentially anonymous and at best, difficult to attribute to the attacker.[56] Cyberspace data move across the world in milliseconds. What's more, code sent by an attacker can traverse numerous countries, and those countries could refuse to pass on the information they have to investigators. Attacking nation-states can easily use the anonymity of cyberspace in their favor.

Many experts say that cyber is the new global commons.[57] While that may be true, one must be careful in making such close comparisons to the air, land, and sea. When thinking about cyberattack, a better comparison may be with the use of biological weapons. Although U.S. adversaries may develop and consider using biological weapons, the USG would not consider responding in kind. The thought of the United States unleashing a biological weapon is unthinkable. Once released, the United States or its allies could not be certain how the weapon would spread. This is comparable to the effect of releasing a cyberattack. Although the United States may target a particular system in cyberspace, there is no guarantee that the attack may not spread beyond the original target, possibly spreading to an ally's infrastructure, or even worse, back to the United States' infrastructure. Richard Kugler, a former Distinguished Research Professor in the Center for Technology and National Security Policy at the National Defense University argues that a United States, "cyber deterrence strategy has not been articulated and released, at least publicly."[58] This fact could easily lead one to believe that the United States does not want to have an explicit cyberdeterrence strategy due to the political and diplomatic problems of endorsing a cyberattack capability.

A strategy of continuing to conduct cyberdefense and cyber exploitation while using non-cyberattack (kinetic and non-kinetic) deterrence options sends a strategic message to Russia and other potential cyber adversaries that cyberattack is unacceptable and is considered an act of war when directed against a U.S. national interest. Again, considering the analogy given with biological weapons given above, responding to a cyberattack with non-cyberattack response options is reasonable. If the United States can determine that Russia has committed a cyberattack against an American interest (to include U.S. allies in the Russian "near abroad") it can consider that event as an act of war and that it would have the endorsement of the international authority to respond to the attack. The response could range from responding with sanctions to kinetic attack to ensure Russia cannot continue the attack. Stating that the United States would respond this way would also provide a deterrent to the Russians and other potential cyber adversaries. Washington could also continue to exploit cyberspace. This would allow the United States to conduct forensics of cyberattacks to determine their origins, allowing it to carry out flexible response options against the aggressive state actor.

Evaluation of a United States Cyberstrategy

While each of the three potential strategies examined above depend heavily on cyberdefense as a foundation, they differ significantly in their ability to deter Russia and other potential adversaries from attacking United States national interests in cyberspace. All differ in the ability to deter a cyberattack. Deterrence has two components, both which are intended to dissuade an attack.[59] The proposed strategy of cyberdefense only, has the component of deterrence by denial. Deterrence by denial is to deny the ability of an adversary to attain successfully their political goal of a cyberattack. Because all cyberattacks exploit vulnerabilities in cyberspace, if all vulnerabilities could be eliminated an adversary would be deterred by knowing that they could not successfully attack a state interest. The next two proposed strategies rely on deterrence by punishment.[60] Punishment can be through a retaliatory cyberattack (as in the second proposed strategy) or retaliation through other kinetic or non-kinetic means (as proposed in the final strategy). Deterrence by denial and deterrence by punishment can work in tandem, thus each of the three strategies has cyberdefense as its foundation.

Cyberspace is a complex set of protocols and underlying technologies which ensure users could *share* information, not to ensure *security* for the information. Therefore, in practice all cyberspace systems are vulnerable.[61] Potentially the gravest threat in cyberspace today is the abysmal state of security of so many of the systems connected to it. Many factors contribute to the problem, including commercial off-the-shelf software, in which many of the desired features and rapid time to get on the market outweigh an underlying security design.[62] It would be naïve to believe that all cyberspace vulnerabilities could be found and eliminated. Instead of ensuring the detection and elimination of all vulnerabilities, some argue that the ability to respond to an attack and restore operations is more important. In the 2003 *National Security Strategy to Secure Cyberspace*, the Bush administration noted that, "the first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events...and to improve the international management of and response to such attacks."[63] In the cases of attacks on Estonia and Georgia, both were able to recover from the attacks in a reasonable amount of time and without permanent damage to any infrastructure.

If cyberdefense alone is not enough to deter Russia, there are two other possible responses to a cyberattack against the United States or an ally. The United States could employ cyberattack capabilities for a retaliatory strike on the networks of Russia or it could "maximize deterrence by applying a full set of other mechanisms – political, diplomatic, economic and military."[64] This is the significant difference between the proposed second and third strategies. Does the United States retaliate with cyberattack or with other kinetic or non-kinetic effects? According to Kugler, "these other instruments may be more potent than cyber retaliation."[65] This may be especially true with Russia, which focuses its capabilities on the cognitive domain of cyberspace. Russia has shown that it is much more willing to coerce its "near abroad" states by denying and disrupting their capabilities to operate in cyberspace rather than destruction of their information or infrastructure. As Thomas explains, the Russian effort "is aimed as much at disrupting an adversary's information as it is at obtaining information supremacy."[66]

Recommendations for a United States Cyberstrategy

The goal of any United States strategy in cyberspace designed to meet the challenges of Russia's cyberstrategy should be to influence them not to launch cyberattacks against the United States or its allies. While there is no substantive evidence that Russia has launched a cyberattack directly against the United States, the case studies examined above indicates that they will either directly or indirectly use cyberattack as part of their integrated strategy to coerce their "near abroad" states. As detailed in the U.S.-CCU report, "it would be very surprising if future disputes and conflicts involving Russia and its former possessions or satellites weren't accompanied by cyber campaigns."[67] The United States and international partners must develop a strategy to counter Russian political motives.

Based on this analysis, the recommended foundational cyberspace strategy for the United States should be to continue to conduct cyberdefense and cyber exploitation but use non-cyberattack (kinetic and non-kinetic) deterrence options. As stated earlier, by not condoning cyberattack, it sends a strategic message to Russia and other potential cyber adversaries that cyberattack is unacceptable and is considered an act of war when directed against a United States national interest. To support this foundational strategy, the USG should implement the following supporting strategic and operational recommendations.

First, at the strategic level, the President of the United States should have an explicit policy that the United States will not conduct cyberattacks and will use all other instruments of national power such as diplomatic, economic and even military to deter or retaliate against cyberattacks directed at America or its allies. This statement should send a clear message to Russia and other potential cyber adversaries that the United States will not tolerate states which conduct cyberattack or knowingly and deliberately harbor cyberattackers and shield them from criminal enforcement. As Kugler states, "a good place to present it would be in the next National Security Strategy."[68]

Second, the USG should work with international partners to build alliances in cyberspace. Working through the United Nations, NATO or even bilaterally for cyber security collaboration, may convince Russia or other potential cyberattackers, "that their efforts, while tactically sound, are strategically counterproductive."[69] The cyberattack on Georgia provides an excellent example of producing an undesired strategic effect. Initially, Georgia attempted to thwart the cyberattacks by blocking Russian Internet Protocol addresses. This response failed when the hackers circumvented the blocks by using foreign servers to stage further attacks.[70] In an unorthodox move, Georgia relocated it cyberspace services to websites in Estonia and within the United States. By relocating services, the Georgian's could filter out the attack traffic and had greater bandwidth to handle the DDOS data.[71] Georgia literally "asymmetrically moved around the attack."[72] International partners should formalize these types of agreements to prepare before a crisis. As the U.S.-CCU report stated, "although the amount of talent the Georgians were able to involve informally was impressive, it is noteworthy that there was no international organization they could contact for help."[73]

Third, the USG needs to build a strategic partnership with private industry and academia. As recommended in *Securing Cyberspace for the 44th Presidency,* "government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated and preventative response activities."[74] This partnership should also include academia and both public and private sector individuals from partner nations. Cyberspace is a global domain which makes vulnerability, anywhere, a vulnerability to the entire network. While the government has authorities to conduct operations in cyberspace, private companies own most of the infrastructure. By bringing the best and brightest from each sector, the United States could reduce the vulnerabilities across cyberspace making it less likely that a cyberattack could be successful. To implement this recommendation, the USG needs to grant the required level of security clearances to individuals in both private industry and academia. Too often the private sector and academicians can't gain the same access as certain government agencies that work cyberspace efforts and this significantly hinders progress in cybersecurity

Finally, the United States should lead the international community to develop a secure cyberspace architecture. As stated earlier, the current architecture was founded on the ability to share information, not to secure it. Although this would take many years to accomplish and would be a huge undertaking, intense efforts should begin now rather than later. This is an area where collaboration between academia, government, private sector and the international community could result in a reliable and robust cyberspace that is less susceptible to cyberattack.

At the operational level, the United States is already moving in the right direction. The establishment of United States Cyber Command

(USCYBERCOM) as a sub-unified command under United States Strategic Command will at least unify efforts in the military's portion of cyberspace. Although this paper has previously recommended not conducting cyberattack, USCYBERCOM should nonetheless study and develop cyberattack capabilities. At first this may seem contradictory. Why study and develop offensive cyberattack capabilities if you explicitly state that you will not use them? First, to defeat a cyberattack, one needs to understand how the attack is occurring. Second, to defend cyberspace, "the military needs to develop a robust modeling and simulation architecture for proactive cybersecurity."[75] By modeling cyberspace, trained military "cyber warriors" can simulate attacks on the network, therefore discovering vulnerabilities before an adversary can use them to attack the network. One cautionary recommendation for USCYBERCOM is that with limited resources, they should not focus on cyberattack at the expense of cyberdefense. As the RAND report concludes, "it is thus hard to argue that the ability to wage strategic cyberwar should be a priority area for U.S. investment."[76]

Conclusions

Whether actually proven to be complicit in the cyberattacks on Estonia and Georgia, it seems evident that Russia does indeed have a cyberstrategy. As Thomas concludes in his chapter on *Nation-state Strategies*, "developments…indicate that Russia's cyber and information strategy deserve examination for the direction they are headed and for basic content."[77] It would appear from the case studies examined here that the Russian strategy is to continue to intimidate and coerce its "near abroad" states with cyberattack. If the United States is to continue to be the champion of spreading democracy across the globe and supporting developing democracies, it is imperative that it not ignore the cyber strategies that other nation-states are using to enforce their political will on their neighbors. Estonia, Georgia and other Russian "near abroad" states look to the United States to support their democratic development. Therefore the United States should implement the recommendations outlined above to deter Russia from using cyberspace to coerce its neighboring states.

Because of the ubiquity of cyberspace, no nation will be able to act alone in dominating this new commons. The United States must work in concert with industry, academia and international partners to exploit and defend cyberspace to protect its national interest and the interest of its allies and partners. The USG should integrate cyberspace operations into all future strategies – the advantage of dominating cyberspace is obvious. While cyberspace strategies and tactics favor nations with robust information technology, the Internet is an extraordinary tool for a weaker state to attack a stronger conventional foe.[78] As President Obama stated on May 29, 2009, in his remarks on securing the nation's cyber infrastructure, "this status quo is no longer acceptable – not when there's so much at stake. We can and we must do better."[79]

Prudens Futuri

Keeping Up with the Drones: Is Just War Theory Obsolete?

Colonel Mary-Kate Leahy
United States Army

> *If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner.*
>
> —General Omar N. Bradley[1]

In 2007, the U.S. military spent $880 million to purchase unmanned aircraft systems (UAS). The Air Force reported Predators and Reapers, the most predominant components of the United States' UAS arsenal, attacked targets in 244 of 10,949 missions in Iraq and Afghanistan in 2007 and 2008, or about 2.2% of the time.[2] In April 2009, in a speech at the U.S Air Force's Air War College, Defense Secretary Robert Gates stated there had been a 48% increase in UAS patrols in combat zones in the preceding year.[3] The Defense Department's Fiscal Year 2010 combined allotment for development and procurement of UAS is more than $4.2 billion.[4] UAS have become so central to U.S. efforts in Pakistan and Afghanistan that some observers have dubbed this front of the war on terror "the drone war." UAS technology which transmits images and information via satellite to distant command centers enables U.S. forces to attack targets within minutes rather than days. UAS are today considered a "must have" capability by military commanders in Iraq and Afghanistan, and the acquisition rate for these systems and the development of force structure to man them is accelerating rapidly based on demands from the field.

The employment of UAS occurs within the context of a rich tradition of Judeo-Christian principles, international laws, and treaties. The "just war tradition," which is the foundation for the existing body of international laws governing the conduct of war is as old as warfare itself. The earliest records of collective fighting indicate that some moral considerations were used by warriors to limit the outbreak of unjustified war and to reduce the devastation and destruction which have historically been the inevitable by-products of conflict.[5] Over time, just war theory has evolved into a coherent set of concepts and principles which enable moral judgments in times of war. These values and concepts have made their way into binding treaties regulating the conduct of states during periods of war. The treaties regarding the conduct of war are collectively referred to as the "laws of armed conflict" or "laws of war."[6]

The introduction of unmanned aircraft systems to the battlefield raises new questions about the validity and modern day relevance of both just war theory and the laws of armed conflict. Have technological advances rendered the principles of just war theory obsolete? Is development of a replacement theory in order? Are there dangerous consequences in the offing if a discussion of these questions is deferred? This new way of waging war, with robotics and unmanned aircraft systems, has the potential to change the definition of who is considered a "combatant" versus a "non-combatant," and who therefore constitutes a legitimate military target. This distinction is at the very core of just war theory.

This paper includes an examination of the origins of just war theory as the basis for commonly agreed laws of land warfare, looks in depth at the *jus in bello* tenet of just war theory, and examines how unmanned aircraft systems challenge the long standing laws of war. The changes in combatants' proximity to the battlefield, the role of decision-making, and the responsibility for errors which new military robotic technology bring to the fore mandate that responsible nations grapple with the implications of employing these weapons systems, and come to agreement on how wars of the future will be morally and ethically waged. Failure to address the gaps this new technology exposes in traditional teachings will have profound implications for Soldiers, political leaders, and the population at large in the years ahead.

On January 13, 2010, the American Civil Liberties Union (ACLU), under the provisions of the Freedom of Information Act (FOIA), asked the U.S. government to disclose the legal basis for the use of UAS to conduct "targeted killings" overseas. The ACLU request asked when, where and against whom UAS strikes can be authorized, and how the U.S. ensures compliance with international laws related to extrajudicial killings.[7] The employment of UAS has increased during the Obama Administration. In March 2010, for the first time the Administration laid out its legal rationale for the use of "drone strikes" in Afghanistan, Yemen, Somalia and Pakistan.[8] The spokesman for the Administration, State Department lawyer Harold Koh, argued the U.S. policy on the employment of UAS takes into account the just war principles of "distinction," (also known as discrimination), in that attacks are aimed at lawful enemy combatants and not civilians; as well as the principle of "proportionality," which prohibits attacks that may be expected to cause excessive damage in relation to their anticipated military advantage.[9] Koh's defense of the Administration's use of UAS was based on compliance with select tenets of just war theory and has been criticized by numerous scholars. Mary Ellen O'Connell, professor of law at Notre Dame, indicated it's "stretching beyond what the law permits for this very extreme action of killing another person without warning – without a basis of near necessity simply because of their status as a member of al-Qaida or a related group."[10] Similarly, the United Nation's chief on Extrajudicial Executions has said "the drone strikes violate international law."[11] The current debate among ACLU members, Obama administration officials, and scholars in the fields of ethics and law is indicative of the tension that has developed because of friction between traditional just war theory and the application of modern military technologies.

In a March 2010 interview, Dyke Weatherington, deputy for the unmanned aerial vehicle planning task force office at the Department of Defense (DoD) said, "it is difficult to find any other technology in the DoD that in a single decade has made such a tremendous impact on the warfighting capability of the department."[12] Today the U.S. leads the world in the development, acquisition and employment of UAS; UAS have become a fundamental component of how we wage war. The U.S. therefore has a responsibility as the global leader in this area to lead the discussion on how the employment of this technology challenges and potentially changes traditional just war theory which has governed the practice of armed conflict for centuries. This topic is of strategic importance not only to the United States but also to the broader global community because it is central to how wars of the future will be prosecuted.

What are Unmanned Aircraft Systems and Why Does the U.S. Military Love Them?

The majority of the military robots which exist today are UAS, also known as "drones." UAS are remotely-controlled, uninhabited aircraft used to support Intelligence, Surveillance and Reconnaissance (ISR); some UAS carry missiles and are used as a weapons platform. It's estimated today there are over 7,000 UAS of various types in the U.S. arsenal. Within NATO, there are more than sixty operational models of aircraft, and more than 2,200 ground control stations.[13] The most famous U.S. UAS, Predators and Reapers, are often piloted by operators located on U.S. military installations in Nevada and Arizona, on the other side of the world from the location of their targets.[14]

The method used to operate UAS in this manner is called reach-back or remote-split operations, meaning the systems are flying in the war zone while the pilot and sensor operators are physically located thousands of miles away, connected to the system via a satellite communications link.[15] The link of the sensors with their extended flight times means an unmanned aircraft system can fly in excess of 3,000 miles, spend 24 hours mapping out a target area of approximately 3,000 square miles, and then fly 3,000 miles back to its home base.[16]

In his widely acclaimed book, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, P.W. Singer documents the rapid increase in UAS employment since the start of the Iraq War. He recounts that when U.S. forces initially entered Iraq, there were no robotic systems on the ground during the original invasion. By the end of 2004, there were 150 such systems in place. This number increased dramatically in succeeding years – growing from 2400 in 2005, to 5000 in 2006, and reaching 12,000 by the end of 2008.[17]

UAS have two great advantages: they are much cheaper to fly than conventional planes, and they keep pilots and Soldiers out of harm's way.[18] As Singer explains, "unmanned systems are used for the jobs that meet the three D's: dull, dirty, or dangerous…as a commander of one of these units told Singer, he likes them because he doesn't have to worry about writing a letter to someone's mother."[19] Experts assert in the coming decade UAS designed to attack enemies on the ground and in the air will be the future of air power.[20] According to Air Force Chief of Staff, General Norton Schwartz, the Air Force will train more "joystick pilots" than new fighter and bomber pilots this year. According to Schwartz, "if you want to be in the center of the action, this is the place to be…it's not a temporary phenomenon…it's a sustainable career path."[21] Another Air Force general officer forecast that given the growth trends, it is not unreasonable to postulate future conflicts "involving tens of thousands" of unmanned aircraft.[22] According to General Schwartz, the trend lines are clear: the U.S. Air Force will increasingly become "less of a manned aviation force."[23] These developments represent a true revolution in military affairs, by transforming the very agent of war – who fights wars and from where – in addition to transforming and advancing what we are capable of doing via technology.[24]

Just War Theory and the Origins of the Law of War

The laws of armed conflict, commonly referred to as the law of war, are a subset of international law. This body of law is based on centuries-old Judeo-Christian teachings which have been well-documented in the writings of a number of revered theologians. The Hague Conventions of 1899 and 1907, the Geneva Conventions of 1949 and the 1977 Protocols, regulate armed conflict and govern the actions of states which are bound by the laws and treaties to which they are signatories. The laws of armed conflict exist in order to establish minimum standards of decency and acceptable behavior on the battlefield. These laws represent a set of rules which are generally acceptable to a majority of nations as the standards for the humane conduct of war.[25] To better understand the laws of armed conflict, it is worthwhile to look closer at their origin and underlying principles.

The concept of justice in war was examined as far back as 400 B.C., in the writings of Plato and Aristotle. Just war theory was further developed and synthesized over time by a number of theologians, most notably St. Augustine and St. Thomas Aquinas in the 13th century.[26] In his *Summa Theologicae*, Aquinas presents the general outline of what has become traditional just war theory. In addition to discussing the justification for war, he examines the kinds of activities which are permissible in war. Aquinas's writings are generally recognized as the model upon which later philosophers and scholars expanded and which gradually became the basis for universally recognized just war theory beyond the realm of Christendom.[27] Just war theory is most commonly divided into three parts. *Jus ad bellum* concerns the justice of resorting to war in the first place; *jus in bello* concerns the proper or acceptable conduct within war once it has begun; and *jus post bellum* concerns the justice of peace agreements when armed conflict has ended.[28]

The culmination of 19th century thought on just war theory led to the translation of moral principles into specific legal codes, in the form of the Hague Conventions, which were drafted and adopted in ten different treaties between 1899 and 1907. Today, this collection of treaties provides the widely accepted principles by which nation states wage war, and sets clear parameters pertaining to "jus in bello" – justice in the conduct of warfighting.[29] Just war theory makes a clear distinction between "justice of war" and "justice in war," which allows the judging of acts within a war to be disassociated from the cause of the war. This distinction allows for the examination of whether or not a nation fighting an unjust war may still be fighting in a just manner.[30]

Applying the Tenets of *Jus In Bello* in the Age of UAS

For the purpose of this analysis, we are concerned with the tenet of jus in bello, rather than the just cause leading up to war, (*jus ad bellum*), or just actions following the termination of hostilities, (*jus post bellum*). *Jus in bello* is the Latin term used by just war theorists to refer to justice in war – to the right conduct in the midst of battle.[31] Within the concept of *jus in bello* are a number of principles which will be examined in the context of the employment of UAS. These principles are discrimination, proportionality, responsibility, *mala in se*, and knightly honor.[32]

The principle of discrimination concerns who are legitimate targets of war.[33] Many war theorists believe the requirement for discrimination and non-combatant immunity are the most important aspects of *jus in bello*, and these are in fact the most stringently codified rules within the international laws of armed conflict.[34] On a pragmatic note, from the perspective of warring governments it is "cheaper and less messy" to keep battles on the battlefield.[35] But beyond that, discrimination is intended to protect the civilian population by clearly defining what qualifies an individual as a valid military target.

The employment of UAS alters the traditional definition of discrimination in that it eliminates the need for the combatant to be in physical proximity to a potential adversary in order to assess his combatant status, actions and the potential danger he poses. In testimony to the U.S. House Armed Services Committee, David Kilcullen, a former Australian Army officer who was a top advisor to General David Petraeus and a key counter insurgency theorist, testified "we need to call off the drones," recounting that "since 2006, we've killed 14 senior al Qaeda leaders using drone strikes; in the same time period, we've killed 700 Pakistani civilians in the same area. The drone strikes are highly unpopular… and deeply aggravating to the population."[36] According to Kilcullen and the testimony of other administration officials, the drones' record for accuracy and discrimination is far from perfect.

A number of human rights groups have also called into question the "discriminate nature" of U.S. drone employment, and have voiced concern about an over-reliance by U.S. forces on UAS in situations where significant uncertainty about combatant vs. non-combatant targeting is widespread. In a highly critical report submitted by United Nations special investigator Philip Alston in June 2009 to the UN Human Rights Council in Geneva, Alston charged the United States had created "zones of impunity" by rarely investigating private contractors and civilian intelligence agents involved in the killing of civilians from "drone attacks."[37] According to Human Rights Watch, those who fail to discriminate between combatants and civilians are responsible for war crimes, citing their position that UAS are covered by the same rules as manned systems, and the personnel who operate drones are no less responsible for their use than other soldiers operating other lethal weapon systems.[38]

The principle of proportionality addresses how much force is morally appropriate or permissible.[39] Proportionality calls upon leaders not to engage in conflict if there are less costly or less destructive options available, for instance employment of economic or diplomatic measures rather than military force. If employing military force, leaders must ensure the relative appropriateness of the force used based on the perceived threat. The principle of proportionality is prudent in that it recognizes at some point the armed conflict will end, and the means and methods by which the war was fought will affect the cost of post-war reconstruction and the prospects for long term peace and security.[40] The principle of proportionality is subjective; it requires a commander or combatant to assess whether or not the employment of a particular system or tactic is appropriate as opposed to another based on the circumstances.

The subjective assessment which is required to evaluate proportionality assumes a human is "in the loop." Some critics believe it is inevitable that over time unmanned aircraft systems infused with artificial intelligence (AI) designed to make employment decisions will be developed, and when this occurs the human controller will be removed from the decision making loop. Opponents of these AI-invested weapons base their opposition on the fact these machines will lack the human perspective and moral awareness to adequately assess proportionality.[41]

According to Singer, it is inevitable that autonomous armed robots are coming to war, because "they simply make too much sense to the people that matter."[42] A 2002 U.S. Army report addressed the challenges military decision makers face because of the exponential increase in the quantity of information and intelligence presented to them – which has the effect of "shrinking" reaction time available for decision-making. In military parlance, this decision-making cycle is known as the OODA loop, which stands for "observe, orient, decide and act."[43] The report identified the solution to the shortened OODA loop as the integration of AI into automated systems – with the end result being machines built with the capability and responsibility to assess and determine appropriate courses of action for their own employment. This development would put the principle of proportionality at risk.

The principle of responsibility mandates agents of war be held accountable for their actions.[44] According to the Geneva Conventions, it is all and only those bearing arms who are legitimate targets in time of war.[45] It is generally accepted that Soldiers killing other Soldiers is part of the nature of war, but when Soldiers turn their weapons against noncombatants or pursue the enemy beyond what is reasonable, they are no longer engaged in legitimate acts of war, but rather acts of murder.[46] When we apply the principle of responsibility to the employment of UAS we encounter a significant challenge when attempting to identify the "agent" responsible for their destruction and deadly effects. For the enemy combatant attacked by a UAS' hellfire missile, the pilot or controller who fired the missile is far from the battlefield. Is the remote pilot the responsible agent? If the answer is yes, and the pilot is stationed at Nellis Air Force Base in Nevada, is that pilot a legitimate target when walking on the Las Vegas strip with his spouse or when attending his child's sporting event in a Nevada suburban park? The distance between operator and target creates a new paradigm which challenges old principles.

In *Just and Unjust Wars: A Moral Argument With Historical Illustrations*, Michael Waltzer argues advances in military technology have effectively extended "combatant status beyond the class of soldiers."[47] Waltzer argues that without troops on the battlefield, attention must be paid to the question of which people, who might otherwise be considered civilians, should instead be considered engaged in the business of war. He raises the question of whether or not it's morally appropriate to target those who are "agentially" responsible for the threat to one's life.[48] When the employment of UAS removes the adversary from the battlefield, does the ring of responsibility expand to include the programmers who created the smart, remote weapons systems? Or to the executives of defense contracting firms who oversaw the weapons' production? Or to political leaders who funded the purchase and endorsed the employment of the technology? Author Suzy Killmister discusses the possibility and legality of the assassination of civilian combatants in public spaces based on their approval of the use of UAS.[49] Similarly, Jeffrey Smith, a former CIA general counsel, said in a Washington Post interview that ongoing drone attacks could "suggest that it's acceptable behavior to assassinate people….Assassination as a norm of international conduct exposes American leaders and Americans overseas"[50] This scenario most certainly has profound strategic implications for all of us. The traditional definitions of responsibility, combatants, and just targets become significantly more complicated and also blurred in the age of UAS.

The principle of *mala in se*, (wrong or evil in itself), holds that Soldiers may not use weapons or methods which are "evil in themselves." Such methods have historically included genocide, ethnic cleansing, rape, and the employment of weapons whose effects cannot be controlled, such as biological weapons or land mines.[51] Can a reasonable argument be made that UAS are unjust in and of themselves? It is a fact that like chemical and biological weapons and land mines, UAS restrict the options of retaliation available to the Soldiers or state under attack. A state under attack from UAS weaponry is unable to respond in the traditional, just war sanctioned manner of targeting combatants on the battlefield – because the combatants simply aren't there.[52]

It is generally agreed the first right of all Soldiers is to kill enemy Soldiers; this is part of international law.[53] The distant "drone pilots" of these systems are safe from attack by virtue of their distance from the battlefield. Just war theory states if you typically cannot identify who's responsible for the employment of a weapon then the weapon itself is unethical. The theory maintains if the nature of the weapon prevents the clear identification of the individual responsible for its employment – and the ensuing death and destruction is causes – the weapon itself violates one of the principle requirements of jus in bello. The argument can be made that UAS fall into this category of prohibited weapons by virtue of the fact the "responsible party" in the drone attack cannot be clearly identified by the enemy.[54]

Similarly, some just war scholars argue that the least we owe our enemies is allowing that their lives are of sufficient worth that someone should accept responsibility for their deaths. Grieving relatives are entitled to an answer as to why their Soldier died and who is responsible. When a UAS is the weapon of choice, it is often the case that neither the enemy Soldier nor his family knows who the attacker was, or specifically why the individual was targeted.[55] So the question we must ask is are UAS *mala in se* by virtue of the fact they deny the enemy the opportunity to know or kill their attackers, and prevent a grieving family from knowing who is responsible for their loss?

The code of honor, or chivalry as it's sometimes called, concerns fighting "fairly," or adhering to the warrior ethos.[56] This principle is understood in the context of the international order of knighthood.[57]

These early traditions invoked considerations of honor, and held that certain acts of war were deemed dishonorable in and of themselves, and were therefore shunned by the warrior class, while other actions were deemed honorable, and therefore permissible.[58] Just war doctrine was developed centuries ago when armed conflict was up close and personal. Soldiers "hacked at one another with blades or shot at one another with arrows."[59] On a very practical level, the weapons available were limited and limiting. Generally, soldiers could kill only one enemy at a time. As described by Eric Patterson, on a moral level, the limited reach of these weapons meant the combatants employing them encountered great personal risk. These face-to-face, mano-a-mano encounters were characterized by an inherent "fairness" as Soldiers faced one another, armed with similar weapons, in a well-defined space.[60]

Singer points out that while the United States may hope its technological superiority will create fear or engender respect from its adversaries, to many Afghans and Pakistanis the use of weapons operated remotely is viewed as dishonorable because the Soldiers employing the systems aren't taking any risks themselves.[61] In the Pashtun tribal culture which is characterized by honor and revenge, face-to-face combat is considered brave, while dropping missiles from UAS flying at 20,000 feet is not.[62]

It is not just our adversaries that have issues with crediting warrior attributes to UAS pilots. Singer, in *Wired for War*, interviewed Colonel Charlie Lyon, assigned to the 57th Operations Group at Nellis Air Force Base, who commands a unit of pilots working twelve hour shifts, seven days a week, fighting the war in Afghanistan from Nevada. When asked if he thought his Predator pilots were "at war," Colonel Lyon said no, explaining it was "exposure to risk that defined whether he respected someone as a fellow combatant."[63] With the removal of pilots from the risk of peril and fear, UAS have created a break in the historic connection that defines warriors and their soldierly values. According to Singer, we must ask if these new warriors are disconnected from the old meaning of courage as well.[64] On a similar note, Air Chief Marshal Sir Brian Burridge, who commanded the British military forces during the Iraq War, described UAS as part of a move toward "virtueless war… requiring neither courage nor heroism, and results in remote soldiers no longer having any emotional connectivity to the battlespace."[65]

Counterpoint: the Moral Argument in Favor of UAS

While there are those who argue against increasing the role of UAS on moral grounds, there are at least an equal number who argue in favor of expanding their role and increasing the UAS inventory. These advocates argue that UAS provide improved "discrimination," and enable a more robust situational awareness and better battlespace visualization. They maintain if enhanced with certain elements of AI, UAS have the potential to be "more ethical" than human combatants. There are also those who argue for any system which lessens the risk to our Soldiers, regardless of whether the "fairness" principle, a critical component of *jus in bello*, is jeopardized. A brief look at each of these arguments is in order.

In his article, "Killer Weapons Systems," Robert Sparrow discusses UAS, and the aspirations of developers for future systems to be capable of discriminating reliably between civilian and military targets. Proponents of UAS argue weapons capable of choosing their own targets are morally superior to "dumb" weapons.[66] In a 2009 study, Human Rights Watch reported on the Israel Defense Forces' (IDF) use of missiles launched from UAS in Gaza from December 2008 through January 2009. Although the report indicated the IDF failed to take reasonable precautions to verify targets as combatants, and therefore violated international humanitarian law,[67] it recognized the precision of Israeli drone-launched missiles.[68] Human Rights Watch investigators praised the systems' high resolution cameras which allowed operators to observe potential targets, the infrared capability which enabled effective day and night employment, and sensors which allowed UAS operators to "tell the difference between fighters and others directly participating in hostilities, who were legitimate targets and civilians, who was immune from attack, and to hold fire if that determination could not be made."[69] The report lauded the ability of the operator, via the missile's remote guidance system, to divert a fired missile in the event there was last-minute doubt regarding a target's legitimacy.[70] Human Rights Watch's Marc Garlasco recounted the employment of UAS during the 2006 Lebanon war, and how remote pilots, because they were not facing risk, were able to loiter over potential targets for hours if necessary in order to determine whether or not it was appropriate to strike them.[71]

Advocates of UAS also argue not only do these machines have the ability to "see" better than humans and therefore make more accurate targeting decisions, but also offer a unique level of consistency which can be incorporated into an ethical decision making model. Proponents of this position assert machines are capable of rigorously following logically consistent principles, while humans easily stray from principles because we get carried away by emotion.[72] Singer, in praising the potential for consistency in AI-infused machines, notes machines are not governed by passions of loss, anger or revenge. They also do not "suffer from fatigue that can cloud judgment, nor do they have those unpredictable testosterone fluctuations that often drive 18-year old boys to do things they might regret later in life."[73]

On a practical level, some argue in favor of UAS' technological capabilities, not because of their moral "fairness," but precisely because they have the potential to provide U.S. forces with an unfair advantage. Singer notes that the development of technological advances over the last few years which have made the UAS of today possible coincided with changing political winds in the United States. With the end of the Cold War, the U.S. military shrunk by more than thirty percent through the 1990's, and public tolerance for military risk began eroding. As described by Major General Robert Scales, the new era of warfare was one in which "dead soldiers were America's most vulnerable center of gravity."[74] It is against this backdrop of public opinion that former Secretary of the Army, Pete Geren, said "we do not ever want to send our Soldiers into a fair fight."[75] Geren, speaking at the 2007 LandWarNet Conference, went on to describe how the Army seeks to integrate "every element of Army modernization and seamlessly connect the Leader to the Soldier…and the Soldier to the information he or she needs."[76] Advocating the "unfair" fight, Geren said "our challenge is to give our Soldiers the edge – in whatever battlespace the enemy chooses – to take the fight to the enemy on our terms – not his."[77]

Is Just War Theory Obsolete?

The principles of just war, codified in the Geneva and Hague Conventions, have to date served humanity and civilized nations fairly well. Historically, responsible nations and internationally recognized institutions such as the United Nations and the International Committee of the Red Cross (ICRC) have worked in concert to restrict, outlaw and condemn certain munitions, weapon systems and practices deemed to violate the laws of war and the tenets of just war theory. The ICRC position on robotics, or rather its lack of a position, is representative of the current breakdown between the traditional laws of war and the reality of conflict in the 21st century.[78]

The current ICRC position states: "we have no particular viewpoint or analysis to provide."[79] As important as the ICRC has been in shaping and guarding international law over the last century, it is not yet driving discussion on what stands to be one of the most important weapons developments of this century.[80] We stand at a crossroads, on the verge of entering a new era regarding how we define "just war," or if the very concept of just war is obsolete. Much is at risk. We must not allow technological advances in weapon systems to surge ahead in a policy vacuum – to do so would be morally irresponsible.

It is indisputable that UAS change the battlefield significantly, by altering the traditional definition of who is and who is not a combatant. The essential elements of *jus in bello* – discrimination, proportionality, responsibility, mala in se, the code of honor – are altered when applied in the context of remote weapons. Because the fundamental tenets of just war theory are inadequate when viewed in the context of our most modern weapons, it is essential the rules for employing these weapons be analyzed and discussed. Many voices ought to take part in this discussion. As noted by Singer, "not merely scientists, but everyone from theologians…to the human rights and arms control communities, must start looking at where the current technology is taking…our weapons and laws."[81] It is essential for responsible nations which have in the past agreed on how we humanely wage war, to convene now to discuss these technological developments and their implications for warfare of the future.

Although the majority of this paper has been focused on just war principles and laws established in treaties and conventions, ultimately the ethical questions raised here have to do with our humanity, and how evolving war technology has the potential to change our values – actually, to change us. One of Singer's most compelling interviews in *Wired for War* is with D. Keith Shurtleff, an Army Chaplain who, at the time was serving as an ethics instructor at Fort Jackson, South Carolina. Shurtleff's main concern was that as "soldiers are removed from the horrors of war and see the enemy not as humans but as blips on a screen, there is a very real danger of losing the deterrent that such horrors provide."[82] Writing in *U.S. Catholic Magazine*, Kevin Clarke also ponders the question of the morality of UAS, saying "somehow the drones effectively hide the bloody hand of extra-judicial killing behind their essential technological coolness."[83] Like Shurtleff, Clarke is concerned the inhuman distance of UAS operators from their targets "threatens to further numb us to the human toll of…war and future conflict."[84]

Failure to examine whether the laws of war remain relevant or should be modified is dangerous. If we delay or indefinitely defer this discussion, the risks associated with this procrastination will continue to accumulate. Without broad agreement on the fundamental issue of who is a legal combatant, ordinary civilians who develop this technology and elected leaders who approve its employment potentially become targets at home and abroad. As the operators of weapon systems become more distant from the physical battlefield, the killing process is "sanitized"; UAS operators' exemption from physical danger creates a scenario in which "virtueless" war becomes the norm. In such an environment, the warrior ethos is potentially forever altered – and not for the good. Another risk we face if employment of this technology proceeds unchecked and its moral implications unexamined, is the arrival of the day when a "human in the loop" in UAS employment becomes unnecessary. If that day arrives, the principle of proportionality is irrelevant – because human assessment of the cost versus benefit decision regarding a military strike will have been eliminated. These are just a few of the eventualities which await us if we fail to adequately address how UAS changes the conduct of modern warfare. The seriousness of these issues makes this an issue of strategic importance not only for the United States, but also for our friends and our adversaries around the globe.

There is a theory called "descriptive realism" which postulates that states either do not (for reasons of motivation), or cannot (for reasons of competition) behave morally.[85] These realists view the international arena darkly, and assert that once war has begun, a state ought to do whatever it can to win.[86] For those with this mindset, or those unconvinced the issue of UAS employment is worthy of examination solely on moral or ethical grounds, there is a parallel argument which is quite pragmatic. The same creativity and innovation that have made UAS technology possible are also responsible for the miniaturization of cameras, GPS receivers, and computer components which make the assembly of small and inexpensive drones not particularly difficult. The result of these advances is that unmanned aircraft systems may soon be widely available to creative insurgents and terrorists targeting American forces, U.S. citizens, and other freedom-loving people around the world. Unfortunately, the United States and its allies do not have a monopoly on the production and employment of these weapons. As noted by Fred Reed of the Washington Times, "usually, we think of military technology as working in favor of American forces. If we are talking about fighting conventional forces, this is reasonable."[87] Reed points out that the wars we are actually fighting these days are against urban guerrillas and insurgents who can blend into rural village populations. With this in mind, he warns that "maybe people who live in glass houses shouldn't invent better stones."[88] The "better stones" now exist. The time has arrived for leaders of responsible states and stakeholder organizations to examine and rewrite the rules governing how we throw them.

Reflections on a Strategy for Computer Network Operations

Colonel John R. Mahoney
United States Marine Corps reserve

Where there is no vision, the people perish.
—Proverbs 29:18[1]

United States Geographic Combatant Commands (GCC's) are unprepared to effectively plan computer network operations (CNO) and incorporate them into military operations. This condition is not due to any failure of GCC commanders to recognize their warfighting responsibility. Current legal authorities and national policy enable CNO primarily at the strategic level of war. They marginalize GCC CNO planning efforts by denying commanders CNO decision-making authority in the more decisive operational cyberwar. This paper will discuss the efficacy of this current approach to CNO within a framework of its missing component: A Department of Defense (DoD) strategic vision for how to use CNO to help win wars in the cyberspace domain.

GCC's do not have sufficient authority to integrate CNO into their operational plans. The Services hold the authority to procure computer network attack (CNA) capabilities (i.e., tools and weapons).[2] GCC authority to conduct cyber attacks remains remarkably limited.[3] A Functional Combatant Command (FCC), U.S. Strategic Command (USSTRATCOM), directs the overall operation and defense of the GCC's computer networks.[4] Additionally, the intelligence collection component of computer network exploitation (CNE) is a function of the intelligence community (IC). GCC's are unable to integrate CNO into their planning process because they do not sufficiently control any of the pillars of CNO.

An additional deficiency that exacerbates this situation is that DoD has no comprehensive CNO strategic vision; "that picture of future changes desired by governmental elites [that] takes into account the probabilities of informed extrapolations of current foreign and domestic trend lines that will affect national security."[5] Strategic vision describes a realistic and compelling future orientation and provides a strategy to achieve it.[6] In today's existing cyberwar, the United States has yet to conceptualize a way to win.

It is important to take an objective look at this current situation to begin creating a strategic vision for how DoD will plan CNO and fight successfully in cyberspace. This paper starts by examining the nature and object of war in cyberspace and the role that CNO plays in it. Next, it identifies key definitions and discusses their implications. It follows with an examination of relevant national strategic guidance, the DoD organizations bound by it, and trends in DoD cyberspace activities. This paper evaluates each of these in terms of its importance to developing a strategic vision. It then makes recommendations for a future CNO planning environment that may better serve U.S. national security interests.

Strategic versus Operational Cyberwar

"The first, the supreme, the most far-reaching act of judgment that the statesman and the commander have is to establish…the kind of war on which they are embarking."[7] This section examines cyberspace war (i.e., cyberwar), its relationship to physical war, and the use of CNO to cause effects at both the strategic and operational levels of war.

There are several unofficial definitions of cyberwar; however, there is currently no authoritative definition in joint doctrine.[8] A general description is that cyberwar is a composite of offensive, defensive, and enabling actions taken in and through the cyberspace domain to compel a state or non-state actor to do the will of an opponent actor.[9] DoD supports both strategic and operational cyberwar but is not currently well postured for the latter.

Strategic Cyberwar

Strategic cyberwar is a campaign of cyberattacks launched by a state or non-state actor against a state and its society primarily to affect the target state's behavior.[10] By its nature, though, cyberwar is non-physical. It is a less dominant form of war than physical war. "It is almost inconceivable that a sufficiently vigorous cyberwar can overthrow the adversary's government and replace it with a more pliable one."[11] Strategic cyberwar cannot produce a decisive battle that determines the outcome of an overall war. It cannot include the disarmament or destruction of enemy forces or the occupation of its geographic territory. Physical war, in contrast, can do these things. Cyberwar can require significant expenditures and cause severe turmoil, but it cannot cause a determined opponent to surrender.[12]

Strategic Cyberwar must seek ends that are more limited than those of physical war. Its enabling assumption, therefore, is that all opponents agree to keep the war non-physical.[13] In a case where one adversary sufficiently denied another's access to cyberspace, the victim would likely escalate to physical war before it would surrender its objective. Escalation to physical conflict, however, causes the nature of a cyberwar to shift from strategic cyberwar to operational cyberwar; one in which operations conducted in cyberspace play a supporting, rather than the dominant role in the overall war. The only realistic ends of strategic cyberwar, therefore, are to frustrate an opponent, exhaust an opponent's resources and to deter escalation to physical war. The achievable ends of the current U.S. strategic cyberwar against various global cyber threats must, for these reasons, be limited to cyber-defense and cyber-deterrence.

Operational Cyberwar

"Operational cyberwar consists of wartime cyberattacks against military targets and military-related civilian targets."[14] Its enabling assumption, therefore, is that the proper use of cyberattack is to "support physical military operations."[15] Like strategic cyberwar, "operational cyberwar cannot win an overall war on its own."[16] Since GCC's plan and direct the execution of operational warfare, it follows that operational cyberwar is more appropriate for them than it is for the FCC (i.e., USSTRATCOM/USCYBERCOM) and the national intelligence agencies that are currently better resourced for its execution.

Unlike strategic cyberwar, operational cyberwar is potentially decisive.[17] It can achieve three basic objectives.[18] The first is to use cyber capabilities to create surprise, quickly but temporarily crippling enemy cyber capabilities (e.g., a surprise cyberattack prior to or simultaneously with a surprise physical attack). The second is to use cyber capabilities as tactical weapons to achieve a temporary, but potentially decisive advantage during an operational campaign (e.g., a denial of service cyberattack against key nodes in an opponent's command and control [C2], propaganda, or intelligence network). The third, used sparingly, can disrupt an enemy's confidence in networked systems, causing shifts to less efficient forms of C2, propaganda, fundraising, recruiting and training (e.g., attacks that randomly redirect C2 emails and webpage access attempts).

The Role of Intelligence in Cyberwar. A primary challenge in cyberwar is to acquire a detailed understanding of the computer networks used by an enemy. More importantly, knowing how an enemy will react to failure of those networks is critical. This underscores the question of who should lead planning and execution of a cyberattack: intelligence operatives or military operators. Intelligence operatives obtain detailed knowledge of enemy networks. Military operators, on the other hand, may better understand how a decision-maker would conduct operations without it. Martin Libicki of the RAND Corporation writes that "those best placed to plan a military campaign that uses operational cyberwar…are more likely to be military operators rather than intelligence operatives."[19] Nonetheless, U.S. policies have favored the intelligence community (IC), which has enjoyed the preponderance of skilled practitioners, equipment resources, and authorities.

Expanding the U.S. Focus to include Operational Cyberwar. Current U.S. national strategic policy over-focuses on strategic cyberwar and marginalizes the potentially more decisive results that GCC's could achieve in operational cyberwar.[20] Authorities and policies empower national strategic organizations to conduct a strategic cyberwar that is best suited for cyber-defense and cyber-deterrence. There is no argument against continuing this vigilance but the goals of strategic cyberwar should no longer be so exclusive that they obfuscate the GCC's ability to conduct operational cyberwar. A strategic vision for CNO would guide decision-makers to realign appropriate legal authorities and cyber resources, and to assign trained personnel to the GCC's, empowering them to plan and conduct operational cyberwar.

Words have Meaning

A first step in drafting a strategic vision for CNO is to examine its often-confusing lexicon.

Cyberspace. Cyberspace is "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."[21] The significance of this definition is that it identifies cyberspace as a new warfighting domain, distinct from the land, air, maritime, and space domains. Domains are where warfighting occurs. Warfighting involves C2, fires, movement and maneuver, sustainment, protection, and intelligence functions.[22] GCC's are the essential directors of these functions, linking "U.S. national strategy and operational activities within a theater."[23]

The ability to plan CNO is critical because effective operations in this domain are "the prerequisite to effective operations across all strategic and operational domains – securing freedom from attack and the freedom to attack."[24] Without the ability to plan effective CNO at the GCC's, military operations in all other domains are at risk.

Cyberspace operations, network operations (NETOPS), and the global information grid (GIG). A term closely related to cyberspace is "cyberspace operations," which is "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include CNO and activities to operate and defend the Global Information Grid (GIG)."[25] This definition implies that "cyberspace operations" consists of at least two distinct activities, CNO and "activities to operate and defend the GIG."

The definition of network operations (NETOPS) is "activities conducted to operate and defend the GIG."[26] Therefore, cyberspace operations include a combination of CNO and NETOPS.

The GIG is "the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for acquiring, processing, storing, transporting, controlling, and presenting information on demand to joint fires and support personnel."[27] Since the infrastructure defined here is on demand to joint fires and support personnel, reference to the GIG means the DoD portion of the Internet.

Computer Network Operations (CNO). The definition of CNO is somewhat vague. It is "comprised of computer network attack (CNA), computer network defense (CND), and related computer network exploitation (CNE) enabling operations."[28] Notably, this definition does not tell the reader what CNO is, only what comprises it.

This definition of CNO implies that "CNA, CND, and related CNE enabling operations" are different activities. The implication from the definition of "cyberspace operations" is that CNO is an "operation" to achieve objectives that contribute to the "employment of cyber capabilities" in or through cyberspace. It then follows that CNO is essentially a planning function that results in an integrated, coordinated, and synchronized operation that is a combination of actions associated with CNA, CND, and related CNE enabling operations.

Computer Network Exploitation (CNE). The definition of CNE is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[29] This implies that CNE has two sub-elements, one that is an operations activity (the "enabling operations"), and another that is an intelligence function ("collection"). At issue is whether it is only the IC that conducts CNE (under its Title 50 authority), or if there is a complementary role for the operations community to perform in the enabling operations function (under its Title 10 authority).

This issue is important for the operations community. The definition of CNO does not include the intelligence sub-element of CNE since it is simply "comprised of CNA, CND, and *related CNE enabling operations*"[30] [emphasis added]. Devoid of the intelligence collection sub-element of CNE, CNO remains an operational function. In doctrine, therefore, CNO is comprised of CNA, CND, and just one of the two sub-elements of CNE.

Computer Network Attack (CNA). CNA is "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[31] CNA is an offensive activity. As such, the authority to conduct a CNA belongs to the operations community. The IC, however, plays a significant role in preparing military operators to execute CNA. Its role involves conducting CNE and providing related intelligence support to the operations community for an attack to be effective.

Current policy correctly assigns responsibility for operational maneuver to GCC commanders, but unfortunately reserves much of the authority to execute supporting CNA to USSTRATCOM. The first issue of concern with this policy is that it conditions the IC to deal more directly with an FCC than it does with the supported GCC. The second issue is that this policy complicates GCC efforts to conduct CNO planning.

To achieve the defensive and deterrent ends of the strategic cyberwar, it is appropriate that the IC maintain its close supporting relationship with USSTRATCOM. In fighting the neglected operational cyberwar, though, the IC must support the GCC's in a similarly direct and timely manner. A strategic vision should propose an equally close supporting relationship between the IC and the GCC's. Without it, CNO planning is further complicated due to reduced intelligence timeliness and insufficient network intelligence detail provided to the GCC's planning staff.

CNA-Operational Preparation of the Environment (CNA-OPE). CNA-OPE is an operational activity, related to CNA, that uses cyberspace tools to gain access, confirm continued access, and to gather information about computers and computer networks being targeted for CNA.[32] The intent of CNA-OPE, therefore, must not be the collection of intelligence even though it may employ tools and techniques similar to those used by the IC. Its purpose is to support cyber targeting and attack. It is similar to the "related CNE enabling operations" discussed in the CNO definition section above.

A practical prerequisite for the GCC to execute CNA-OPE is that the IC first provides an initial description of the key network links and nodes against which an attack will occur. The GCC commander can then better conduct CNA-OPE in order to ensure target access and validate attack parameters before executing a successful CNA. A strategic vision for CNO should emphasize this important GCC requirement.

Computer Network Defense (CND). Joint Publication (JP) 3-13, *Information Operations*, defines CND as "actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks."[33]

There is often confusion about the difference between CND and the "defend" role identified in the definition of NETOPS. In theory, the difference is that CND considers the potential impact of cyber threats from outside the network. NETOPS considers the reliability and efficiency of the network that can be achieved by "hardening" it from the inside. As a practical matter, the personnel with CND expertise are the same individuals that do NETOPS; the information technology (IT) professionals normally assigned to the Communications (G/S-6) section and similar, specialized organizations. CND and NETOPS, therefore, have an overlapping relationship. NETOPS professionals conduct CND while CNO planners integrate CND activities with CNA, CNE, and other related actions in support of the commander's overall mission objectives.

Computer Network Defense – Response Actions (CND-RA). An authority closely related to CND is CND-RA. It is "deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks *under attack or targeted for attack* [emphasis added] by adversary computer systems/networks."[34] There are several increasingly aggressive levels of CND-RA.

While at its most aggressive level[35] there are similarities between CND-RA and CNA, a CND-RA is aggressive but not offensive. It is a defensive act, not an attack, executed to prevent an ongoing or anticipated attack against the friendly network from being more effective than it would be without an aggressive response.

Practical Implications. In practice, CNO is a planning function that integrates, coordinates, and synchronizes the five activities identified above: CNA, CNA-OPE, CND, CND-RA, and CNE. The CNO planner performs none of these activities. The planner's job is to communicate with the individuals, organizations, and agencies that execute the activities and coordinate for their conduct to support the military objectives articulated by the commander.

To support the requirements of the strategic cyberwar, current national policies retain most authorities and resources for the execution of the five activities at national strategic organizations and agencies. This has a detrimental effect on GCC's because it negatively affects their ability to plan and execute CNO in support of the operational cyberwar. The following section includes a more detailed examination of these national policies.

National Strategic Direction

Much of the guidance published about cyberspace operations and CNO is classified. This section is, therefore, limited in its scope by the guidance available at the unclassified level. A strategic vision should evaluate the necessity of maintaining so much of the relevant discussion at the classified level. Perhaps the broader operations community could provide better insights once it is more widely informed from new unclassified literature and discussion.

National Security Strategy (NSS) of the United States of America. The NSS, signed by the President, declares that DoD is "pursuing a future force that will provide tailored deterrence of…threats (including ...terrorist attacks in the...information domain)."[36] It is not hard to see this seminal guidance reflected in the national focus on cyber-deterrence and its emphasis on the strategic level of cyberwar. The document does not address CNO specifically but it does reveal the strategic direction in which the DoD is to move.

The NSS recognizes that DoD "is transforming itself to better balance its capabilities [against]…disruptive challenges from…actors who employ technologies and capabilities (such as…cyber operations)."[37] This guidance encourages a military transformation within DoD and specifies the need for "a better balance" in its approach to cyberspace operations. A strategic vision for CNO, therefore, should provide an achievable future orientation on how the military can support both the strategic and the operational cyberwar.

National Strategy to Secure Cyberspace (NSSC).[38] The NSSC provides overarching policy guidance regarding the nation's defensive approach to cyber security. It identifies several national critical infrastructures and the lead government agencies that are responsible for their cyber security. The NSSC also identifies the top five national cyber security priorities in terms of needed plans or programs.

This document calls for transparency and collaboration among all sectors of the U.S. government and private sector. Even though more recently published cyber security guidance is discussed below, none of it supersedes or rescinds the NSSC. It continues to inform all subordinate NETOPS and CND planning and operations.

Comprehensive National Cyber-security Initiative (CNCI). "Rather than serving as an overarching national strategy document with specific instructions for federal agency implementation…, the CNCI is seen as a plan of action for programs and initiatives."[39] It identifies several objectives that support its goal of comprehensively addressing the nation's cyber security concerns. Each is consistent with the national priorities described by the NSSC and, in this sense, is a natural extension of that document. It serves as a key roadmap for the roles of government and private activities at the strategic cyberwar level. It does not address the GCC's role specifically so it has limited significance as a guide to commanders planning military activities in the operational cyberwar.

Cyberspace Policy Review (CPR, also known as "The 60-day Review"). Conducted shortly after President Obama took office, the CPR emphasizes the need for the nation to take immediate action to secure cyberspace. It provides both near- and mid-term action plans to assure "a trusted and resilient information and communications infrastructure."[40] President Obama approved the recommendations of the CPR in May 2009, establishing them as national strategic guidance. The CPR's focus is also at the strategic cyberwar level and thus provides little guidance to GCC's regarding the conduct of CNO.

The Unified Command Plan (UCP). The UCP, signed by the President, "establishes the missions and geographic responsibilities among the [ten Unified] Combatant Commands."[41] It has assigned significant responsibilities to USSTRATCOM for cyberspace operations.[42] The UCP serves as a principal source of guidance for CNO planning. It establishes a central role for USSTRATCOM but, by requiring coordinated cyberspace operations with the GCC's, implies that the GCC's have unique CNO authorities apart from USSTRATCOM.[43] It creates advantages for USSTRATCOM that include more efficient C2, improved unity of command, and a degree of standardization. A strategic vision might recommend UCP changes that specify the cyber missions and responsibilities of the GCC's in more detail.

The National Military Strategy for Cyberspace Operations (NMS-CO). An unclassified, publically available version of the NMS-CO offers guidance that supports this paper's thesis; that the ability to plan and conduct CNO should not be limited primarily to national-strategic organizations. Subordinate echelons can achieve decisive results if given appropriate authorities and CNO capabilities.

The NMS-CO declares, "Operations to achieve desired effects in and through cyberspace require integration of organizations, capabilities, functions, technologies, and mission."[44] It is also specific about the responsibility of military leaders. First, it directs that "senior leaders must establish a structure that integrates all mission areas and dismantles stove-piped organizations that hinder collaboration and lengthen decision-making cycles."[45] It guides more than just the responsibility of senior leaders. The NMS-CO warns that the DoD will also "hold leaders at all levels responsible and accountable for cyberspace operations in the same manner as accountability is addressed in the other domains."[46]

The current practice of maintaining most CNA authorities and capabilities at national strategic organizations is inconsistent with the NMS-CO. The document advises senior military leaders to "integrate capabilities across the full range of military operations using cyberspace [and] conduct collaborative planning for integrated cyberspace operations synchronizing with other military and intelligence operations."[47] It even tells commanders how to do this.

"C2 in cyberspace operations is achieving unified action vertically and horizontally, among all levels of war, and throughout organizations."[48]

The NMS-CO shows that Defense Department policy favors a decentralized, cross-echelon distribution of CNO authorities, capabilities, and planning responsibilities. The practice of executing current national policy, which stresses interagency coordination due to its focus on strategic cyber defense and cyber deterrence, fails to loosen the reigns of centralization that impede the effective conduct of the operational cyberwar by the GCC's. A strategic vision for CNO planning might emphasize a need to restructure organizations, C2, training, and the allocation of cyber resources.

Doctrinal Guidance. As late as February 2010, there were 78 currently approved joint doctrine publications.[49] Issues pertaining to cyberspace are a primary topic in only two of them: JP 6-0, *Joint Communication Systems*, which discusses NETOPs[50] and CND;[51] and JP 3-13, Information Operations (IO), which describes CNO as a core capability of IO.[52] Although a new classified publication, Joint Test Publication 3-12, *Cyberspace Operations*, is currently under development, these two unclassified publications do not adequately address specific CNO training requirements or the details of the CNO planning process. A strategic vision for CNO would propose the development of a more robust doctrinal library.

Organizational Trends

This section seeks to evaluate existing conditions, extrapolate emerging trends, and identify the underlying motivations in some of today's key cyberspace-related decisions. Three important trends are developing today that could transform the CNO community within the next five to fifteen years. They are the creation of U.S. Cyber Command (USCYBERCOM), sub-delegation of CNO authorities and capabilities, and the increasingly significant role of the IC, specifically the Signals Intelligence (SIGINT) community, in the execution of not just CNE, but of CNO in general.

U.S. Cyber Command (USCYBERCOM). This new sub-unified command is a subordinate organization under USSTRATCOM. In the past, USSTRATCOM had sub-delegated CND missions to Joint Task Force – Global Network Operations (JTF-GNO). Concomitantly, it had sub-delegated CNA missions to Joint Functional Component Command – Network Warfare (JFCC-NW). The commander of JFCC-NW had also been "dual-hatted"[53] with the Director of the National Security Agency (DirNSA). DirNSA directs a Title 50 intelligence agency with the authority to conduct CNE, although USSTRATCOM has no authority over DirNSA in the execution of its Title 50 responsibilities.

In 2008, USSTRATCOM transferred operational control (OPCON) of JTF-GNO to JFCC-NW. For the first time, one three-star general held authorities for all the CNO components (i.e., CNA, CND, and CNE). The observed trend has been an evolving consolidation of organizations that exercise authority for CNA (i.e., JFCC-NW), CND (i.e., JTF-GNO), and NSA (i.e., CNE).

In June 2009, the Secretary of Defense (SECDEF) approved the establishment of USCYBERCOM, which would combine and then disestablish JTF-GNO and JFCC-NW.[54] Its commander would be the same three-star JFCC-NW commander, still dual-hatted as DirNSA. In May 2010, Congress approved promotion for the commander of USCYBERCOM (and of DirNSA), creating a new four-star, Title 10 commander of USCYBERCOM who now has authority for CNA and CND (and, under his Title 50 authority as DirNSA, for CNE as well).

Although speculative, the President may eventually break USCYBERCOM out from under USSTRATCOM, establishing it as a separate unified command. If this occurs, one independent FCC uniquely configured to support cyberspace missions could significantly improve DoD CNO support to the various government and private sector cyber-security communities engaged in the strategic cyberwar. The major potential downside would be if increasing support requirements for the strategic cyberwar caused USCYBERCOM to decrease its integration and support to the GCC's, and thus further marginalize their CNO capabilities in the operational cyberwar.

Sub-Delegation of CNO Authorities and Capabilities. GCC frustration with the often arduous and time-consuming Request and Approval

(RAP) process for CNO support is growing. Both General Petraeus[55] and General Odierno[56] appealed to their superiors in Washington for more CNO support during their tenures as Commanding General of Multi-National Forces Iraq (MNF-I). As cyber threats and opportunities expand, future GCC Commanders are increasingly likely to request improved support in the operational cyberwar.

Time, and the expanding challenges of cyberwar, will help to identify the appropriate command level to execute specific cyber operations. Eventually, the question from the operating forces will no longer be about what support the national community can provide. It will be about why the operating forces do not already have authorities and organic capability in place.

Graduate research at the Air Force Institute of Technology examined three models – Independent, Interdependent, and Organic – for how USSTRATCOM [or USCYBERCOM] could accommodate this expected increasing demand for CNO support at lower command echelons.[57] A strategic vision might consider these three models as separate options or, alternatively, as a single process that starts with the first and matures into the second and third over time. For example, each GCC's Service Component Commands (SCC's) might initially establish a CNO proponent. Each GCC would next designate a cyberspace coordinating authority and USCYBERCOM would coordinate, integrate, and synchronize CNO planning and operations through them. As expertise and confidence grow, the Services could program more CNO personnel to support the GCC's through their SCC's. Eventually, the GCC's could establish subordinate CNO-JTF organizations with augmentation from USCYBERCOM. Then, as these CNO-JTF's matured, they could become sub-unified commands under each GCC, greatly expanding the capacity of each for CNO planning and execution. The biggest challenges to this seem to be insufficient willingness to commit resources to it and a strategic vision to guide the process.

Expanding Role of the SIGINT Community. Neither the CNA nor the CND communities can currently match the CNE (i.e., SIGINT) community in knowledge of the net combined with knowledge of the cyber threat. The operations community, which has authority to conduct CNA, CNA-OPE, CND, and CND-RA, is thoroughly dependent on the IC to provide detailed network intelligence in a timely manner. While USCYBERCOM and NSA are rectifying this challenge by consolidating capabilities into a command that the SIGINT community can support, they have not yet effectively addressed it for the benefit of the GCC's. Instead of expanding NSA support to the GCC's, the trend seems to be toward expanding the IC's activities into functions that are traditionally operational.

The Electronic Warfare (EW) community, for example, is becoming concerned that the convergence of electronic and computer technology may eventually result in their community becoming absorbed into the cyberspace community. The EW community, operating under Title 10 operational authorities, has enjoyed relatively simple and often tactical level execution authorities in the past. Once aligned with the CNO community, however, they are afraid that they will lose their flexibility to conduct operations. Additionally, SIGINT personnel employ many of the same technologies used by the EW community. The SIGINT community is large and well funded whereas the EW community is a relatively small community which few senior leaders truly understand. The concern is that the SIGINT community will eventually execute EW missions rather than simply support them.

The most telling sign of this trend, though, is that in the establishment of USCYBERCOM, the officer chosen to lead it was not from the operations community, but from the SIGINT community (i.e., DirNSA). This most significant CNO command assignment could have been a Title 10 operational commander (with authority for CNA and CND) who gained an expanded mission that included Title 50 CNE authority. Instead, an existing Title 50 commander (i.e., DirNSA) gained an expanded Title 10 mission. If USCYBERCOM is to better integrate CNO for the GCC's in the future, a strategic vision should address whether an intelligence operative can achieve that goal better than if a military operator were in command.

Recommendations

This research has identified several issues that a strategic vision for CNO could address. The areas in which they find consensus with the views of other writers, commanders, planners, and practitioners could form the basis for a unifying strategic vision about CNO. The following are some initial recommendations for that vision.

First, national strategic leaders should immediately apportion to the GCC's appropriate legal authorities, cyber resources, and trained personnel, empowering them to organically plan and conduct operational cyberwar. The primary advantage of doing this is that it will enable the GCC's to directly plan and employ CNO capabilities in support of decisive operational actions that achieve overall strategic ends. The chief disadvantage is that it will decrease the overall capability of USCYBERCOM by redirecting some of the CNO resources programmed to support it. The chief risk is that by refocusing the NSA and the IC on the GCC's, they will lose focus on the strategic cyberwar. This is unlikely, though, since the Director of National Intelligence (DNI) and the President determine the national intelligence priorities.

Second, the SECDEF should develop and approve a plan within the next year to mature subordinate CNO JTF's at each GCC. The plan should direct each SCC supporting a GCC to establish a CNO proponent to coordinate with USCYBERCOM and NSA. Each GCC should establish a Cyberspace Coordinating Authority (CCA) to oversee all CNO proponent issues with the CNO stakeholder community. The plan should request that the Services augment the SCC CNO proponents and GCC CCA's with trained CNO personnel. It should also establish the objective of maturing these organizations into a standing CNO JTF, with appropriate legal authorities and organic CNO capabilities, at each GCC within ten years. The great advantage of this is that it enables the warfighting commanders the ability to employ CNO decisively in support of operational maneuver when it is applicable. Its main disadvantages are that it requires significant personnel and other resources that the Services are not currently programmed to provide. The greatest risk, though, is having U.S. operational forces face enemies who shape operations with a devastating cyber attack followed quickly with a vigorous physical one.[58]

Third, DoD should significantly expand training programs that teach military CNO technical capabilities and planning skills. This should also include the development of doctrine, tactics, techniques, and procedures that are more extensive and kept at the unclassified level where possible. The advantage of this is that it will standardize both the lexicon and the processes for conducting CNO. The main disadvantage is that it will be difficult to gain wide consensus on the best approach. Nonetheless, the risk of not choosing a reasonable end state that empowers the GCC's leaves U.S. operational forces relatively unarmed for battle in the cyberspace domain.

Fourth, a strategic vision for CNO should establish the goal of selecting a former GCC commander as a future commander of USCYBERCOM. This commander should also be dual-hatted as the DirNSA while an intelligence officer remains the Deputy DirNSA. The main advantage of this is that it will bring greater operational perspective to cyberspace operations. Its chief disadvantage will be the change necessary within the DoD cyber community culture; from one led by an experienced and well-trained IC to one in which the operations community becomes equally capable. The risk, however, is that maintaining the focus of the IC on the strategic cyberwar at the expense of the operational cyberwar puts the successful accomplishment of both in jeopardy.

Conclusion

This research indicates the national strategic community has focused on enabling a few key military organizations to support its fight in the strategic cyberwar. While this is well intentioned, it has not enabled the GCC's to succeed in the potentially more decisive operational cyberwar. Military adversaries that would challenge U.S. strategic interests remain likely to engage GCC's in synchronized cyber and physical attacks at the operational level of war. It is time to empower the GCC's to fight them.

Prudens
Futuri

Strategic Impact of Cyber Warfare Rules for the United States

Mr. Paul A. Matus
National Security Agency Civilian

> *So cyberspace is real....It's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy.*
>
> —Barack Obama[1]

The cyberspace domain is becoming increasingly complex interconnecting commercial, governmental and private equipment, networks and systems. Actors in cyberspace are diverse: law-abiding citizens, groups, corporations, and governments; belligerent state and non-state actors; and military elements acting by direction of their host states. Activities vary along a continuum ranging in severity from legal commerce to what may be considered acts of war. And yet, few laws, treaties or other rules specifically for this domain have been implemented. Why is this so?

This paper examines the existing framework of cyber warfare rules, using the summer of 2008 cyber attacks against Georgia as an example, and determines the strategic impact of existent and nonexistent cyber warfare rules for the United States.

The United States along with a host of other information-age countries are becoming increasingly vulnerable to belligerent activities in cyberspace. In 2007, Sami Saydjari, President and Founder of the nonprofit Cyber Defense Agency, testified before the House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology and described a digital "Hurricane Katrina" for the entire country following a cyber attack.[2] He stated the cyber attackers are a well-funded cadre biding their time against would-be victims increasingly dependent on integrated information systems.[3] Others have warned of a "digital Pearl Harbor" where U.S. electrical grids, air traffic control systems or nuclear power plants are infiltrated and disrupted or destroyed.[4] During World-Wide Threat Hearings in early 2009, Admiral (retired) Dennis Blair, Director of National Intelligence, stated that:

> our information infrastructure is…becoming vulnerable to catastrophic disruption in a way that the old analog decentralized systems were not. Cyber systems are being targeted for exploitation and potential for disruption or destruction by a growing array of both state and non-state actors.[5]

Others argue the United States is not as vulnerable as these experts suggest. According to Jim Lewis, Director and Senior Fellow at the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), it is difficult to cause mass casualties using cyberspace against a country like the United States which is reliant on many different infrastructures.[6] The cyber attacks against Estonia in 2007 and Georgia in 2008, while conducted on a large scale caused little tangible damage according to *The Economist*.[7]

Admiral Blair further testified on the need to build defenses against nations like Russia and China which:

> can disrupt elements of the U.S. information infrastructure. We must take proactive measures to detect and prevent intrusions before they do significant damage. We must recognize that cyber defense is not a one-time fix. It requires continual involvement in hardware, in software, in cyber defenses, and in personnel.[8]

More specifically, Admiral Blair cited the ability of an adversary to "doctor" computer chips associated with communications and military equipment. Adjustments to the chips, which are embedded with virtually all equipment operating system software, could permit the adversary to disrupt or destroy the targeted system.[9]

These vulnerabilities induce costs to the United States. "The compromise of our nation through this invisible battleground has cost billions of dollars from our economy in terms of theft of both intellectual property and the destruction of information systems,"[10] according to Michael Assante, Chief Security Officer, North American

Electric Reliability Corporation, before the House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology. Air Force General Kevin Chilton, Commander United States Strategic Command (USSTRATCOM) – the combatant command assigned the cyber defense mission – also cited the vulnerabilities our nation faces "…we're seeing a lot of…intrusions into our military networks" for the purposes of "exploitation or espionage."[11]

In addition to presenting vulnerabilities to the United States, actions in cyberspace continue to become more complex. According to Assante, "cyber weapons are often not flagged and their true origins are unknown and therefore un-attributable, and most importantly, they have been largely successful in evading the instruments available to prevent and deter it."[12] General Chilton described the actions against Estonia and Georgia as "coordinated cyber attacks that were aimed at the computer infrastructure of those countries or those operations and tried to take away their ability to use their computer networks to conduct operations."[13] In contrast to other domains of warfare, "in cyberspace, enemy combatants can pry, spy, implant, extract and dismantle more quickly and more secretly." according to Amber Corrin, *SIGNAL* magazine's Assistant Editor.[14]

Many experts believe the volume of belligerent acts will continue to grow exponentially. According to a defensetech.org online posting by Kevin Coleman in January 2010, "cyber attack volume[s will] escalate dramatically." In support of this forecast, he further stated "malware [malicious software] grew [in 2009] at the highest rate in 20 years. Multiple security reports showed that more than 25 million new strains of malware were identified" with predictions of this continued trend.[15]

Trends also suggest an increasing variety of cyberspace belligerents, possibly an increase in the numbers as well. The types of actors can be characterized in several ways. According to General Chilton "our threats actually span the spectrum from the…bored teenage hacker…to the criminal element…to the organized nation-state."[16] Admiral Blair in testimony affirmed for Senator Barbara Mikulski that high-tech states, organized crime groups and individual hackers for hire "could pose threats to our critical infrastructure." Admiral Blair further testified that the main threats come from these groups of actors (i.e.

hackers, organized crime and state-sponsored) in Russia and China and that the bulk of cyber intrusions against the United States come from Internet Protocol (IP) addresses in China and Russia.[17]

In her presiding remarks before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, Representative Yvette Clarke cited a *Wall Street Journal* article from April 2009 stating cyber intruders from Russia and China have already penetrated the electric power grid and were "positioned to activate malicious code that could destroy portions of the grid." Further testimony elaborated that China's cyber warfare doctrine seeks "global electronic dominance by 2050, to include the capability to disrupt financial markets, military and civilian communications capabilities, and the electric grid prior to the initiation of a traditional military operation." North Korea and Iran were also cited as countries having offensive cyber attack capabilities in addition to Russia and China.[18]

Given the vulnerability of the United States and her allies, the complexity of cyberspace, increasing volume of belligerent acts, and the wide variety of legitimate and belligerent actors, the cyberspace domain needs rules to establish accepted norms and govern activity. Major Arie Schaap's 2009 article, "Cyber Warfare Operations: Development and Use Under International Law," in the *Air Force Law Review* concluded:

> …as states begin to focus their energies on developing doctrine and weapons for conducting cyber warfare operations, it is essential that we move beyond just the realization that cyberspace is an important new battleground for conducting warfare operations and recognize the need to come to an understanding of what rules regulate this new battlefield.[19]

Two year earlier, Duncan Hollis discussed the notion of "e-war rules of engagement" where "nations could agree to waive sovereignty and permit a direct response to cyber attacks (e.g. Rules of Cyberwar)."[20] Both of these studies advocate the need for cyber warfare rules.

What are U.S. strategic objectives in cyberspace? According to Colonel Jeffrey Caton, a professor at the U.S. Army War College, they are "to prevent cyber attacks, reduce national vulnerability to cyber attacks, and minimize damage and recovery time should attacks occur." Two of the five national priorities for the 2003 cyberspace strategy were to secure governments' (not just the United States) cyberspace and international cooperation with the realization that the U.S. domain is only as secure as the weakest domain with which it is connected. [21]

Analyzing the U.S. approach toward international collaboration in cyberspace involves many variables, and providing definitions will help establish a common understanding of the terms. For example, how is a cyber attack different from exploitation or counter-attack? This paper reviews existing international rules to include treaties and laws and examines the cyber attacks against Georgia for relevance to the topic of international rules. These examples help determine the strategic impact to the United States as well as provide analytical conclusions along with recommendations for the future.

Definitions

The October 2008 update to Joint Publication 1-02 defines 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.[22]

Simply put, the cyber domain (e.g., cyberspace) is a complex system of systems that spans the globe and extends into space. In a virtual sense it makes every state and non-state actor a next-door neighbor and yet does not recognize the rules of sovereignty (e.g., national borders) or private property in many ways. Transactions in cyberspace occur at almost the speed of light, over an almost infinite volume, and with a variety of data that changes almost daily. The "three V's" (i.e., volume, velocity, and variety) of cyberspace further complicate efforts to codify international rules and U.S. government policy.

Actions in cyberspace can be categorized three ways; legitimate (i.e., lawful and not considered illegitimate), criminal (e.g., unlawful – a law cites the action as criminal), and illegitimate (i.e., considered malicious by a state or non-state actor, but no law exists to cite as criminal).

Both legitimate and criminal actions in cyberspace are reasonably understood; the international community has little disagreement once actions can be categorized as such. The contention among parties occurs over illegitimate actions in cyberspace.

A further delineation of actions in cyberspace is helpful when considering U.S. and other state or non-state actor offensive actions. While all things cyber are not computer and vice versa, computer network operations (CNO) – specifically computer network attack (CNA) and computer network exploitation (CNE)[23] – are cyberspace activities likely considered illegitimate and possibly criminal. At this point it is helpful to step back and review the United Nations' (UN) point of view and look for analogies in cyberspace.

Article 1 of the UN Charter cites its purpose "to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace..."[24] Article 1 of UN General Assembly Resolution 3314 defines aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[25] Arguably, illegitimate actions in cyberspace (i.e. CNA and CNE) could fit the definition of an act of aggression according to this article. The debatable point for this analysis is the reference to "armed force."

Article 2 of the UN Charter cites "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[26] Illegitimate activities in cyberspace arguably fit this definition, however, the debate rests along the reference to the "use of force." According to Article 3 of Resolution 3314:

> Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provision of article 2, qualify as an act of aggression:
>
> (a) The invasion or attack by the armed forces of a State or of the territory of another State, or any military occupation,

> however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
>
> (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
>
> (c) The blockade of the ports or coast of a State by the armed forces of another State…[27]

These acts limit belligerents to state actors. While there may be some doubt if an illegitimate cyberspace action is an "act of aggression," this article provides examples of situations, whether in the cyber domain or not, where illegitimate actions in cyberspace (i.e. CNA and CNE) are "acts of aggression." Cyber warfare such as denial of service attacks that "block" a host nation's servers may be regarded as a "blockade." Also, installation of malware on a host nation's telecommunications infrastructure may be regarded as an "invasion."

How are acts of war and acts of aggression differentiated? The UN has defined "acts of aggression," which could be interpreted as acts of war. There is a slight difference between the two in that an act of war suggests a measure of response from the victim, while an act of aggression merely acknowledges a hostile event on a scale not reaching the level of war. Martin Libicki of RAND Corporation defined acts of war along three axes: universally, multilaterally, and unilaterally.[28] Basically, a universally declared act of war is one where all states believe an event to be an act of war. Those along the multilateral axis suggest more than one nation declares the event as an act or war, and the unilateral axis provides that one state declares an event an act of war. While counter actions can be debated, ultimately, it may be in the interest of the victimized state to declare an event an act of war. Having agreement from other nations (i.e., multilateral or universal) provides improved justification (i.e., the "moral high ground") for counter actions as well as the potential for increased levels of support from other nations.

Rules for Cyber Warfare

In 2007, Duncan Hollis suggested that rules for cyberwar and regulations prescribing how state and non-state actors should fight in cyberspace were limited.[29] In 2009, Libicki characterized deterrence and war in the cyberspace environment (e.g. cyber warfare) as "its own medium with its own rules." He further elaborated on the complexities for establishing rules.

> Cyber attacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce. The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again.[30]

Defining a rule as an "authoritative regulation for action or established practice that serves as a guide,"[31] introduces several potential categories of rules for fighting in cyberspace. For example, existing treaties, conventions (e.g., Geneva Convention) and laws (e.g., Law of Armed Conflict) may articulate accepted and non-accepted rules for performing cyber warfare. Also, prescribed rules of engagement (ROE) and collaborative operations can help define levels of acceptance for cyber warfare. According to Hollis, "war has entered the Information Age, and it's time for the international law to get a needed update,"[32] but laws are only one of several ways to provide the requisite governance. Examining existing rules (i.e. laws, treaties, conventions, ROEs and collaborative operations) may help identify and codify acceptable boundaries for cyber warfare.

In 1960, the UN Security Council concluded that the United States U-2 overflights of the Soviet Union's sovereign airspace did not constitute an unlawful use of force in accordance with Article 2(4) of the UN Charter.[33] Applying this scenario to the cyber domain suggests that computer network exploitation, a form of cyberspace intelligence, surveillance and reconnaissance (ISR), also might not meet the threshold of an unlawful use of force.

The Geneva Conventions and Council of Europe Convention on Cybercrime (CoECC) may have applicability to cyber warfare. The United States joined the CoECC, which went into effect in January 2007.[34] The convention, which is the only legally binding multilateral instrument for computer-related crime, was designed to protect citizens from hacking, organized crime and terrorism.[35] The CoECC has several purposes including "a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation." This objective recognizes "the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offenses may be stored and transferred by these networks."[36] The protection of society and use of computer networks to commit crimes have applicability to cyber warfare. Chapter II, Substantive Criminal Law, Title 1, Offenses against the confidentiality, integrity and availability of computer data and systems, of the CoECC identifies three articles which have direct applicability to cyber warfare (emphasis added).

> Article 2 – Illegal access: Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the *access to the whole or any part of a computer system without right.*
>
> Article 4 – Data interference: Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the *damaging, deletion, deterioration, alteration or suppression of computer data without right.*
>
> Article 5 – System interference: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by *inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*[37]

Each of these articles specifies criteria which may be considered reasonable first-order consequences of cyber warfare. Even acts of CNE fit this criterion; of course, attribution of the CNE must be determined before pursuing criminal charges – the belligerent actor must be identified.

While not providing specific language relating to cyber warfare, Protocol 1 to the Geneva Conventions provides rules through analogy. Article 51 of this document protects civilian populations and defines unlawfully indiscriminate attacks as: "(a)those not directed at a specific military objective; (b)...which cannot be directed to a specific military objective; or (c)...which cannot be limited as required by this protocol."[38] The language suggests CNA performed against specific military objectives may be considered as lawful action, while events against non-military objectives are unlawful or criminal. Subjectivity arises when non-military resources are attacked which are determined by the belligerent to be military associated. In 2008, Stephen Korns and Joshua Kastenberg judged that CNA rose to the level of an armed attack in accordance with Article 51.[39] Air Force Major Arie Schaap further assessed Korns and Kastenberg's interpretations in the Air Force Law Review that CNA which causes physical damage to a sovereign nation's assets could meet the threshold of an armed attack in accordance with Article 51.[40]

While the United States is involved in no international treaties directly tied with cyber warfare, it is worth highlighting recent dialogue on the subject. As recent as June 2009, an anonymous Department of State (DoS) official noted that the United States and Russia disagreed on the implementation of a cyberspace treaty. According to the DoS official, Russia favored a treaty along the lines of those implemented for the production of chemical weapons, while the U.S. argued a treaty was unnecessary. The focus should be toward international law enforcement cooperation which would increase security against cyber crime and thus extend into military campaigns, according to the U.S. official. Russia, on the other hand, suggested without a treaty, a cyber arms race would begin. Earlier that same year, Vladislav P. Sherstyuk, a Deputy Secretary of the Russian Security Council described their position which banned a state actor from secretly embedding malicious codes or circuitry in computer systems that could be later activated in the event of war. Other proposals include applying humanitarian laws against the application against noncombatants and banning deception operations; however, U.S. officials argued these proposals would be ineffective given the difficulty in ascertaining attribution of an attack from a state, a proxy, or an independently acting non-state actor.[41]

During the DNI's testimony before the Senate Select Committee on Intelligence in early 2009, Senator Feinstein pressed the issue of developing cyber treaties in order to help hold belligerents accountable for their actions.

> …and yet it seems to me that, other than the intelligence world, there is a very real policy gap out here where the diplomatic world needs to step in. And when things happen, countries need to get demarched, as opposed to keeping all of this under raps so that all one does is build one's own technology to get closer and closer to cyber warfare….I am interested in holding countries responsible for the behavior of their entities. And I think it's a much more responsible course in the long-run if you have American policymakers heavily engaged with their counterparts in other countries, driving toward international treaties and agreements which prevent cyber intrusions which could result one day, if left unaddressed, a cyber war? [42]

Although Admiral Blair acknowledged the Senator's remarks, he diverted the language from "international treaties or agreements" to a "code of conduct" – presumably less binding language. Admiral Blair's exact response was "I agree that if we could develop some sort of a code of conduct an approach that the major nations agreed on to cyber space….And it [code of conduct] would apply some regulation to these [cyber] activities more at the source than having to deal with it the way we do now."[43]

Presently, no international laws specifically address the issue of cyber warfare; however, the Law of Armed Conflict (LOAC) can be applied to determine whether cyber warfare (i.e. attack) is criminal as recognized by the international community. In 2009, Major Schaap concluded that cyber attack is generally viewed as acceptable (i.e., non-criminal) in accordance with the LOAC principles of military necessity, distinction, proportionality, unnecessary suffering, perfidy, and neutrality.[44] Of course, each principle would be assessed individually given the relative circumstances of the belligerent cyber event.

For example, the "international law community appears to be coalescing around the general concept that use of the Internet to conduct cross-border cyber attacks violates the principle of neutrality."[45] According to Jeffrey Kelsey, for a state actor to remain neutral in a cyber conflict, that nation must refrain from assisting either side of the conflict, must not originate the attack, and must take action to prevent a cyber attack from transiting its cyber domain[46] – a difficult task to say the least. And, a state that takes no action against actors using its territory for cyber attack risks losing its neutral status. Lawrence Greenberg went further to suggest "a belligerent (actor) violates neutrality law when it launches a cyber attack that crosses the Internet nodes of a neutral state." The International Telecommunications Union (ITU) took a tougher position and cited that "cyber attacks could be treated as acts of war and be brought within the scope of arms control or the Law of Armed Conflict."[47]

In 2007, Duncan Hollis argued for a new legal framework for cyberspace; an international law for information operations (ILIO). "Existing rules have little to say about the non-state actors that will be at the center of future conflicts…the technology is mostly inexpensive, easy-to-use, and capable of deployment from virtually anywhere."[48] Hollis identified four substantial flaws toward the existing "law by analogy" approach for cyberspace. First, there are translation problems extending existing rules to cyberspace with regard to armed conflict. Second, the majority of language extending existing rules to cyberspace focuses on state-versus-state conflict, when recent history suggests irregular warfare to be more popular in cyberspace. Third, absent *lex specialis*,[49] conflict in cyberspace applies to multiple and overlapping legal regimes. Fourth, existing rules focus on restrictions for cyber warfare rather than include potential benefits such as limited physical and collateral damage.[50] At present, no international law exists (nor pressure toward its establishment) despite Hollis' assessment that "devising a new legal framework – may offer the most effective response to the challenges of regulating cyberspace conflicts."[51]

With respect to the 2008 cyber attacks against Georgia, Hollis' assertions received support from the NATO-accredited Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia. The center concluded "it is highly problematic to apply the Law of Armed Conflict to the Georgian cyber attacks – the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect."[52] Meanwhile, the debate continues.

Rules of engagement are not internationally formed or accepted treaties, laws or conventions, but they may provide self-policing, unilateral guidelines for operation in cyberspace (or within other domains). If made public, they may help establish shared guidelines with other state and non-state actors. Whether a state restricts its actions to the ROEs is another matter. In 2002, the U.S. President signed the National Security Presidential Directive (NSPD) 16, "which called for a national policy on the rules of engagement for using cyber warfare as a weapon."[53] The NSPD also notes the U.S. government reserves the right to respond as necessary if the United States comes under cyber attack, and that response could employ cyber weapons.[54]

Like ROEs, cooperative operations provide activities acceptable in a multilateral manner, and thus may provide clarity beyond the mere publishing of ROEs. Over time, operations in cyberspace provide accepted examples from which rules can be formed, whether formally (i.e., laws, conventions, treaties) or informally.

According to John Lynch, Deputy Chief for Computer Crime at the Department of Justice (DOJ), the DOJ has been working with Romanian law enforcement officials to combat the threat of organized crime groups stealing hundreds of millions of dollars from the U.S. economy. In April 2008, the U.S. Attorney General announced the Law Enforcement Strategy to Combat International Organized Crime, citing "cybercrime operations efforts with foreign law enforcement agencies [which] specifically addresses the threats these groups pose in cyberspace." The strategy builds on DOJ's cooperation with the G8, Interpol and the Council of Europe, which facilitates operations with other foreign nations. Given that suspected state-sponsored cyber crime is pushed to the DOJ as a law enforcement issue, it is fortuitous that existing statutes permit law enforcement officials to request search warrants in order to obtain evidence from service providers, for example. While changes to U.S. Codes for computer crimes are enacted – some as recently as August 2008 – these statutes are purposefully kept broad to mitigate the slowness of the process to build laws associated with the velocity and variety of cyberspace.[55]

Cyber crimes are just one element of the triad of cyberspace events (i.e., legitimate, criminal, and illegitimate). In 2008, allies of the North Atlantic Treaty Organization (NATO) signed an agreement to fund a center in Tallinn, Estonia, to boost defenses against cyber attacks. Defense chiefs from Estonia, Latvia, Lithuania, Germany, Italy, Spain and Slovakia signed an agreement to staff and fund the center, while the United States noticeably joined the project only as an observer.[56] In October 2008, China reportedly started engaging with regional states through the Shanghai Cooperation Organization to help shape the legal framework and rules of engagement for cyber warfare.[57] The Obama administration is now studying how laws of war and international obligations need to be reworked to account for cyber attacks.[58]

Cyber Attacks on Georgia

In the summer of 2008, Georgia came under cyber attack, likely by Russia. While the debate continues as to whether the Russian government originated, sponsored, or served as a neutral party in the attack, analysis of the events continue to provide a case study for framing the debate on international rules for cyber warfare. Such analysis is enhanced by considering the context of the attacks against Georgia in relation to other recent cyber warfare events. They are:

- April to May 2007: Websites of Estonia's parliament, banks, ministries, newspapers and broadcasters were shut down by hackers. Estonia accused Russia of conducting a cyber war in retaliation for a decision to move a Soviet-era war memorial.[59]

- June-July 2008: Hundreds of government and corporate websites in Lithuania were hacked, and some were covered in digital Soviet-era graffiti, implicating Russian nationalist hackers.[60]

- August 2008: Cyber attackers hijacked government and commercial websites in Georgia during a military conflict with Russia.[61]
- January 2009: Attacks shut down at least two of Kyrgyzstan's four Internet service providers during political squabbling among Russia, the ruling Kyrgyzstan party and an opposition party.[62]
- April 2009: An attack on Kazakhstan shut down a popular news Web site.[63]
- July 2009: Servers in South Korea and the United States sustained a series of attacks reportedly by North Korea.[64]

The series of events surrounding the 2008 cyber attacks against Georgia suggest that Russian government involvement was reasonable to affirm. The conventional ground war, which commenced on 8 August, lasted five days, left hundreds of people dead, crushed the Georgian army, and left Abkhazia and South Ossetia – Georgian territory – in Russian occupation. And, the non-conventional cyber attacks disrupted Georgian communications by disabling 20 websites for more than a week.[65]

Three weeks prior to the ground war, on 19 July, unidentified entities used a U.S.-based, commercial IP address to launch a distributed denial of service attack (DDoS) against the Georgian President's website. The malware was identified as a "MachBot" DDoS controller written in Russian and commonly used by Russian hackers.[66]

During the evening of 7 August, one day before the Russian ground invasion, Georgian governmental websites came under further cyber attack.[67] On 8 August, a larger number of Georgian governmental, bank (National Bank of Georgia)[68] and media websites were attacked by a larger wave of DDoS attacks and defaced.[69] The owner of TSHost, a U.S.-incorporated company, who happened to be visiting Georgia at the time, offered to help reconstitute Georgian internet capabilities. One day later, the Georgian government transferred key websites, including those of the President and Ministry of Defense (two of the attacked sites) to servers in the United States.[70] Servers in Poland and

Estonia were also used to host other Georgian Internet assets.[71] By 10 August, most of Georgian governmental websites were shut down by the apparent DDoS attacks[72] and the "Georgian government found itself cyber-locked, barely able to communicate on the Internet."[73]

Post event analysis of the cyber attacks revealed several interesting results. The findings of Project Grey Goose – a voluntary compilation of more than 100 Internet security members from organizations as diverse as Microsoft, Oracle, the Defense Intelligence Agency (DIA), SAIC, the Department of Homeland Security (DHS) and Lexis-Nexus – showed no direct link with the Russian government; however the assault was coordinated through a Russian on-line forum prepared with target lists and Georgian web site vulnerabilities before the conventional war started. The on-line forum *Xaker.ru* encouraged pro-Russian hackers to join a private, password-protected forum called *StopGeorgia.ru*. Within this forum, members were provided targets lists of Georgian websites with associated vulnerabilities, exploitation methods, and the procedures to render them inaccessible. "The level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government and or military" according to Jeff Carr, a Project Grey Goose principle investigator. The investigation also revealed evidence contradictory to a DDoS attack. According to Billy Rios, a Grey Goose investigator, the "benchmark" feature of MySQL (a software suite used to manage back end databases) was manipulated to send bogus database queries which in effect overwhelmed the web servers, making the websites they hosted inaccessible. Previously, investigations suggested an army of disparate computers querying the website caused the servers to crash. Rios further elaborated that the event "indicate[d] that all the information from the attacked systems was most likely already compromised and pilfered before the injection point was posted"[74] showing premeditation and coordination, and possible Russian government collusion.

In contrast to manipulating Microsoft Corporation MySQL software, the U.S. Cyber Consequences Unit (CCU) reported that the hackers coordinated their "botnet" attacks against Georgia on Twitter and Facebook, two U.S.-based social networking sites.[75] The CCU identified the source of the "botnet" attacks (ordinary computers hijacked by viruses to perform such attacks without their owner's knowledge[76]) to 10 websites registered in Russia and Turkey, which were previously used by Russian cyber crime groups. In typical DDoS fashion, the commandeered computers attempted to access the targeted websites simultaneously, thus rendering them inaccessible. Once the attacks occurred, fledgling attackers started collaborating on the forums – including Twitter and Facebook – exchanging attack codes, sharing target lists and recruiting others to join.[77]

According to the CCU Chief Technical Officer, John Bumgarner, "taking out communications systems at the onset of an attack is standard military practice."[78] The denial-of-service attacks were accomplished with precision and discipline, according to Scott Borg, co-author of the CCU report. While Russian military direction is still uncertain, the military and the attackers exchanged a significant amount of information on message boards.[79]

While the target and intent of the cyber attacks against Georgia were clear, attribution still remains elusive. Shortly after the attack, the *Los Angeles Times* reported no clear Russian military involvement, only that the originating Russian servers were associated with organized crime groups and the perpetrators may have been nationalists.[80] A week after this report, another news agency pondered official Russian involvement or that of "rogue hackers supportive of the South Ossetian cause."[81] Two seasons later, other labels of "cyber criminal, cyber citizen-mobs, and self-styled cyber militia" were used to characterize the attackers. No matter what labels were used, there remains a "growing trend of cyber conflict between nations and ad-hoc assemblages."[82]

Despite the lack of evidence against Russian government direction of the cyber attacks against Georgia, the timing of the main thrust – just hours after the conventional war began – suggests the Russian government may have coordinated with the cyber attackers. Despite the accusations, Yevgeniy Khorishko, a Russian Embassy spokesman in Washington stated "Russian officials and the Russian military had nothing to do with the cyber attacks on the Georgian Web sites."[83]

While the attacks were occurring and afterward, the Georgian government protested, but to no avail. There was no formal avenue to appeal – the existing treaties and defense pacts obligate no parties to perform a cyber or reciprocal counter-attack.

Strategic Impact to the United States

First and foremost, the cyber attacks against Georgia represent a strategic challenge to U.S. national security. In May 2009, President Obama characterized the cyber threat as "one of the most serious economic and national-security challenges we face as a nation." According to William Lynn, Deputy Secretary of Defense (DepSecDef) the "cyber threat to the Department of Defense represents an unprecedented challenge to our national security by virtue of its source, its speed and its scope." The DepSecDef further elaborated in the June 2009 speech that criminal groups and individual hackers were building global capabilities and then selling their services to the highest bidder, becoming in effect "cyber mercenaries."[84] In May 2009, several thousand U.S. military computers became infected with malware, intentionally placed by an adversary. The event, characterized as an "attack," forced military personnel to discontinue use of external memory devices and thumb drives – a drastic change from existing protocols.

The anonymity and efficiency of cyber warfare help promote its use. According to Brigadier General Mark Schissler, USAF Director for Cyber Operations, "the ability to attack an organization or even a nation surreptitiously is precisely what makes cyber warfare so dangerous and attractive." General Schissler continued to suggest the exponential increase in cyber warfare activity will make it more difficult to secure U.S. networks. "Cyberspace is one of the most asymmetric approaches to warfare" according to Schissler, who added, military officers include this type of warfare in defensive and offensive plans.[85]

The United States critical infrastructure may be increasingly vulnerable to cyber attack despite defense expenditures. The DepSecDef noted that DoD is spending billions of dollars annually to protect and defend its networks proactively, but the U.S. infrastructure remains vulnerable to attack. Representative Yvette Clarke stated that "because of expanding digital and computerized connections, our electric grid is now, more than ever, vulnerable to cyber and physical attacks." Nation-state and rogue nation adversaries of the United States can attack the critical infrastructure from remote locations with less cost than a conventional campaign and anonymously, cited Representative Dan Lundgren during the same Subcommittee on Emerging Threats, Cyber Security and Science and Technology hearings in July 2009.[86] But the risk of cyber attack is not limited to the government.

Cyber defenses need to be bolstered in the commercial and private sectors as well. McAfee Incorporated published a cyber security report in November 2009 which noted that a cyber conflict between nation-states would very likely cause collateral damage to private sector resources.[87] General Schissler earlier insisted that government, academia and businesses all share the same risks, especially if they are "unwilling to cooperate and collaborate" on cyber issues. He further stated the need to be creative in this cooperation.[88] In July 2009, General Robert Kehler, Commander Air Force Space Command, characterized cyber warfare as that which occurs in an urban environment citing the variety and density of legitimate and illegitimate actors. Critical to an effective U.S. approach is to organize with the "appropriate authorities to behave in cyberspace the right way" according to General Kehler.[89]

To mitigate the risk of "a growing array of cyber threats and vulnerabilities," in June 2009, the Secretary of Defense created U.S. Cyber Command (USCYBERCOM) as a subordinate unified command under USSTRATCOM. Mr. Gates stated "to address this risk effectively and to secure freedom of action in cyberspace, the DoD requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations." He further elaborated on the need to collaborate across departments and nations. "[T]his command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners" according to Gates.[90]

While the United States spends vast amounts of money on defensive measures, other countries including Russia and China continue to develop their offensive cyber capabilities. Russia's armed forces in collaboration with academia and the information technology sector have developed a cyber warfare doctrine[91] with much of the attention focused on offensive cyber warfare capabilities.[92] According to the doctrine, Russia's cyber arm is to be employed as a force multiplier, in effect serving to compliment other forms of military power, including conventional and irregular warfare. The primary target of the cyber offensive is the opponent's critical infrastructure including the financial market, telecommunications networks (military and civilian) all of which is to be carried out prior to initiation of conventional force on force warfare.[93] According to the U.S. Cyber Consequences Unit, someone on the Russian side exercised "considerable restraint" by not inflicting physical damage to Georgia's critical infrastructure through its use of cyber weapons,[94] or alternatively, the Russian military did not lead the attack. As previously stated, China's cyber warfare doctrine seeks "global electronic dominance by 2050, to include the capability to disrupt financial markets, military and civilian communications capabilities, and the electric grid prior to the initiation of a traditional military operation."[95]

Mere words will not create the change necessary to deal with this strategic challenge. The United States needs to drastically change its culture to leverage capabilities and avoid catastrophes in cyber space. According to the DepSecDef, the DoD needs to "respond rapidly, at network speed, before the networks could become compromised and ongoing operations or the lives of our military are threatened."[96] The "Pentagon must ultimately change its culture" in order to collaborate across the military, the rest of government, and commercial sectors – a necessity to ascertain and respond to any given threat.[97] Given the interconnectedness of the global telecommunications infrastructure – the medium through which most attacks will occur – this collaboration should extend beyond the U.S. borders with other nation-states and include the world's stakeholder companies.

As with the seas, the Internet and the global telecommunications infrastructure has become part of the global commons. The global commons have long been recognized as a vital U.S. interest and therefore have been improved, maintained and policed by U.S. resources. According to Richard Mereand of the National Security Watch, "the United States, as a major beneficiary of all that cyberspace has to offer, should take the lead – vigorously and without delay" in "maintaining a free and open Internet."[98] But, maintenance of the global commons is not entirely up to the United States. International cooperative efforts, even those short of official agreements are needed to ensure a holistic approach is achieved. In a 2009 interview with National Public Radio, General Chilton, USSTRATCOM Commander, suggested the need to improve military dialogue with other nations in order to deal with international threats. "Threats in cyberspace are being taken seriously by all governments around the world…we already [do] have dialogues with…Australia, the United Kingdom, [and] France,"[99] stated General Chilton. The NATO-generated Cooperative Cyber Defense Center of Excellence, headquartered in Tallinn, Estonia, could serve as an example of solidifying roles and responsibilities across national boundaries for securing the global infrastructure.[100]

Preventing other nation or non-nation-state actors from disrupting the global cyberspace domain may be accomplished in a variety of ways; however, deterrence is likely not one. During the Cold War, nuclear deterrence based on mutually assured destruction had value. But in the cyberspace domain, the difficulty of determining the source of the attack eliminates a viable retaliation, thus defeating a necessary element for successful deterrence.[101] William Lynn, DepSecDef, reiterated the difficulty in attribution as it relates to deterrence, stating "deterrence is predicated on the assumption that you know the identity of your adversary, but that is rarely the case in cyberspace."[102]

Absent deterrence, internationally recognized rules could help prevent actions being perceived wrongly during cyber warfare. Lynn stated how the DoD defines the "rules of the road" will help "ensure our cyber security in the decades ahead."[103] While no international laws exist that prohibit cyber warfare operations, the application of cyber warfare has legal limitations. Under the LOAC cyber warfare operations have the potential of constituting an illegal use of force. For example, in some scenarios the principle of neutrality may present ambiguities. The U.S.-incorporated company TSHost inadvertently broke the position of neutrality by its actions to transfer Georgian governmental web servers to those in the United States. Further complicating the matter, the U.S. declared no official stance in the Georgia-Russian conflict. If the

United States "linked its cyber support to its overall humanitarian aid effort it would have signaled that U.S. Internet support to Georgia was for humanitarian purposes, and therefore not in violation of any Hague Conventions."[104] The position of neutrality is also questionable when an aggressor uses a third party's cyber domain to launch or otherwise enable an attack against an adversary. A third party who inadvertently allows a belligerent to use its cyber domain to launch or otherwise enable an attack potentially breaks its position of neutrality as well. A void of international rules surrounding a cyber "Pearl Harbor" may cause the creation of overly restrictive and reactionary regulations rather than ones that are purposefully and unemotionally developed with more rational minds.[105]

Part of the dilemma with current international laws is that the line between cyber crime and cyber war is blurred. According to the McAfee cyber security report, the recent attacks against Georgia showed that "nation-states have already demonstrated that they are willing to tolerate, encourage or even direct criminal organizations and private citizens to attack enemy targets." Were these acts against Georgia's Internet resources an act of war or a crime?[106]

It may be beneficial for the U.S. government to "clearly demarcate its cyber relationship vis-à-vis cyber belligerents" given that "current international laws are ambiguous and ill-suited to define contemporary cyber rules of engagement." Even though the U.S. government did not officially sanction the actions of TSHost and Google to support Georgia during the second wave of DDoS attacks – Internationally recognized as cyber war – Russia and other parties could have viewed the U.S. companies' actions as offensive and launched attacks against those portions of the U.S. commercial infrastructure.[107] The attacks the Pentagon refused to take a position whether the cyber attacks against Georgia were acts of war.[108] In light of these risks and ambiguities, U.S. policymakers should consider "invigorating multinational efforts to clarify the terms and conditions of cyber neutrality" and "the wisdom of continuing a cyber strategy that appears to rely heavily on the loosely controlled actions of private industry."[109]

An arms control treaty would be another example of internationally recognized rules for cyberspace, however, the United States appeared reluctant to move toward that end. Shortly before the cyber attacks on Georgia, the Russian government "called for a ban on cyber attacks as part of arms control deals, but the U.S. government refused" to take part in any discussions.[110] In the fall of 2009, a Russian delegation led by General Vladislav Sherstyuk met with U.S. DoS, DoD, DHS, and National Security Council officials to "limit the development and military use of cyber weapons," but the results of the meetings were not available. Some argue that cyber arms control treaties would only cause the weapons development to move underground causing greater uncertainty among adversaries.[111] Certainly, developing treaties is complicated – the executive branch leads foreign policy development, but the Congress regulates foreign commerce and the Senate must agree to any treaties the United States may consider.[112]

Short of developing treaties for cyberspace, countries could form alliances or agreements to help guide warfare. The DepSecDef stated that international cooperation is a logical step to defend against cyber attacks, the majority of which originate overseas. Also confronting the complexities of national sovereignty and international law as it relates to cyber warfare is not something that only one country could tackle, according to Lynn.[113] During the 2009 meeting with U.S. government officials General Sherstyuk also discussed international cooperation for investigating cyber attacks. Given the broad publicity of recent cyber attacks, there is growing concern that terrorists will begin to use this form of warfare more frequently.[114]

While it appears the U.S. government remains reluctant to enter into any cyber warfare treaties, unilateral cyber assaults to preempt attacks is an issue under debate. Arguably, belligerent actions in cyberspace are enabled through actions in other domains and vice versa, so it seems reasonable for a potential victim of an attack to counter-attack in whatever domain effectively stops the attack and mitigates the damage. Three recent terrorist attacks or attempted attacks against the United States were facilitated through belligerent actors' use of the Internet. The Nigerian Umar Farouk Abdulmutallab who attempted to down Delta Flight 253 on Christmas 2009 viewed a blog and website of the radical cleric al-Awlaki for "counseling and companionship." The five young Americans recently arrested by the FBI in New York for planning a terrorist attack contacted militant groups over the Internet, and U.S. Army Major Nidal Malik Hasan, who killed 14 soldiers in November 2009, used the Internet to communicate with the radical cleric Awlaki. In a recent House Armed Services Committee meeting the question was posed whether the United States should launch preemptive cyber attacks against those Internet assets used to facilitate such terrorist attacks against the United States.[115]

A preemptive attack against a potential belligerent actor would require an offensive capability; however, most countries like the United States are reluctant to reveal their true offensive capabilities. When asked about U.S. offensive cyber capabilities in a 2009 interview, General Chilton, although reluctant to elaborate stated "it's an area that we're focused on…because we recognize that a good defense also incorporates elements of an offensive capability."[116] Some argue developing these new kinds of weapons is a dangerous practice. The "ability to disable a nation's infrastructure and cripple its military defenses without firing a shot sounds appealing, [however] condoning and launching cyber warfare is a slippery slope." The United States should carefully consider second and third order effects before unleashing these new weapons.[117]

Conclusions

The United States is more vulnerable to cyber attack than ever before; it relies on the Internet for communications, commerce, and governance as well as computer-automated systems for infrastructure control. Such interdependence of sector networks (i.e., financial, energy, military, and telecommunications) complicates state-supported defensive operations and increase network weaknesses. The volume, velocity and variety of Internet activity further complicate defensive strategies. While a single cyber attack launched by a belligerent state or non-state actor may not disrupt all U.S. critical infrastructures, significant damage can result. Illegitimate and criminal cyber activities cost the United States significant amounts, estimated in the billions of dollars annually in terms of theft, destruction and defensive measures.

Cyberspace continues to become more complex. In addition to the difficulties in attributing cyber attacks, state and non-state actors continue to grow and increase their cyber warfare capabilities. China, Russia, North Korea, and Iran – non-allies of the United States – have cyber warfare capabilities, and non-state actor belligerent activities are growing almost exponentially. Recent attacks against Georgia and Estonia show a pattern of premeditation and coordination not previously witnessed.

Few international rules exist that specifically address accepted norms in cyberspace and those that do are contradictory. Short of internationally accepted rules, cyber warfare is judged mostly through analogy with existing norms. Computer network exploitation appears to remain a legitimate form of cyber intelligence, surveillance and reconnaissance according to the articles of the UN. While possibly an act of aggression, according to the UN Charter, CNA used in accordance with the LOAC principles of military necessity, distinction, proportionality, unnecessary suffering, perfidy, and neutrality are arguably legal. Determining CNA's congruence with the LOAC principles is subjective, however, the Council of Europe Convention on Cybercrime's Articles 2, 4 and 5 cite descriptions of criminal offenses specifically associated with CNE and CNA.

The argument for developing internationally-accepted cyber warfare rules appears to be gaining momentum within U.S. government circles. Although DoS officials opted away from developing a cyberspace arms treaty with Russia, and the Chairman of the Senate Select Committee on Intelligence pressed for treaties, the DNI, Admiral Blair, preferred a "code of conduct."

The 2008 cyber attacks against Georgia exemplify the complexities of cyber warfare. While Russian government involvement whether through collaboration or incitement was likely, attribution of the cyber attacks remains elusive. The collection of hactivists (i.e., hacker activists) formed via the Internet are more likely to be considered criminals than warriors, but current international laws call for investigation and prosecution by the host nation – Russian government – an unlikely administrator of justice. The TSHost's actions to mitigate damage to Georgian government communications by hosting their servers in U.S. networks arguably broke the U.S. government's position of neutrality during this conflict and potentially opened U.S. infrastructure to attack. The fact that U.S.-hosted social networking sites were used to coordinate attacks against Georgia could also jeopardize the U.S. government's position of neutrality. Finally, no published rules provide clarity regarding a proportional counter-attack if one was waged by Georgia. For example, would it have been appropriate for Georgia to attack hosts in Russia and Turkey from which the DDoS attacks were launched?

Cyber warfare may represent a greater strategic challenge than opportunity to U.S. national security. As a form of asymmetric warfare, cyber attack is increasingly popular given its anonymity of source, quickness in operation, relative simplicity in accomplishment, and breadth across an array of sectors. As a hegemonic power, the United States will naturally attract belligerent actors seeking asymmetric means to achieve their objectives. With DoD network security spending greater than a billion dollars annually, the cost to the U.S. government could be overwhelming by itself, especially given the current economic environment. Despite public awareness of network and infrastructure vulnerabilities, the U.S. government, commercial and private sectors increasingly move toward a greater information systems reliance creating greater interdependencies between systems and networks. A network is only secure as its weakest link. China, Russia, North Korea and Iran, some with published cyber warfare doctrines, seek capabilities to degrade and destroy critical national infrastructures. And, like the seas, the United States will feel the need to maintain "freedom of navigation" in cyberspace as a primary beneficiary of its existence. Such issues represent significant strategic challenges to U.S. national security.

Recommendation

Given the significant strategic challenge that cyber warfare poses on U.S. national security, the United States should seek to establish rules to clarify accepted norms. The existence of cyber warfare rules will identify thresholds for legitimate and illegitimate actions in cyberspace, mitigate collateral damage during times of war, and help hold belligerent actors accountable. The safety and security of U.S. citizens and property are of vital interest to the United States, therefore the government has an obligation to protect and respond to attacks against these resources in all domains including cyberspace. The flow of commerce much of which now occurs in cyberspace (e.g., financial transactions) is arguably also of vital interest to the United States, and therefore must be protected. Since cyber attacks can harm lives, property and commerce, the U.S. government should develop clear rules for cyber warfare and a synchronized U.S. government response to mitigate further destruction, fratricide, and hold the belligerent actor accountable. Therefore the United States and the international community need rules to identify accepted norms and provide governance to help hold belligerent actors accountable and deter would be assailants.

The United States should develop these cyber warfare rules multilaterally. This approach will be difficult to accomplish, but consensus achieved through participation will provide the best result – rules by which most nation-states abide. Even though non-state belligerent actors would likely not participate in the development of cyber warfare rules, state actor involvement is a necessary component of non-state actor prosecution. Gaining consensus among the international community on cyber warfare rules will be difficult to achieve. Even if a formalized international policy is not achieved, the dialogue at an international scale will help clarify thresholds and appropriate responses that will be accepted by the U.S. government and international community.

Manifestation of these rules should be accomplished in a holistic manner. For example, the United States should use a variety of means to develop and maintain cyber warfare rules to include treaties, laws, multinational operations, directives, and policies. The means through which cyber warfare rules are documented will extend beyond the contemporary model of interpretation through analogy, although in some cases interpretation through analogy may suffice.

Prudens Futuri

Endnotes

Preface

1. Reagan, Ronald. *National Security Decision Directive 130*. Washington, D.C.: The White House, 6 March 1984. Available from http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm (accessed 23 December 2005.)

2. Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as "Instruments of Power." It further states that Information, while not an instrument of power, forms a backdrop as all activity has an informational backdrop.

3. Neilson, Robert E. and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* (Autumn 1999): 40.

Section One: Information Effects in the Cognitive Dimension

Introduction

1. William Rosenau, "Waging the 'War of Ideas,'" in *The McGraw-Hill Homeland Security Handboo*k, ed. David G. Kamien (New York: McGraw-Hill, 2005): 1132.

Narratives of Empowerment: A Cultural Analysis of Hezbollah

1. Al-Manar TV, "Sayyed Nasrallah: We Will Defeat Enemy, Change Region's Face," January 15, 2010, http://www.almanar.com.lb/newssite/NewsDetails.aspx?id=119979&language=en (accessed February 15, 2010).

2. Various sources attribute this statement to different individuals, and there is no consensus on its exact interpretation. Several sources attribute it to Pierre Gemayel, founder of the Phalange Party in Lebanon. A few interpretations include: there are so many outside powers dabbling in Lebanese affairs that no one power will ever completely dominate its affairs; the weakness of the central government (to include the military) allows for the efficient running of the state through powerful, unofficial forces, such as powerful families and community leaders; Lebanon's initial ability to not become heavily embroiled in the Arab-Israeli conflict, and be seen as a significant force in the debate, left it free to look out for its own interests; The weakness of Lebanon's armed forces allowed its democratic society to develop without the threat of a military coup. For various interpretations, see, for example: Robert I. Rotberg, ed., *State Failure and State Weakness in a Time of Terro*r (Washington, D.C.: Brookings

Institution Press, 2003); Fawaz A. Gerges, *Journey of the Jihadist: Inside Muslim Militancy* (Orlando, Florida: Harcourt, 2006); Tareq Y. Ismael and Jacqueline S. Ismael, ed., Politics and Government in the Middle East and North Africa (Gainesville, Florida: University Presses of Florida, 1991).

3. Thomas Collelo, ed., *Lebanon: A Country Study* (Washington, D.C.: Library of Congress, Federal Research Division, 1989), 20.

4. Amal Saad-Ghorayeb, *Hizbu'llah: Politics and Religion* (London: Pluto Press, 2002), 7-15.

5. Alternative here implies alternative to prominent Western conceptions of world order.

6. Jiyul Kim, *Cultural Dimensions of Strategy and Policy*, (Carlisle Barracks, PA: Strategic Studies Institute, 2009), 6.

7. See Kim, vii, "Cultural proficiency at the policy and strategic levels means the ability to consider history, values, ideology, politics, religion, and other cultural dimensions and assess their potential effect on policy and strategy."

8. The notions of dynamism and negotiation are recurring themes in the field of cultural studies and anthropology. Specifically, as they apply to the strategic level, see Sheila Miyoshi Jager, *On the Uses of Cultural Knowledge*, (Carlisle Barracks, PA: Strategic Studies Institute, 2007), 9. Here, she states "Cultural knowledge at this (strategy) level thus requires a complex understanding of culture as a dynamic entity, an on-going process of negotiation between past and present. Far from reproducing the values and beliefs of a static and unchanging culture, extremist groups like al-Qai'da have appropriated and reinterpreted Islamic texts, belief-systems, and traditions to justify their own radical ideology; in other words, they have used culture instrumentally. Cultural knowledge as applied to the level of strategy must be concerned with the dynamic understanding of culture and how different Islamic radicals emphasize different aspects of their historical past and traditions to legitimize their political actions and behavior in the present." Note, also, for example, the statement "systems of signification are subject to contestation and renegotiation by people who are both constructed by and also agents in their world…" from Lisa Wedeen, *Ambiguities of Domination: Politics, Rhetoric, and Symbols in Contemporary Syria* (Chicago: The University of Chicago Press, 1999), 25.

9. Kim, "Cultural Dimensions of Strategy and Policy," 14.

10. Nicholas Noe, ed., "Victory: May 26, 2000," trans. Ellen Khouri, in *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah* (New York: Verso, 2007), 237.

11. Middle East Weekly Reporter, no. 3664 (July 27, 1993): 8, quoted in Judith Palmer Harik, *Hezbollah: The Changing Face of Terrorism* (New York: I.B. Tauris, 2004), 115.

12. Augustus Richard Norton, *Hezbollah: A Short History* (Princeton: Princeton University Press, 2007), 84.

13. Noe, Nicholas, ed. “Elegy for Sayyed ‘Abbas Mussawi: February 18, 1992,” trans. Ellen Khouri, in *Voice of Hezbollah: The Statements of Sayed Hassan Nasrallah* (New York: Verso, 2007), 52.

14. For the story of Karbala, see, for example David Pinault, *The Shiites: Ritual and Popular Piety in a Muslim Community* (New York: St. Martin’s Press, 1992), 4-6.

15. Ibid., 4-6, 39-40.

16. Norton, *Hezbolla*h, 66.

17. Fouad Ajami, *The Vanished Imam* (Ithaca, NY: Cornell University Press, 1986), 25.

18. Ibid., 141-144.

19. Ibid., 144.

20. Lara Deeb, *An Enchanted Modern: Gender and Public Piety in Shi’i Lebanon* (Princeton: Princeton University Press, 2006), 138.

21. Norton, *Hezbollah*, 67.

22. Ibid., 66.

23. Ibid., 58.

24. Ibid., 140.

25. Deeb, *An Enchanted Modern: Gender and Public Piety in Shi’i Lebanon*, 90.

26. Matthew Levitt, Policy Watch#1202 “Shutting Hizballah’s Construction Jihad,” Washington Institute for Near East Policy, Policy Watch, February 20, 2007, http://www.washingtoninstitute.org/templateC05.php?CID=2571 (accessed February 13, 2010).

27. Ibid., Harik, *Hezbollah: The Changing Face of Terrorism*, 84.

28. Harik, *Hezbollah: The Changing Face of Terrorism*, 92.

29. Ibid.

30. Norton, *Hezbollah*,108.

31. Deeb, *An Enchanted Modern: Gender and Public Piety in Shi’i Lebano*n, 52.

32. Ibid., 57.

33. Ibid.

34. Here, the concept of the ‘cult of personality’ is based on Lisa Wedeen, *Ambiguities of Domination: Politics, Rhetoric, and Symbols in Contemporary Syria*, (Chicago: The University of Chicago Press, 1999). For example, she speaks of the power of images as follows: “Asad’s image as the transcendent leader, his gaze monitoring the actions of Syrian citizens, by signifying the anonymous, panoptic security forces – in the words of one Syrian, Asad’s “eyes and ears” – allows the police to be “present” even when one knows they are not,” 147. The term ubiquitous also comes from this page: “the image of the ubiquitous, all-seeing Asad…”

35. Noe, *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, 237.

36. Wedeen, *Ambiguities of Domination: Politics, Rhetoric, and Symbols in Contemporary Syria*, 147.

37. Nicholas Noe, ed. "Interview with New TV: August 27, 2006," trans. Ellen Khouri, in *Voice of Hezbollah: The Statements of Sayed Hassan Nasrallah* (New York: Verso, 2007), 385.

38. Augustus Richard Norton, *Amal and the Shi'a: Struggle for the Soul of Lebanon* (Austin: The University of Texas Press, 1987), 181.

39. Sheila Miyoshi Jager, *The Politics of Identity: History, Nationalism, and the Prospect for Peace in Post-Cold War East Asia*, (Carlisle Barracks, PA: Strategic Studies Institute 2007), 15.

40. Noe, *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, 233.

41. Ibid., 241.

42. Ibid., 239.

43. "Full speech of H. E. Sayyed Nasrallah: Hizbullah´s New Political Manifesto … We Want Lebanon Strong & United," Islamic Resistance in Lebanon, November 30, 2009, http://english.moqawama.org/essaydetails.php?eid=9632&cid=231 (accessed February 10, 2010).

44. Noe, *Voice of Hezbollah: The Statements of Sayyed Hassan Nasrallah*, 237.

45. Ibid.

46. Ibid.

47. Ibid.

48. UN Security Council, Resolution 1701, *The Situation in the Middle East*, 11 August 2006.

49. Ibid., p3, Para. 8

50. Sami G. Hajjar, *Hizballah: Terrorism, National Liberation, or Menace?*, (Carlisle Barracks, PA: Strategic Studies Institute 2002), 10-11. "Hezbollah adheres to a Manichean notion of the world as being divided between oppressors (mustakbirun) and oppressed (mustad'ifin). The relationship between the two groups is inherently antagonistic-a conflict between good and evil, right and wrong…The conflicting relationship cannot be resolved by some mechanism leading to a win-win situation. Rather, "the meek shall inherit the earth," not in the life after, but here and now through their activism."

51. Casey L. Addis, "Lebanon: Background and U.S. Relations," *Congressional Research Service* (November 30, 2009), 20-21.

52. UN Security Council Resolution 1701, p2, para 6 "calls on the international community to take immediate steps to extend its financial and humanitarian assistance to the Lebanese people." See also Addis, 6 which characterizes

economic aid from the international community as an effort to assist the Lebanese government against Iran and Hezbollah in a struggle for the "hearts and minds of many Lebanese citizens who had lost homes and businesses as a result of the [July 2006] conflict."

53. U.S. Central Command, "Lebanon," http://www.centcom.mil/en/countries/aor/lebanon/ (accessed February 17, 2010) reads: "Stabilizing Lebanon requires ending Syria and Iran's illegal support to Hizballah, building the capabilities of the Lebanese Armed Forces, and assisting the Lebanese government in developing a comprehensive national defense strategy through which the government can exercise its sovereignty, free of interventions from Hizballah, Syria, and Iran."

54. Steven Simon and Jonathan Stevenson, "Disarming Hezbollah: Advancing Regional Stability," January 11, 2010, *Foreign Affairs*, http://www.foreignaffairs.com/articles/65921/steven-simon-and-jonathan-stevenson/disarming-hezbollah (accessed February 10, 2010) reads, "[T]he effort in Lebanon should be confined to back channels and implemented by mid-level U.S. officials until Hezbollah's willingness to cooperate has been established" and "the organization would be more inclined to go along with a demilitarization process involving quiet, negotiated decommissioning than one driven by grand démarches by outside powers." For discussions on approaches to disarming Hezbollah – to include potentially 'absorbing' some of its military wing into the state – see Bilal Y. Saab "Rethinking Hezbollah's Disarmament," *Middle East Policy XV*, no. 3 (Fall 2008).

55. Sami Hajjar, "The Convoluted and Diminished Lebanese Democracy," *Democracy and Security 5*, no. 3 (2009): 274. Hajjar promotes the development of the LAF in order to produce "a modern professional institution that could have a transformational impact on Lebanese public institutions and politics."

56. Aram Nerguizian, *The Lebanese Armed Forces: Challenges and Opportunities in Post-Syria Lebanon*, (Washington, DC: Center for Strategic and International Studies, 2009), 26.

57. Hajjar, "The Convoluted and Diminished Lebanese Democracy," 274. The notion of the LAF as a "model" institution is from the statement "A strong, modern, and efficiently administered LA could very well become a model for other governmental departments and agencies to emulate."

58. The idea of Hezbollah holding the Lebanese government hostage is from Zeina Karam, "Lebanese PM Warns of Israeli Threats, Says It Will Support Hezbollah in Event of New War," *Associated Press*, February 10, 2010 (accessed on February 16, 2010), which includes the following statement from Israel's Foreign Minister "As prime minister, he's (Lebanese PM) simply a hostage of Hezbollah, which has veto power in his Cabinet…" http://hosted.ap.org/dynamic/stories/M/ML_LEBANON_ISRAEL?SITE=WIJAN&SECTION=HOME&TEMPLATE=DEFAULT (accessed February 13, 2010)

The Role of Religion in National Security Policy Since 9/11

1. I wish to express my deep gratitude for the contributions of Dr. Tami Davis Biddle. Her global perspective, national security insights, and sensitivity to perceptions over religious issues provided critical context and caution as I wrote this manuscript. Dr. Biddle is Professor of National Security Strategy and Military History, U.S. Army War College, Carlisle Barracks, Pennsylvania.

   National security policy rightly addresses both internal and external threats that impact the nation's enduring beliefs, ethics, and values; the national interests; and the grand strategy of the nation state. This paper largely bypasses discussion of internal threats, in order to focus on external threats and the role of religion in visualizing and meeting those threats.

2. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, Oxford Paperbacks, 1971), 84.

3. Carl von Clausewitz, *On War*, ed. and trans. Michael and Peter Paret (Princeton, NJ: Princeton University Press, 1976). See Clausewitz, 89. He conceives of war at its most basic level as "primordial violence, hatred, and enmity." To empower such violent conflict, "the passions that are to be kindled in war must already be inherent in the people." Why would one omit religion as a constitutive power within a society, especially as that power comes into play in the calculus of war?

4. The Judeo-Christian heritage participated in the West's just war tradition, which grounds war in the civil realm's responsibility to prevent harm to innocents and punish evil doers in the cause of justice. Islam possesses its own just war tradition which grounds war historically and theologically in the necessity of the struggle to defend and spread the faith. See the monumental volume, Andrew G. Bostom, ed., *The Legacy of Jihad: Islamic Holy War and the Fate of Non-Muslims*, with a foreword by Ibn Warraq (Amherst, NY: Prometheus Books, 2005). Bostom provides voluminous primary source materials translated for the English reader. For a helpful discussion of Islamic conceptions of *jus ad bellum* and *jus in bello*, see *The Islamic Law of Nations: Shaybani's Siyar*, trans. and with an introduction by Majid Khadduri (Baltimore: John Hopkins Press, 1966).

5. Adolf Köberle, *The Quest for Holiness*, trans. John C. Mattes from the 3d German ed. (Evansville, IN: Ballast Press, 1999). In his sweeping analysis, Köberle examines world religions against the frameworks of moralism, mysticism, and speculation, and their engines of will, spirit, and thought. He tracks the inevitable futility of theological synergism, which he demonstrates can finally be overcome only by a robust divine monergism which, by the declaration of acceptance and the gift of the Spirit in Christ, enables human fulfillment and sanctification. Köberle was a confessional Lutheran scholar and professor at the University of Basel.

6. Ibid., 1. Latin: "Grant us peace."

7. Federal pronouncements that would promote or proclaim the comparative value of a religion could, on the one hand, violate the First Amendment of the U.S. Constitution for internal audiences, and on the other, be inappropriate and even counterproductive for foreign audiences.

8. The frameworks espoused by Presidents Bush and Obama are discussed in detail with source citations in part III of this paper.

9. The date of 9/11 is commonly used to mark the start of persistent conflict for the United States. Equally significant is that this persistent conflict has been oriented against an adversary who defines himself chiefly in terms of religion vis-à-vis the U.S. and the West. How the U.S. and the West define the adversary is another matter.

10. By historiographers, I mean those who write on history as a phenomenon and propose a paradigmatic view of history. This does not mean that the four authors herein surveyed consider themselves, or are, primarily historiographers. Indeed, Francis Fukuyama and Samuel Huntington have used historiography as a tool for their major discipline of political science.

    I am especially indebted to Dr. Adam Francisco for his insight that a serious discussion today on the role of religion in national security policy requires handling the issues raised in Fukuyama's and Huntington's disparate treatments of religion's connection to the world of human conflict. His insight helped determine the structure of this paper. Dr. Francisco is Associate Professor of History, Concordia University Irvine, Irvine, California.

11. In only a very limited sense does part two of this paper – by way of an historical review of Islam – provide a window to past connections of religion to national security policy.

12. Alvin Toffler, *The Third Wave* (New York: William Morrow and Company, Inc., 1980).

    Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992). This book represents a substantial development beyond Fukuyama's initial investigation published as "The End of History?" *The National Interest* 16 (Summer 1989): 3-18.

    Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 1996). This book develops in detail, and asserts the validity of, the hypothesis that Huntington initially published in question form, "The Clash of Civilizations?" *Foreign Affairs* 72, no. 3 (Summer 1993): 22-49.

    Robert D. Kaplan, *The Coming Anarchy: Shattering the Dreams of the Post Cold War* (New York: Random House, 2000). Chapter One, "The Coming Anarchy," was first published in the February 1994 edition of *The Atlantic Monthly*.

13. Alvin Toffler, an American futurist, has written on patterns of societal change, to include revolutions in the fields of technology, communication, and business.

For further background on Toffler and his futurist views, see Peter Schwartz, "Shock Wave (Anti) Warrior," *Wired* 1.05, November 1993, http://www.wired.com/wired/archive/1.05/toffler.html (accessed 27 February 2010).

14. Toffler, *The Third Wav*e, chapters 11-23, 143-365.

15. Ibid., 21.

16. Ibid. In discussing First and Second Wave confluence, Toffler emphasizes battles internal to a society, although he also touches on external violence. At 39: "As the Second Wave moved across various societies it touched off a bloody, protracted war between the defenders of the agricultural past and the partisans of the industrial future. The forces of First and Second Wave collided head-on, brushing aside, often decimating, the 'primitive' peoples encountered along the way." For further discussion, see chapter 2, "The Architecture of Civilization," 37-52.

17. Ibid., 453.

18. Ibid. Quotes at 375 (similarly, at 273: "Our religious views, like our tastes, are becoming less uniform and standardized."), 26, 306, and 392.

19. Ibid., 435. "The first, heretical principle of Third Wave government is that of minority power. It holds that majority rule, the key legitimating principle of the Second Wave era, is increasingly obsolete. It is not majorities but minorities that count. And our political systems must increasingly reflect that fact."

20. Ibid., 347. Toffler terms the long-term struggle in civilization between the Second and Third Waves "the coming super-struggle." Religion will continue as a source of traditional conflict, but, more significantly for Toffler, will also be absorbed as a critical component within the larger ideological super-struggle. See Toffler, 25-34, 452-456.

21. Francis Fukuyama has written broadly on state governance, political and economic development, social order, biotechnology, and the philosophy of history. He currently serves as professor at the Paul H. Nitze School of Advanced International Studies of Johns Hopkins University, Washington, DC. For further information, consult his biography posted at the website for the Paul H. Nitze School of Advanced International Studies, http://www.sais-jhu.edu/faculty/ fukuyama/Biography.html (accessed 27 February 2010).

22. Fukuyama, *The End of History*, 55. For an overview of Fukuyama's argument, see his fine introductory chapter, "By Way of an Introduction," xi-xxiii.

Fukuyama frequently uses the word "man" in its universal and generic sense, to denote in the concrete, individual case the fullness of humanity therein presented. In the discussion which follows, I retain Fukuyama's usage of "man." In related terminology, Fukuyama also speaks of the "last man," i.e., that man who is the final manifestation of human evolution, who no longer possesses the fullness of what previously had properly belonged to humanity.

23. Ibid., chapter 1, "Our Pessimism," 3-12, in which he rejects the pessimism founded on twentieth century wars. This pessimism he regards as historically anomalous. An example of his optimism is his rejection of political realism in chapter 23, "The Unreality of 'Realism," 245-253, and chapter 24, "The Power of the Powerless," 254-265. At 254: "Realism rests on two extremely shaky foundations: an impermissible reductionism concerning the motives and behavior of human societies, and failure to address the question of History."

24. Ibid., chapter 4, "The Worldwide Liberal Revolution," 39-51, in which he documents the rise of liberal democracies worldwide across time, and chapter 5, "An Idea for a Universal History," 55-70, in which he argues for the philosophical possibility of "a meaningful pattern in the overall development of human societies generally." Fukuyama tracks a general decline of totalitarian regimes and ideologically-driven nation states.

    Fukuyama formally distinguishes liberalism from democracy. "Political liberalism can be defined simply as a rule of law that recognizes certain individual rights and freedoms from government control," 42. Fukuyama focuses on civil, religious, and political rights. "Democracy, on the other hand, is the right held universally by all citizens to have a share of political power, that is, the right of all citizens to vote and participate in politics," 43. Fukuyama notes that although liberalism and democracy do not always go together, they usually do, and his view of the end of history finds them united.

25. Ibid. When Fukuyama speaks of the end of history, he is speaking of the idea of "a coherent and directional History of mankind that will eventually lead the greater part of humanity to liberal democracy," xii. Fukuyama borrows heavily from Hegel, who viewed history as a rational process that "would come to an end with an achievement of free societies in the real world. This would, in other words, be *an end of history*. This did not mean that there would be an end to events arising out of births, deaths, and social interactions of humankind, or that there would be a cap on factual knowledge about the world. Hegel, however, had defined history as the progress of man to higher levels of rationality and freedom, and this process had a logical terminal point in the achievement of absolute self-consciousness," 64, emphasis in original.

26. Ibid., xiv. See especially chapters 6-8, at 71-108.

27. Ibid. Fukuyama anchors man's struggle for recognition is Plato's *thymos*, or spiritedness, a concept he sees embedded in many philosophical systems. For example, Hegel's "first man" desires "to be recognized as a *man*," which involves first and foremost his "ability to risk his own life," 146. Closely connected to this desire to be esteemed and valued by others is the self-reflection of being worthy of such esteem, i.e., of being better than another. This desire to be regarded as superior to others Fukuyama terms *megalothymia*, calling its opposite, the desire to be regarded as the equal of others, *isothymia*. For a discussion of how *thymos* and *megalothymia* have led to war, and societies composed of slave and victor classes, see 146-152, 181-198.

28. Ibid. Fukuyama lauds Christianity as that religion which "first introduced the concept of the equality of all men in the sight of God, and thereby conceived of a shared destiny for all the peoples of the world," 56. He also criticizes Christianity because it relegated that vision of equality and freedom to the spiritual realm, judging the religion as "untrue in certain crucial respects," 197.

29. Ibid. Fukuyama relates Hegel's critique of Christianity without dissent. "The last great slave ideology, Christianity, articulated for the slave a vision of what human freedom should be. Even though it did not provide him with a practical way out of his slavery, it permitted him to see more clearly his objective; the free and autonomous individual who is recognized for this freedom and autonomy, recognized universally and reciprocally by all men," 198. Hegel believed that Christians were guilty of perpetuating a form of self-alienation by creating the concept of God, and then subordinating their "free wills" to that God and to their temporal conditions through the retention of slave identities; see 195-197.

    This assessment of Christianity turns on the power of the "free will" to choose and act. Historic Christian confessions have embraced the concept of a will which is empowered to choose and act freely, but only after Christ has come and first made it free.

30. Ibid. See Fukuyama's discussion at 195-199; quote at 195. It should be noted that for Fukuyama, it is only that absolutist quality of religion that, like nationalism, makes itself an obstacle to liberalism: "The second cultural obstacle to democracy has to do with religion. Like nationalism, there is no inherent conflict between religion and liberal democracy, except at the point where religion ceases to be tolerant and egalitarian," 216.

31. Ibid. Fukuyama, 300-312; quote at 300, emphasis in original. Here Fukuyama follows Nietzsche. If all men are absolutely free and equal, and all recognition is universal, what is the quality of such recognition? If the last man has plenteous security and luxury, if the last man has no values compelling enough to die for, and if striving and excellence require discontent, what will the end state of humanity be? Fukuyama concludes, "Looking around contemporary America, it does not strike me that we face the problem of an excess of *megalothymia*. Those earnest young people trooping off to law and business school, who anxiously fill out their résumés in hopes of maintaining the lifestyles to which they believe themselves entitled, seem to be much more in danger of becoming the last men, rather than reviving the passions of the first man," 336.

32. Ibid. That the loss of religion would coincide with the loss of true humanity suggests that Fukuyama's anthropology, based on economic and recognition privation (or positively, on the need for economy and recognition), is inadequate. I believe Fukuyama's anthropology fails to take into account the fullness of the first man's privation. Beyond economy and recognition, man strives for love, hope, joy, reconciliation, righteousness, peace, and unending life—arguably the deliverables of religion. Unless the fullness of man participates in history,

which itself is part of the history of effects, the fusion of history cannot achieve its final and rational end. This line of thinking suggests that unless the divine substantively enters into the human race to supply what is ontologically lacking, the history of effects cannot achieve a finally satisfying end, and there can be no end of history in Fukuyama's sense. Within Christian dogma, this entrance of the divine into human flesh is the Incarnation of the Son of God. For a superb analysis of the principle of the history of effects and the fusion of history at an end, see "The Elevation of the Historicity of Understanding to the Status of a Hermeneutical Principle" in Hans-Georg Gadamer, *Truth and Method*, 2d revised ed., translation revised by Joel Weinsheimer and Donald G. Marshall (New York: Continuum, 1988), 265-307.

33. Ibid., 328. We would then "return to being first men engaged in bloody and pointless prestige battles, only this time with modern weapons."

34. Ibid., 322-327.

35. Ibid., 326-327.

36. Ibid. Fukuyama uses the image of a wagon train to show the different evolutionary stages of societies and governments on the way to democratic liberalism and the end of history. "The apparent differences in the situations of the wagons will not be seen as reflecting permanent and necessary differences between the people riding in the wagons, but simply a product of their different positions along the road." That said, on the last page of *The End of History and the Last Man* he stops short of guaranteeing a final universal destination of democratic liberalism, noting that, for now, "the direction of the wagons' wanderings must remain provisionally inconclusive," 339.

37. Ibid. This is the point of Fukuyama, chapter 26, "Toward a Pacific Union," 276-284. "For the foreseeable future, the world will be divided between a post-historical part, and a part that is still stuck in history. Within the post-historical world, the chief axis of interaction between states would be economic, and the old rules of power politics would have decreasing relevance.

    "...The historical world would still be riven with a variety of religious, national, and ideological conflicts depending on the stage of development of the particular countries concerned, in which the old rules of power politics continue to apply. Countries like Iraq and Libya will continue to invade their neighbors and fight bloody battles," 276-277.

38. Ibid., 211.

39. Ibid., 45-46. Fukuyama believes, however, that "the Islamic world would seem more vulnerable to liberal ideas in the long run than the reverse," 46.

40. Samuel P. Huntington, born 1927, was a brilliant and conservative political scientist. He graduated from Yale at 18 and received his Ph.D. from Harvard at 23, at which time he began teaching in Harvard's Department of Government. His areas of study included national security, civil-military relations; and the

role of culture in national identity, political governance, and international civilizations. He died on Christmas Eve 2008. For fuller biographical and professional background, see Robert Kaplan, "Looking the World in the Eye" *The Atlantic*, December 2001, http://www.theatlantic.com/magazine/archive/2001/12/looking-the-world-in-the-eye/2354/ (accessed 27 February 2010).

41. Huntington, *The Clash of Civilizations*, 21. The three blocs were: states aligned with the United States, states aligned with the Soviet Union, and the remaining unaligned states.

42. Ibid., 20; my emphasis.

43. Ibid., 21.

44. Ibid., Map 1.3, 26-27, and discussion at 45-48. The certain seven are: Western, Latin American, Islamic, Sinic, Hindu, Orthodox, and Japanese. The possible eighth is African. Buddhism is excluded, because "while Buddhism remains an important component of [certain] cultures, these societies do not constitute and would not identify themselves as part of a Buddhist civilization," 47.

45. Ibid., 321.

46. Ibid. For Huntington, fault line wars are violent communal conflicts fought between states or groups from different civilizations. Warring sides in fault line wars almost always come from different religions. For characteristics of fault line wars and communal wars, see 252-254.

47. Ibid. See discussion at 42-47; quote at 47. Although certain postmodern commentators may be offended by the claim that civilizations rest on religious foundations, consciences may be soothed by understanding the claim in its historical significance. One must ask which great civilizations were not founded on a profoundly religious understanding of identity, belief, and practice. It is another matter to bring such historical significance forward, to discuss whether a civilization's current identities, beliefs, and practices reflect those same foundations. It is yet another matter to ask whether, or to what extent, cohesive civilizations still exist today.

48. Ibid. On references in this paragraph, see Huntington, 183. On the micro-macro distinction, see 207-209. Huntington notes that "while at the macro or global level of world politics the primary clash of civilizations is between the West and the rest, at the micro or local level it is between Islam and the others," 255.

    On the capitalization of "west" and "western," there is no single, authoritative literary convention. I follow the convention which capitalizes the proper nouns "West" and "Westerner," but not adjectival forms, when used to denote the generalized civilization and set of values associated with the United States and Europe. Huntington follows a different convention which additionally capitalizes the adjective "Western," reflected in quotations at notes 56 and 60.

49. Ibid. Religion is clearly in view in the projected micro and macro level wars. Regarding Huntington's three contributing causes for projected dangerous wars, Islamic intolerance is overtly religious, western arrogance is derivatively religious, and Sinic assertiveness is least religious, and perhaps even nonreligious.

    On western arrogance and religious elements, see chapter 7, "Core States, Concentric Circles, and Civilizational Order," 155-179. Huntington builds the historic case that the civilizational roots of the West, to include those of the United States, lie in the Holy Roman Empire and western Christianity. He also charges that the West now arrogantly believes that its culture is universal, i.e., that the world should adapt its "superior" culture; see 310. For Huntington, the derived religious significance of western arrogance is adequately established by the fact that Islamic militants point to the West as "Christian" and urge Muslims to fight against it. Huntington does not go so far as to say that the arrogance of the West springs from its western Christian civilizational roots.

    For a discussion of China's assertiveness as a function of its "history, culture, traditions, economic dynamism, and self-image," see Huntington, 229-238.

50. Ibid., 109-121. Huntington capitalizes "Resurgence" in "Islamic Resurgence" because "it refers to an extremely important historical event affecting one-fifth or more of humanity, that is at least as significant as the American Revolution, French Revolution, or Russian Revolution, whose 'r's' are usually capitalized," 109.

51. Ibid., 109-110.

52. Ibid., 111. Huntington notes correctly that this Resurgence is similar to the Protestant Reformation's effect on historic Christianity. If one defines the Protestant Reformation as the general reform movement in which Martin Luther and John Calvin stood as pillars, then that reformation was without doubt an attempt to return Christianity to its original, more pure religious foundations. It is interesting to note that there are a number of modern commentators who suggest that Islam, and radical Muslims today, are in need of a "reformation," using the term to signal a need for moderation and a less demanding form of piety. Use of this term in this sense demonstrates a failure to apprehend both the historical moorings and the effects of the Protestant Reformation. In the historic, theological sense, the goals of many radical Muslims today are reformational. For example, the view of the Taliban and Al Qaeda is that they are calling Muslims to return to their historic religious beliefs and practices.

53. Ibid., 121. "The Resurgence will leave a network of Islamist social, cultural, economic, and political organizations within societies and transcending societies. The Resurgence will also have shown that 'Islam is the solution' to the problems of morality, identity, meaning, and faith, but not to the problems of social injustice, political repression, economic backwardness, and military weakness."

54. Ibid., 174-179.

55. Ibid., 174.

56. Ibid., 209-218.

57. Ibid., 210. Huntington notes that "Islam is the only civilization which has put the survival of the West in doubt, and it has done that at least twice."

58. Ibid., 263. See Huntington's discussion of the Islam's bloody borders and related causes of war, 254-265.

59. Ibid., 211.

60. Ibid. Huntington's policy recommendations include recognizing civilizational differences, retooling current policies in that light, and abandoning all myths of universal culture, especially the myth that western culture is universal. For Huntington, part of recognizing civilizational differences means that the United States must, on the one hand, embrace its own identity as a western, and not a multicultural, civilization, and on the other hand, accept a multicultural world composed of multiple civilizations. Regarding the non-universal nature of the West, Huntington stands opposite Fukuyama. See Huntington, 308-321.

61. This restates my earlier contention that religion—not as a standard of belief, but as a power which drives human behavior—must have a seat at the table of national security policy, if that policy is to embrace the fullness of the human condition, and prove effective in the long run.

62. Robert Kaplan is an American journalist who has written extensively for *The Atlantic*. A well-traveled author and foreign correspondent, his trips to dangerous locations—including Iraq in 1984, Afghanistan in 1990, the Middle East, North Africa, Eastern Europe, and Central Asia—have helped him document a position that emphasizes cultural and environmental factors as decisive for post-Cold War national security. For further information and a list of his books, see his biography at *The Atlantic Online*, http://www.theatlantic.com/past/unbound/kaplan/kapbio.htm (accessed 27 February 2010).

63. Kaplan, *The Coming Anarchy*, 19; emphasis in original. Kaplan continues, "The political and strategic impact of surging populations, spreading disease, deforestation and soil erosion, water depletion, air pollution, and, possibly, rising sea levels in critical, overcrowded regions like the Nile Delta and Bangladesh—developments that will prompt mass migrations and, in turn, incite group conflicts—will be the core foreign-policy challenge from which most others will ultimately emanate, arousing the public and uniting assorted interests left over from the Cold War," 19-20.

    For an opposing view on the threat of the environment, see Mark Steyn, *America Alone: The End of the World as We Know It* (Washington, DC: Regnery Publishing, 2006). Steyn argues that the insistence that the environment is the biggest national security issue for the future distracts the United States from the more concrete, deadlier threats that are accompanying changing Muslim demographics, especially in western Europe.

64. Ibid, 24.

65. Ibid., 22. "While a minority of the human population will be, as Francis Fukuyama would put it, sufficiently sheltered so as to enter a 'post-historical' realm, living in cities and suburbs in which the environment has been mastered and ethnic animosities have been quelled by bourgeois prosperity, an increasingly large number of people will be stuck in history, living in shantytowns where attempts to rise above poverty, cultural dysfunction, and ethnic strife will be doomed by a lack of water to drink, soil to till, and space to survive in."

66. Ibid. Based on personal experiences from his frequent travels, Kaplan illustrates friction between Muslims, and between Muslims and the West, anchoring the friction in cultural differences. In this sense, he usually subordinates religious animosities to cultural ones, but without denying the foundational religious clash. For example, "Two months of recent travel throughout Turkey revealed to me that although the Turks are developing a deep distrust, bordering on hatred, of fellow-Muslim Iran, they are also, especially in the shantytowns that are coming to dominate Turkish public opinion, revising their group identity, increasingly seeing themselves as Muslims being deserted by a West that does little to help besieged Muslims in Bosnia and that attacks Turkish Muslims in the streets of Germany.

    "In other words, the Balkans, a powder keg for nation-state war at the beginning of the twentieth century, could be a powder keg for cultural war at the turn of the twenty-first century: between Orthodox Christianity (represented by the Serbs and a classic Byzantine configuration of Greeks, Russians, and Romanians) and the House of Islam. Yet in the Caucasus that House of Islam is falling into a clash between Turkic and Iranian civilizations," 29.

67. Ibid. See Kaplan's discussion of Huntington's "Clash of Civilizations," 26-30.

68. Ibid., 35.

69. Ibid., 35, quoting the 1951 work of Carleton Stevens Coon.

70. Ibid., 35; emphasis in original. Kaplan does not discuss the doctrine of *jihad*. Rather, in the context of environmental crises and failing states, he sees Islam as providing the political framework – to include forms of extremism – that will gain traction among Muslims. "Much of the Arab world...will undergo alteration, as Islam spreads across artificial frontiers, fueled by mass migrations into the cities and a soaring birth rate....

    "...As state control mechanisms wither in the face of environmental and demographic stress, 'hard' Islamic city-states or shantytown-states are likely to emerge," 41-42.

    His view of the result across Islamic lands – part of the coming anarchy – leads Kaplan to conclude that maps of the world of nation-states will be obsolete. In a nice parody of Fukuyama, Kaplan discusses "The Last Map," 50-56.

71. Ibid., 32. See 30-37 for Kaplan's discussion of the successes of Turkey's secular government, built on a powerful Turkish Muslim culture. At 36: "Turkey has been living through the Muslim equivalent of the Protestant Reformation." Here Kaplan presents a positive view of the secular Turkish government and what he characterizes as its moderating, modernizing, and stabilizing effects. For additional information on Turkey's current struggles, see note 144.

    From an historical and theological perspective, Kaplan is misguided in using the Protestant Reformation as a framework for such effects; see note 52.

72. Ibid. See chapter two, "Was Democracy Just a Moment?" in Kaplan, 59-98. For Kaplan, democracies are inherently value-neutral and do not necessarily make societies more civil, at least not in the short run; see 61-63. He suggests that in certain circumstances it may make sense to sacrifice justice for the sake of order. This could mean supporting a tyrannical regime, where grave injustices are perpetuated in the name of religion. Kaplan follows Kissinger in arguing that, in the final analysis, "disorder is worse than injustice," 134. As a policy example, consider Kaplan's "Third World aid policy" based on proportionalism, where the evil endured is outweighed by the good accomplished; see 121-122.

73. Ibid., 93. Kaplan applies this principle in multiple contexts – ancient, postmodern, national, and international – concluding that "the category of politics we live with may depend more on power relationships and the demeanor of our society than on whether we hold elections," 96.

74. By "faith dimension" I mean religion as a comprehensive set of beliefs about God, which interprets the past, integrates human longings across time, and brings the world to fulfillment.

    This faith dimension includes ontology and epistemology. Religion as an ontological system generally begins with a conceptual essence of God and proceeds outward to include humanity and the world. Since the Enlightenment, religion as an epistemological method generally begins with the experiences of humanity and works its way toward God. In my analysis of Islam, I focus on religion as an ontological system. This approach aligns with inner structure of the religion of Islam.

75. I am indebted to Dr. Adam Francisco for his help in navigating the vast sea of available works on Islam. His bibliographical expertise proved invaluable in part II of this paper. Dr. Francisco studied Arabic and Islamic Theology at the Centre for Islamic Studies, University of Oxford, receiving his D.Phil. for his work in the history of Christian-Muslim relations.

    I have relied on a number of resources. For a general overview of Islam and the significance of the *Qur'an* and the *Sunnah*, see: John L. Esposito, *Islam: The Straight Path*, rev. 3d ed., updated with new epilogue (New York: Oxford University Press, 2005). Daniel Madigan, "Themes and Topics," in *Cambridge Companion to the Qur'a*n (Cambridge: Cambridge University Press, 2006), 79-96. Sayyid Abul A'la Maududi, *Toward Understanding Islam*, revised ed., trans.

and ed. by Khurshid Ahmed (no publication data, 1960). Fazlur Rahman, *Major Themes of the Qur'an* (Minneapolis: Bibliotheca Islamica, 1980). Tariq Ramadan, *Western Muslims and the Future of Islam* (New York: Oxford University Press, 2004). Efraim Karsh, *Islamic Imperialism: A History*, updated ed. (New Haven: Yale University Press, 2007).

On *usul al-fiqh* (principles of Islamic jurisprudence), *Sharia'ah* (divine law), and *fatwas* (legal rulings), see Mohammad Hashim Kamali, *Principles of Islamic Jurisprudence*, 3d revised and enlarged ed. (Cambridge: The Islamic Texts Society, 2003).

On *siyar* (the Islamic law of nations), see Khadduri, *The Islamic Law of Nations* (note 4 above). Khadduri provides superb analysis of Shaybani, "the most important jurist to write on the siyar," 22. For a transmission of the classical, traditionalist *siyar*, see Muhammad Hamidullah, *The Muslim Conduct of State*, rev. and enlarged ed. (Lahore, Pakistan: Sh. Muhammad Ashraf, 1968). For a modern interpretive view of *siyar*, compare Labeeb Ahmed Bsoul, *International Treaties (Mu'ahadat) in Islam: Theory and Practice in the Light of Islamic International Law* (Siyar) according to Orthodox Schools (Lanham, MD: University Press of America, 2008).

On *jihad* (struggle or war), see all the above resources for the foundations of *jihad* in the *Qur'an*, *Sunnah*, *Sharia'ah*, and constructs within *usul al-fiqh* and *siyar*. For the most comprehensive modern history and primary source compilation regarding *jihad*, see Bostom, *The Legacy of Jihad* (note 4 above). In addition, see Shmuel Bar, *Warrant for Terror: Fatwas of Radical Islam and the Duty of Jihad* (Lanham, MD: Rowman & Littlefield, Inc., 2006). David Cook, *Understanding Jihad* (Berkeley, CA: University of California Press, 2005).

On English spelling, there are many ways of transliterating from the Arabic. I italicize and generally follow the formally correct transliterations of Kamali. This means that direct quotes from other authors may introduce different spellings, based on their personal preferences. Certain authors do not use italics for Arabic words, a standard convention for foreign language words. In such cases, for the sake of consistency I italicize the Arabic words, even in direct quotes, noting in the end note, "my italics." (This is different from end note references to "my emphasis," which marks my addition of italicized text in a quote as *my emphasis*, rather than as a foreign language.)

76. I offer the comparison with Christianity as a frame of reference, because most readers of this paper will certainly be from the western or Christian tradition.

77. Esposito, Islam: *The Straight Path*, 17. Out of respect, Islam capitalizes "Prophet" when referring to Muhammad.

78. Ibid., 17-20, on the radical nature of Islam's monotheism. God is radically transcendent and exists as Unity in himself, apart from his creation. The Qur'an serves to bring the law – *Shari'ah* – which, in turn, affects the rule of God. By obedience to this law, the Muslim submits to God as God. This law defines the

Muslim and his life. A human becomes a Muslim through submission to the law of this radically transcendent God who is Unity in himself. This submission initially occurs by confessing the *shahada* (testimony), "There is no god but God and Muhammad is the Prophet of God." The *shahada* is the first so-called pillar of Islam, signifying agreement with two propositions: Allah alone is to be worshiped, and Muhammad is the final and perfect Messenger of that God. The other pillars are *salat* (prayer), *zakat* (alms), *sawm* (fasting), and *hajj* (pilgrimage). On the five pillars and their centrality for Islamic life and practice, see Esposito, 68-114.

79. The variety of forms and lack of chronology lead to interpretive difficulties, which are discussed below.

80. This distinction is important, as the Meccan passages enjoin peaceful behavior, while the Medinan verses generally enjoin war.

81. The *Sunnah* is regarded as revelation but it is qualitatively different than *Qur'anic* revelation. The *Qur'an* is viewed as God's eternal and unerring word. The utterances and deeds of Muhammad are revelatory in the sense that they are inspired, but not necessarily inerrant.

82. Out of respect, Islam capitalizes "Companions," based on their closeness to the Prophet.

83. The *sirah*, the biographical accounts of Muhammad's life, draw heavily upon the *hadith*. The earliest *sirah* was written by Ibn Ishaq's Sirat al-Rasul Allah, but this work is no longer extant. A redaction of it does exist, from Ibn Hisham (9th century) available in an English translation: *The Life of Muhammad: A Translation of Ibn Ishaq's Sirat Rasul Allah*, translated and annotated by Alfred Guillame (London: Oxford University Press, 1955).

84. *Shari'ah* was never a codified, completed body of law. Instead, it includes the *Qur'an* and *Sunnah*, together with the discussions, commentaries, and fatwas of authorized Islamic legal experts, as authoritative practice for the *ummah*. See Kamali, *Principles of Islamic Jurisprudence*, 16-186.

85. For an overview of the relation of *usul al-fiqh* to *Shari'ah*, and *usul al-fiqh's* location within the broader Islamic sciences, see *Ramadan, Western Muslims and the Future of Islam*, 55-61. Note especially the helpful chart at 57.

86. Within radical Islam, *fatwas* are frequently used to justify *jihad* and acts of terror. See Bar, *Warrant for Terror*, which superbly documents this use of *fatwas* in the modern period.

87. The *Sunnah* attests to these revelations, through the utterances and deeds of Muhammad.

88. For examples of the liberal position, see discussion of John L. Esposito, and of the postmodern position, see Tariq Ramadan, below.

89. Bostom, *The Legacy of Jihad*, 23. From Ibn Warraq's foreword.

90. For an introduction to the meanings and usages of the word *jihad*, see Rudolph Peters, "Jihad: An Introduction," in Bostom, *The Legacy of Jihad*, 320-325. Although *jihad* in its most basic sense means "to strive, to exert oneself, to struggle," Peters notes that most occurrences in the *Qur'an* and among the Islamic jurists carry the sense of "armed struggle against the unbelievers," 320.

91. Khadduri, *The Islamic Law of Nations*, 5. Khadduri communicates the perspective of a devout Muslim. In explaining Islamic military aggression, he understands the motivation as religious zeal for the conversion of those who would be conquered. Khadduri subordinates any expansionistic desire to this religious motivation.

    Certain liberal Islamic apologists note that Christianity has no less a universal vision of its faith and similarly seeks the conversion of the world. This is true, as far as it goes. But such a comparison fails to account for historical distinctions, i.e., for Islam's norm of submission through warfare and Christianity's norm of conversion through proclamation. The former worked through external domination, the latter through internal affection. This is not to deny that historic Islam desired, sought, and achieved conversion through proclamation, but to recognize that such was a penultimate means, with external *jihad* providing the final means, at least for the initial Islamic centuries.

92. Ibid., 10-14, for the classical position. Like Khadduri, Bsoul follows Shaybani as the definitive commentator on siyar in the classical tradition. See Bsoul, *International Treaties (Mu'ahadat) in Islam*, 14-26, for his discussion of *dar al-Islam* and *dar al-harb*, covering both classical and reformed perspectives, with more of an evolutionary approach to law. Bar, *Warrant for Terror*, 18-24; also covers the classical and reformed perspectives, with greater emphasis on the effects for the *ummah*.

    For the additions of *dar al-ahd* (the territory of treaty), *dar al-amn* (territory of safety), and *dar al-dawa* (territory of invitation), see Ramadan, *Western Muslims and the Future of Islam*, 66-75.

93. Khadduri, *The Islamic Law of Nations*, 12.

94. Ibid., 13. On the conditions for temporarily halting hostilities, see 5-14, and Bsoul, *International Treaties (Mu'ahadat) in Islam*, ix.

95. Khadduri, *The Islamic Law of Nations*, 15; my italics.

96. Hamidullah, *The Muslim Conduct of State*, paragraph 312, 163. This is not to claim that the benefits do not accrue to the individual for participation in *jihad*. Those who undertake *jihad* receive both the spoils of war, and the rewards of Paradise. Indeed there is no more certain way in classical Islam to inherit Paradise than to participate in *jihad*. See Khaddurri, *The Islamic Law of Nations*, note 28, at 15; 72; and chapter three of Shabaybani's *Siyar*, in Khadduri, 106-129.

97. *Qur'an* 9:111, *Sahih Internationa*l, http://quran.com/9/111 (accessed March 13, 2010). Accessed at this same location and date is the *Tafsir al-Jalalayn*

commentary on the first part of the verse: "Indeed God has purchased from the believers their lives and their possessions, that they expend it in obedience of Him – for example by striving in His way – so that theirs will be [the reward of] Paradise: they shall fight in the way of God and they shall kill and be killed (this sentence is independent and constitutes an explication of the [above-mentioned] 'purchase'; a variant reading has the passive verb come first [sc. *fa-yuqtalūna wa-yaqtulūn*, 'they shall be killed and shall kill'], meaning that some of them are killed while those who remain, fight on)."

98. *Qur'an* 9:5, *Sahih International*, http://quran.com/9/5 (accessed March 13, 2010). Accessed at this same location and date is the *Tafsir al-Jalalayn* commentary on the first part of the verse: "Then, when the sacred months have passed – that is, [at] the end of the period of deferment – slay the idolaters wherever you find them, be it during a lawful [period] or a sacred [one], and take them, captive, and confine them, to castles and forts, until they have no choice except [being put to] death or [acceptance of] Islam."

99. *Qur'an* 9:29, *Sahih International*, http://quran.com/9/29 (accessed March 13, 2010); my italics. Accessed at this same location and date is the *Tafsir al-Jalalayn* commentary on the first part of the verse: "Fight those who do not believe in God, nor in the Last Day, for, otherwise, they would have believed in the Prophet (s), and who do not forbid what God and His Messenger have forbidden, such as wine, nor do they practise the religion of truth, the firm one, the one that abrogated other religions, namely, the religion of Islam – from among of those who (*min*, 'from', explains [the previous] *alladhīna*, 'those who') have been given the Scripture, namely, the Jews and the Christians, until they pay the jizya tribute, the annual tax imposed them, readily ('*an yadin* is a circumstantial qualifier, meaning, 'compliantly', or 'by their own hands', not delegating it [to others to pay]), being subdued, [being made] submissive and compliant to the authority of Islam."

It is true that within conquered lands under *Shari'ah*, Jews and Christians were allowed to live as second class citizens, provided they paid the annual tax. Their status, called *dhimmitude*, was frequently characterized by repression. For a comprehensive survey of *dhimmitude* with hundreds of historical examples, see Andrew G. Bostom, "Jihad Conquests and the Imposition of Dhimmitude—A Survey," in Bostom, *The Legacy of Jihad*, 24-124.

100. *Qur'an* 4:95, *Sahih International*, http://quran.com/4/95 (accessed March 13, 2010); my italics. The phrase, "with their wealth and their lives," implies that the true *jihad* is that struggle whereby one gives his wealth to support Islamic war and follows up this support by fighting as a combatant. Accessed at the same location and date is the *Tafsir al-Jalalayn* commentary on the verse: "The believers who sit at home, away from the struggle, other than those who have an injury, such as a chronic illness or blindness or the like (read in the nominative, *ghayru ūlī l-darar*, 'other than those who have an injury', as an adjectival clause; or in the accusative, *ghayra ūlī l-darar*, as an exceptive clause) are not the equals of those who struggle in the way of God with their possessions and their lives. God has preferred those who struggle with their possessions and their lives over the ones who sit at home, on account of some injury, by a degree, by [a degree of] merit, since both have the same intention, but the extra degree is given to those who have carried out the struggle; yet to each, of the two groups, God has promised the goodly reward, Paradise, and God has preferred those who struggle over the ones who sit at home, without any injury, with a great reward (*ajran ʿazīman*, is substituted by [the following, *darajātin minhu*])."

101. *Qur'an* 8:39, *Sahih International*, http://quran.com/8/39 (accessed March 13, 2010); my italics. Accessed at this same location and date is the *Tafsir al-Jalalayn* commentary on the verse: "And fight them until sedition, idolatry, is, exists, no more and religion is all for God, alone, none other being worshipped; then if they desist, from unbelief, surely God sees what they do, and will requite them for it."

102. See M. K. Kister, "The Massacre of the Banu Qurayza: A Re-examination of a Tradition," *Jerusalem Studies in Arabic and Islam* 8 (1986): 61-96. For a summary of Kister, see Bostom, *The Legacy of Jihad*, 17-19.

103. Muhammad ibn Umar al-Waqidi, *Kitab al-Maghazi*, (London: Oxford University Press, 1966), 3: 1113.

104. *Qur'an* 22:78, *Sahih Internationa*l, http://quran.com/22/78 (accessed March 13, 2010); my italics. Accessed at this same location and date is the *Tafsir al-Jalalayn* commentary on the verse: "And struggle in the way of God, in order to establish His religion, a struggle worthy of Him, by expending all effort therein (*haqqa* is in the accusative because it is a verbal noun). He has elected you, He has chosen you for His religion, and has not laid upon you in your religion any hardship, that is, [any] constraint, for He has facilitated [adherence to] it during times of difficulty, such as [His permitting you] to shorten prayers, to seek ritual purification from earth, to eat of carrion, and to break the fast during illness or travel – the creed of your father (*millata* is in the accusative because the genitive preposition *kāf* [sc. *ka-millat*i, 'like the creed of'] has been omitted) Abraham (*Ibrāhīma*, an explicative supplement). He, that is, God, named you Muslims before, that is, before [the revelation of] this Book, and in this, that is, [in] the *Qur'ān*, so that the Messenger might be a witness against you, on the Day of Resurrection, that he delivered the Message to you, and that you might be witnesses against mankind, that their messengers delivered the Message to them. So maintain prayer, observe it regularly, and pay the alms, and hold fast to God, trust in Him. He is your Patron, your Helper and the Guardian of your affairs. An excellent Patron, is He, and an excellent Helper, for you."

105. *Qur'an* 9:81, *Sahih International*, http://quran.com/9/81 (accessed March 13, 2010). Accessed at this same location and date is the *Tafsir al-Jalalayn* commentary on the verse: "Those who were left behind, from [the journey to] Tabūk, rejoiced at remaining behind the Messenger of God, and were averse to striving with their wealth and their lives in the way of God. And they said, that is, they said to one another, ‘Do not go forth, do not set off to [join] the fight, in the heat!’ Say: ‘The fire of Hell is hotter, than Tabūk, and more worthy for them to guard against, by not staying behind, did they but understand’, this, they would not have stayed behind.”

106. *Qur'an* 2:256, *Sahih International*, http://quran.com/2/256 (accessed March 14, 2010); my italics. Note that although this verse does not use the word *jihad*, or a derivative, the verse is frequently invoked to argue that true *jihad* is non-violent. Accessed at this same location and date is the *Tafsir al-Jalalayn* commentary on the verse: “There is no compulsion in, entering into, religion. Rectitude has become clear from error, that is say, through clear proofs it has become manifest that faith is rectitude and disbelief is error: this was revealed concerning the *Ansār* [of Medina] who tried to compel their sons to enter into Islam; so whoever disbelieves in the false deity, namely, Satan or idols (*tāghūt*, ‘false deity’, is used in a singular and plural sense), and believes in God, has laid hold of the most firm handle, the tight knot, unbreaking, that cannot be severed; God is Hearing, of what is said, Knowing, of what is done.”

107. I have based much of my discussion of the greater and lesser *jihad* on Cook, *Understanding Jihad*, 32-48. Quote at 35; my italics. It appears that the “greater *jihad*,” as an inner and spiritual struggle, is documented only after the initial military expansion of Islam stalled.

108. Such a possible synthesis assumes the enduring validity of *jihad* as warfare. Khadduri, *The Islamic Law of Nations*, explains this as follows: “The believers may fulfill the *jihad* duty by heart in their efforts to combat the devil and to escape his persuasion to evil; by their tongue and hands in their attempt to support the right and correct the wrong; and by the sword in taking part in actual fighting and by sacrificing their ‘wealth and lives,’” 15-16, note 29, my italics.

109. On *naskh*, see Kamali, *Principles of Islamic Jurisprudence*, 202-227. “Abrogation applies almost exclusively to the *Qur'an* and the *Sunnah*,” 203. Most Islamic legal scholars believe that *naskh* exists and applies within the *Qur'an*.

Six juridical conditions must be satisfied before *naskh* can be applied. For a discussion of these six conditions, see Kamali, 207. The first stipulation is that the “text itself has not precluded the possibility of abrogation.” Kamali notes that *jihad* can never be abrogated “because the *hadith*...proclaims that ‘*jihad* shall remain valid till the day of resurrection.’”

110. Ibid., 24-25, anchors the permissibility of *jihad* in the later Medinan revelations.

Also see Raymond Ibrahim, “How Taqiyya Alters Islam's Rules of War,” *The Middle East Quarterly* 17, no. 1 (Winter 2010), http://www.meforum.org/2538/taqiyya-islam-rules-of-war (accessed January 18, 2010). Ibrahim notes, “The [Islamic legal scholars] were initially baffled as to which verses to codify into the *Shari'a* worldview – the one that states there is no coercion in religion (2:256), or the ones that command believers to fight all non-Muslims till they either convert, or at least submit, to Islam (8:39, 9:5, 9:29). To get out of this quandary, the commentators developed the doctrine of abrogation, which essentially maintains that verses revealed later in Muhammad's career take precedence over earlier ones whenever there is a discrepancy. In order to document which verses abrogated which, a religious science devoted to the chronology of the Qur'an's verses evolved (known as *an-Nasikh wa'l Mansukh*, the abrogater and the abrogated)."

Another important dialog within Islam, which parallels the dynamics of the applicability of *naskh*, is the discussion of whether legitimate *jihad* is defensive or offensive in nature. Interpreters emphasizing the defensive posture cite earlier Qur'anic passages, while those justifying offensive actions cite the later revelations. A credible argument for defensive *jihad* may be made theologically, but not historically. Islamic clerics sometimes see a theological principle at work, where that portion of humanity which has not submitted to Allah is in truth attacking the universalizing work of the *ummah* and the will of Allah. In this theological sense, the Islamic invasion of foreign lands may be construed to be defensive in nature. That said, the historical perspective of Islamic warfare expanding to take the fight into Spain, France, and Italy cannot credibly be called defensive.

111. See Bar, *Warrant for Terror*, 2-3, for *naskh* as the questionable basis for terrorist *fatwas*.

Within the discussion of the priority of the *Qur'anic* Medinan texts over the early Meccan texts, and of the militant over the peaceful *jihad*, it is important to call attention to an intensifying factor frequently present in such interpretations. This is the apocalyptic factor. See Cook, *Understanding Jihad*, 22-25, for a discussion of how Islamic military expansion may have been tied to popular views that the world was about to end. Cook extends this line of thought in his analysis of modern radical Islam; see 157-161.

See also Timothy R. Furnish, *Holiest Wars: Islamic Mahdis, their Jihads, and Osama bin Laden* (Westport, CT: Praeger Publishing, 2005). He documents Islamic eschatology and the rise of *Mahdism* – the belief that a messiah, *al-Mahdi*, would reveal himself and usher in a worldwide Islamic state. Furnish tracks eight *Mahdi* movements within *Sunni* Islam. He also briefly discusses *Shi'i* Muslims who look for the Hidden Imam to reveal himself and usher in the final universalization of Islam. Many terrorists subscribe to such *Mahdist* views, and believe that their attacks, both against the West and against heterodox Muslims, will usher in the final Islamic fulfillment.

112. In no way do I intend the use of the term "problem" to be derogatory. When I speak of the "problem" of Islam, or of any religion for that matter, I mean that religion's essential framework for understanding God and integrating a problematic humanity within that framework. In short, the problem of a religion propels the structure of that religion to deliver the power of that religion.

An example which may prove helpful for western audiences would be the problem of Christianity. The problem of Christianity is arguably the problem of love. Christianity conceives of the essential nature of God as love, with all other conceptions such as justice subordinated within the Godhead. This love exists within the one God himself, in the relation of the Persons of Father, Son, and Spirit. For the Christian: Father, Son, Spirit is God, and there is no God but Father, Son, and Spirit. Love binds Father and Son together in the unity of the Spirit. The problematic nature of love is seen in fallen humanity's failure to love God and one's neighbor purely and fully. The solution to the problem occurs in the enfleshment of the Son, who suffers and overcomes humanity's failures and fallenness. This Son sends his Spirit through word and baptism to create faith and graft humanity into his own body. Connected with God's love through the Son, humanity begins to love God and neighbor aright. This example shows how the problem of Christianity propels the structure of Christianity to deliver the power of Christianity.

113. This truth applies to the individual, the *ummah*, and the world.

114. This does not deny the internal, spiritual struggle that *jihad* also implied, and continues to imply. Rather, it emphasizes the continuing potential for legitimate, violent *jihad*.

115. My six categories overlap somewhat with Esposito's four categories, from which I have drawn some of my materials. See Esposito, *The Straight Path*, 228-232. Esposito divides the Islam of today into four categories—secularist, conservative, neotraditionalist, and reformist. The apparent similarity with my nomenclature, however, may be deceiving.

Esposito's overarching purpose is to articulate how groups or positions within Islam address the need for change within Islam. Based on this approach, Esposito does not discuss radical traditionalist Islam as a position within Islam; this position sees no need to modernize the assumptions of historic Islam. Instead, Esposito speaks of a "radical activist" segment, which category largely overlaps my category of radical traditionalist Islam. See Esposito, 166.

Esposito also fails to distinguish the liberal and postmodern reformed positions, perhaps because both include a concept of change which addresses modern, political processes.

My approach differs from Esposito's. My overarching purpose here is not to address perceptions about Islam's need for change, but to articulate how groups or positions within Islam today address the central question of the Islamic faith – how Islam is to achieve its universalization. That Esposito addresses another question which is central neither to the *Qur'an* nor to Muhammad as we know him from the *Sunnah* and his biographies – i.e, how Islam is to change – is a reflection of Esposito and his assumptions from the liberal reformed position.

116. Regarding the naming of Islamic positions, I find certain terms currently in use to be less than helpful. For example, is an "extremist" one who is simply taking

a good idea too far, i.e., to the extreme? If so, how far ought he to take his good idea? If "*jihadists*" are those Muslims who take *jihad* seriously, wouldn't this term necessarily apply to all faithful Muslims, irrespective of variances in their particular understandings of *jihad*? What about "fundamentalists"? Are these people who subscribe to the fundamentals of their faith? If so, what religious adherent would want to subscribe to something other than that which was fundamental for that faith? "Islamists" and "Islamicists" are equally problematic terms, attempting to create a pejorative for a certain party within Islam, without identifying the distinctive nature of that party. Names matter and should articulate what is distinctive about the position being named.

117. On the distinctions between Wahhabists and Salifists, the often unexpected alliances between *Sunni* and *Shi'ah* groups, and the significant ideological differences within the broader radical Arab Sunni population, see Samuel Helfont, *The Sunni Divide: Understanding Politics and Terrorism in the Arab Middle East* (Philadelphia, PA: Foreign Policy Research Institute, 2009). Helfont's work is published under the Foreign Policy Research Institute's Center on Terrorism and Counterterrorism and is available at http://www.fpri.org/pubs/Helfont.SunniDivide. pdf (accessed November 11, 2009).

There are multiple ways to transliterate words affiliated with *Sunni* and *Shi'ah* Islam. I follow the usages of Furnish and Kamali, which seem to represent the Arabic most faithfully. For the collective name of the sects, when used either as a noun or adjective, I use *Sunni* and *Shi'ah*. For the name of an adherent, when used either as a noun or adjective, I use *Sunni* and *Shi'i*. For the plural form of adherents, I use *Sunnis* and *Shi'is*.

118. On radical Islam and contemporary *jihad* theory, see Cook, *Understanding Jihad*, 93-127. On Osama bin Laden and global radical Islam, see Cook, 128-161, and Esposito, *Islam: The Straight Path*, 262-263.

119. Inter-Islamic warfare often breaks down into *Shi'ah* versus *Sunni*. This historic divide within Islam has erupted into war countless times. It is also true that Abd al-Wahhab considered "the overwhelming majority of Muslims as infidels," and that many Wahhabists today make similar judgments; see Helfont, *The Sunni Divide*, 5. The scale of potential *Shi'ah–Sunni* sectarian violence was graphically manifested following the 2006 bombing of the *Al 'Askari* mosque in Samarra, Iraq.

120. See Helfont, *The Sunni Divide*, 25-52, for a review of various terrorist organizations throughout the Middle East. Helfont's study is chiefly structured against the backdrop of the *Sunni* division between the Muslim Brotherhood and Wahhabists, but does take into account *Shi'i* Iran and its drive for regional hegemony.

121. *Qur'an* 4:29, *Sahih International*, http://quran.com/4/29 (accessed March 16, 2010): "O you who have believed, do not consume one another's wealth unjustly but only [in lawful] business by mutual consent. And do not kill yourselves [or one another]. Indeed, Allah is to you ever Merciful."

122. See Cook, *Understanding Jihad*, 142-147. Cook views with skepticism the applicability of such *Qur'anic* passages quoted by Islamic terrorists.

     Cook notes that even if one grants the permissibility of martyrdom operations within Islam, there still remains the problem of legitimate authorization for undertaking terrorist attacks and, for that matter, any militant *jihad*. Radical Muslim movements "disregard the necessity of established authority," for the history of Islam shows that only "a legitimate authority such as a caliph or an *imam* could declare *jihad*."(164) The radical Muslim, however, finds the needed authorization in *fatwas* produced to address precisely this dilemma.

123. See Khadduri, *The Islamic Law of Nation*s, 57-59, on adjustments to the Islamic concept of *jihad* in light of Islam's relative loss of power.

124. Ibid., 20-21, 57-70, on adjustments to the Islamic concept of universalization, due to geo-political realities.

125. Kamali, *Principles of Islamic Jurisprudence*, 501.

126. Ibid., 513.

127. This list follows the analysis of Esposito, *Islam: The Straight Path*, 229-231.

128. For example, consider the Muslim Brotherhood. Helfont points out that the Brotherhood has taken a more political than theological approach in addressing Islamic conflict, and has recognized the principle of nonviolence. Nonetheless, its sanctioned practice includes suicide bombings and other terrorist tactics. "In several cases, such as in Iraq and Afghanistan, the Muslim Brotherhood's understanding of *jihad* represents a direct military threat to the U.S. and its allies," 53, my italics.

129. For another postmodern vision of Islam, see Abdulaziz Sachedina, *The Islamic Roots of Democratic Pluralism* (New York: Oxford University Press, 2001).

130. See Ramadan, *Western Muslims and the Future of Islam*, 3-7. "There is one Islam, and the fundamental principles that define it are those to which all Muslims adhere, even though there may be, clothed in Islamic principles, an important margin allowed for evolution, transformation, and adaptation to various social and cultural environments," 9.

131. Ibid., 14.

132. Ibid. Ramadan is representative of the postmodern Muslim position, for he rejects traditionalist understandings of *Shari'ah* as a defined set of rules and of *jihad* as an external struggle. Instead he views *Shari'ah* as "the path that leads to the spring," 31. He characterizes *jihad* as those "individual and collective efforts, *jihads*, to be made at various levels and in various areas. On the intimate level, it is working on one's self, mastering one's egoisms and one's own violence; on the social level, it is the struggle for greater justice and against various kinds of discrimination, unemployment, and racism; on the political level, it is the defense of civil responsibilities and rights and the promotion of pluralism, freedom of expression, and the democratic processes; on the economic level, it

is action against speculation, monopolies, and neocolonialism; on the cultural level, it is the promotion of the arts and forms of expression that respect the dignity of conscience and human values," 113.

133. Ibid., 17. For Ramadan, because none of the constitutive elements of man is positive or negative in itself, no external battle to achieve unity makes sense. Instead, the responsible conscience will seek the original testimony of the traces of the Creator left within man. In this way Ramadan moves the basis for Islamic unity from outside man to within man. See Ramadan, 14-19.

134. Ibid., 151; emphasis in original.

135. Ibid., 148-152.

136. Ibid., 214. "Islam stands as a civilization as a result of this singular ability to express its universal and fundamental principles across the spread of history and geography while integrating the diversity and taking on the customs, tastes, and styles that belong to the various cultural contexts."

The nomenclature of "Islamic civilization" raises Huntington's thesis. To a degree, Ramadan resonates with this thesis. He notes that "if the clash is not a reality, the ingredients that could lead to it are very present in current mentalities; on both sides, the lack of knowledge of the other (and of self), the acceptance of simplistic and absolute caricatures and final judgments, not to mention conflicting political and geostrategic interests, are objective features that could lead to the breakdown," 226. Interestingly, Ramadan concludes that the West will not likely meet Islam at the "geopolitical frontiers." Rather, it will be "within European and American societies" where successful listening and dialog must occur, to preclude a breakdown.

137. John L. Esposito is a Professor of Islamic Studies and the Founding Director of the Prince Alwaleed bin Talal Center for Muslim-Christian Understanding at the Walsh School of Foreign Service, Georgetown University. The Prince Alwaleed bin Talal Center for Muslim-Christian Understanding was founded in December 2005 through a $20 million dollar gift from Prince Alwaleed Bin Talal of Saudi Arabia. Previously the institute existed as the Center for Muslim-Christian Understanding.

138. The assumptions of theological liberalism inform Esposito's method of analyzing Islam.

139. Esposito, Islam: The Straight Path, 12.

140. Ibid., my emphasis.

141. Ibid., 13-14. Esposito further interprets *jihad* today as the broader "religious, intellectual, spiritual, and moral" struggle to bring Muslims into "a progressive, constructive, modern Islamic framework in response to the realities of Muslim societies," 266-267.

142. Ibid., 31.

143. Western political leaders have frequently hailed such a vision as a welcome basis for finding common cause with Islamic nation states. Interestingly, Esposito goes out of his way to note that Islam, Christianity, Judaism, and Hinduism have each been wrongfully accused of supporting terrorism; see Esposito, 270. This is true as far as it goes, but Esposito fails to note certain critical historical distinctions among the religions. For example, unlike Jesus, Muhammad was a warrior who did command his followers to wage war. That Esposito omits this demonstrates that his method is more committed to transhistorical principles than to historical data.

For an opposing view to Esposito, see Michael Scheuer, *Imperial Hubris: Why the West Is Losing the War on Terror*, with new epilogue (Dulles, VA: Potomac Books, 2005). Scheuer argues that traditionalist Muslims will not give up their ideology to embrace the liberal perspective that all ideologies are essentially equal.

144. For a critical snapshot of the challenges that continue to face Egypt, consider that 53 percent of Muslims in Egypt find terrorist actions to be justifiable in defense of Islam, under certain situations. See related discussion at Table 8. For a discussion of the political mobilization of Islam in Mubarak's Egypt, see Carrie Rosefsky Wickham, *Mobilizing Islam: Religion, Activism, and Political Change in Egypt* (New York: Columbia University Press, 2002).

Regarding Turkey and the rise of the Justice and Development Party (AKP) beginning in 2002, see Morton Abramowitz and Henri J. Barkley, "Turkey's Political Revolution: Ankara's Civil-Military Struggle Has Global Significance," *The Wall Street Journal*, March 22, 2010, http://online.wsj.com/article/SB100 01424052748704207504575129313434669400.html?mod=WSJ_Opinion_ LEFTTopBucket (accessed March 22, 2010). The article documents the threat of the evolution of Turkey from a secular democracy to a more religious and authoritarian state. For a similar discussion of current pressures to move Turkey toward Islamic nation state status, see Bassam Tibi, "Islamists Approach Europe: Turkey's Islamist Danger," *The Middle East Quarterly* 16, no. 1 (Winter 2009), http://www.meforum.org/2047/ islamists-approach-europe?gclid=C P684dLJw6ACFcN05QodLjMhZw (accessed March 18, 2010). For another discussion of secular-state Turkey confronting a challenge to move toward a more Islamic government and still remain pluralistic, see M. Hakan Yavuz and John L. Esposito, eds., *Turkish Islam and the Secular State: The Gülen Movement* (Syracuse, NY: Syracuse University Press, 2003).

145. See Thomas F. Lynch III, *Sunni and Shi'a Terrorism: Differences that Matter*, Occasional Paper Series, West Point Combating Terrorism Center, December 29, 2008; http://gsmcneal.com/wp-content/uploads/2008/12/sunni-and-shia-terrorism-differences-that-matter.pdf (accessed March 19, 2010).

146. Ibid., 64. On *Shi'i* "campaigns" versus *Sunni* "waves," see especially charts on 23 and 28. Lynch offers policy recommendations that address *Sunni* and *Shi'i*

terrorism as discrete threats; see 59-65. Lynch offers a list of *Sunni* and *Shi'i* terror organizations, many of which he references in his study; see 66-72.

147. Helfont, *The Sunni Divide*, 1; my italics. Helfont finds these *Sunni* divisions to be "generally indicative of the political order in the Middle East."

148. See Helfont, 4-8, for his discussion of Wahhabism. Wahhabism identifies Saudi Arabia as its ideological home, and continues to have a strong presence there.

149. See Helfont, 8-23, for his discussion of the Muslim Brotherhood.

150. For a comparison of the Muslim Brotherhood and Wahhabism, with special attention to differences in their concept of *jihad*, see Helfont, 23-24, 44-52.

151. See Helfont, 25-41, for a discussion of the Middle East regional implications of the three-way power struggle between Wahhabism, the Muslim Brotherhood, and Iran.

152. For Helfont's policy recommendations, see 53-73. Helfont believes that it is imperative that the United States support neither Wahhabist nor Muslim Brotherhood organizations. He advocates treating such organizations separately, while pursuing broad support for open, stable societies throughout the region.

153. Studies of "those who support" radical Islam or terrorism are also called "demand side studies." The paucity of such studies is due in part to the size of the religion of Islam, the dangers in areas of conflict, and the requirement for significant resourcing. Also, there is the challenge of dividing radical Islam as religion from terrorism as tactic. Additionally, there are the terminological difficulties with unclear and overlapping meanings of the rule of Shari'ah, extremism, radicalism, *jihadism*, and Islamism, to name but a few. Finally, and perhaps most significantly, I believe there is the fear that demand side investigation might come off as judgmental.

154. See John L. Esposito and Dalia Mogahed, *Who Speaks for Islam?: What a Billion Muslims Really Think* (New York: Gallup Press, 2007). Esposito and Mogahed's book is long on interpretation, but short on the Gallup data it seeks to represent. In fact, the book does not contain one table or chart of data. The study has been criticized as subjective and unscientific. For a critique of this study, see Hillel Fradkin of Middle East Strategy at Harvard, Weatherhead Center; http://blogs.law.harvard.edu/mesh/2008/04/who_does_speak_for_islam/ (accessed March 23, 2010). See also the critique of Martin Kramer, a fellow at the Washington Institute for Near East Policy, and at the Adelson Institute for Strategic Studies, Shalem Center, and at the Olin Institute for Strategic Studies, Harvard University; http://sandbox.blog-city.com/ dr_esposito_and_the_seven_percent_solution.htm (accessed March 23, 2010).

155. For the first applicable Islamic demographics from the Pew Research Center, see the first major report of the Pew Global Attitudes Project, *What the World Thinks in 2002*, Pew Global Attitudes Project, December 4, 2002; http://people-press.org/reports/pdf/165.pdf (accessed March 19, 2010). Henceforth,

2002 Pew Report. The Pew Research Center has continued to release regular Islamic studies, with the latest release of data in 2007.

156. C. Christine Fair and Bryan Shepherd, "Who Supports Terrorism?: Evidence from Fourteen Muslim Countries," *Studies in Conflict & Terrorism* 29, no. 1 (2006): 51-74. Conclusions cited are found at 71. Fair and Shepherd are aware of the limitation of the original data having been collected before OPERATION IRAQI FREEDOM. They wonder if the rates of support for terrorism would have been higher, had the data been collected later; see 73.

157. See *Support for Terror Wanes Among Muslim Publics*, Pew Global Attitudes Project, July 14, 2005; http://pewglobal.org/reports/pdf/248.pdf (accessed March 19, 2010). Henceforth, 2005 Pew Report.

Also see Muslim Americans: Middle Class and Mostly Mainstream, Pew Research Center, May 22, 2007; http://pewresearch.org/assets/pdf/muslim-americans.pdf (accessed March 19, 2010). This document also provides important data based on an April 2006 Pew Research Center survey of Muslims living in Muslim countries. Henceforth, 2007 Pew Study.

158. The 2005 Pew Report and the 2007 Pew Study both used the words "Islamic extremism" in its survey questions. The surveys themselves show the difficulty of using this nomenclature. My judgment is that the 2005 Pew Report and the 2007 Pew Study intend by this nomenclature to include all positions that would advocate any of the following: the rule of *Shari'ah* law at the governmental level, the potential legitimacy of violent *jihad*, and the potential legitimacy of the use of the tactics of terror. This would include all traditionalist positions – radical, conservative, and neotraditionalist – as well as terrorists. See related discussion at Tables 5 and 6.

159. The 2002 and 2005 Pew Reports, and the 2007 Pew Study, all fail to distinguish between acts which are part of militant *jihad*, which lies within the position of traditionalist Islam, and acts of terrorism. Also problematic is the pertinent survey question, which speaks of "suicide bombing and other forms of violence against civilians," failing to recognize terrorism which might be committed against service members. For example, acts of violence committed against wounded service members out of the fight, or against prisoners of war, or against service members of neutral forces participating in humanitarian relief operations, would be terrorist acts, judged according to the Geneva Conventions and the just war tradition. These limitations notwithstanding, the survey question helps shed light on how many Muslims would support terrorist acts as defined by Pew. See related discussion at Tables 7, 8, and 9.

160. See 2005 Pew Report, 34, for question "MQ.18" and responses. A number of respondents volunteered that they were equally Muslims and citizens.

161. Ibid., 34-35, for question "MQ.19" and responses. The 2002 data, drawn from the 2002 Pew Report and included at "MQ.19" of the 2005 Pew Report, does not appear to yield any remarkable conclusion.

162. Ibid., 35, for question "MQ.20" and responses.

163. Ibid., 36, for question "MQ.25" and responses. The large numbers of those who could not or would not answer may suggest the possible inadequacy of the terminology "Muslim extremism."

164. Ibid., 36-37, for question "MQ.26" and responses.

165. See 2007 Pew Study, 91, for question "QH.1".

166. There is a somewhat hopeful trend demonstrated among those countries which were surveyed also in the earlier 2002, 2004, and 2005 Pew Reports. The 2007 Pew Study shows in Pakistan, Jordan, and Indonesia a decline among the rates of Muslims who find acts of terror justified; however, in Turkey there is an increase. All told, the overall rates remain high.

167. On the Muslim population of the United States, see 2007 Pew Study, 3. On the age breakdown of Muslims in the United States, Great Britain, France, German, and Spain, relative to their support for suicide bombing and other terrorist acts, see 2007 Pew Study, 54. It is distressing that a reported 26 percent of Muslims in America ages 18-29 hold that such terrorist acts can be justified.

168. See 2005 Pew Report, 38, for question "MQ.31" and responses.

169. Richard L. Pace, *The Role of Religion in the Life and Presidency of George W. Bush*, Strategic Research project (Carlisle Barracks, PA: U.S. Army War College, March 19, 2004). See also Stephen Mansfield, *The Faith of George W. Bush* (New York: J. P. Tarcher, 2003). Mansfield recounts that most United States Presidents have used religious language in their speeches, but notes, "By the early decades of the twentieth century, however, religion had declined as an influence in the United States, but presidents still spoke religiously of the nation as a nod to a Christian memory and as an attempt to baptize the American culture of their day," xvii.

170. See Pace, *The Role of Religion*, 8. Pace finds that certain of the terms President's Bush used in connection with the global war on terrorism reflected "the lens of his personal faith." He cites examples such as "the axis of evil" and, regarding the war against terrorists, "Freedom and fear, justice and cruelty have always been at war, and we know that God is not neutral between them."

171. Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2002), 131. Woodward quotes President Bush's comments on the repressiveness of North Korea and Iraq: "There is a human condition that we must worry about in times of war. There is a value system that cannot be compromised – God-given values. There aren't United States-created values. There are values of freedom and the human condition and mothers loving their children. What's very important as we articulate foreign policy through our diplomacy and military action, is that it never looks like we are creating – we are the author of these values."

172. Pace notes that President Bush used policy to support freedom of religion for all religions, because he viewed religious practice as one of the most basic universal

freedoms; see 7. Had President Bush's policy been based on his own particular faith, it likely would not have supported freedom of religion for all faiths.

173. *The National Security Strategy of the United States of Americ*a, September 17, 2002, http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/nss.pdf (accessed March 24, 2010). The National Security Strategy of the United States of America, March 16, 2006, http:// georgewbush-whitehouse.archives.gov/nsc/nss/2006/nss2006.pdf (accessed March 24, 2010).

174. *2002 National Security Strategy*, iv, vi. Note that at vi, freedom is defined as the demand of human dignity; throughout the NSS freedom and human dignity are held to be two sides of the same coin.

On the freedom as a universal value, see also 3: "The United States must defend liberty and justice because these principles are right and true for all people everywhere."

175. Ibid., 3. The entire quote runs as follows: "America must stand firmly for the nonnegotiable demands of human dignity: the rule of law; limits on the absolute power of the state; free speech; freedom of worship; equal justice; respect for women; religious and ethnic tolerance; and respect for private property."

176. Ibid., 4. The 2002 NSS did not limit to Muslim countries its promotion of religious freedom. In its discussion of the main centers of global power, the 2002 NSS argued that "only by allowing the Chinese people to think, assemble, and worship freely can China reach its full potential," 28, my emphasis.

177. Ibid., 6: "We will also wage a war of ideas to win the battle against international terrorism. This includes...supporting moderate and modern government, especially in the Muslim world, to ensure that the conditions and ideologies that promote terrorism do not find fertile ground in any nation."

178. *2006 National Security Strategy*, 7.

179. Ibid., 6-7.

180. Ibid., 9-10. The articulated long-term solution was to build democratic societies defined by ownership stake in society, the rule of law, freedom of speech, and the respect for human dignity; ibid., 10-11. The short-term solution was to prevent attacks by terrorist networks before they could occur, deny weapons of mass destruction to rogue states and terrorist allies, deny terrorist groups the support and sanctuary of rogue states, and deny terrorists the control of any nation that they could use as a base of operations; Ibid., 12.

181. President Obama's remarks at the National Prayer Breakfast, Washington, DC, February 5, 2009, http://www.whitehouse.gov/blog_post/this_is_my_prayer/ (accessed October 18, 2009). Within his prayer breakfast remarks, President Obama commented that his father was a Muslim who became an atheist, his grandparents were non-practicing Methodists and Baptists, and his mother was skeptical of organized religion.

182. Ibid. The pertinent text reads in full: "We know too that whatever our differences, there is one law that binds all great religions together. Jesus told us to 'love thy neighbor as thyself.' The Torah commands, 'That which is hateful to you, do not do to your fellow.' In Islam, there is a hadith that reads 'None of you truly believes until he wishes for his brother what he wishes for himself.' And the same is true for Buddhists and Hindus; for followers of Confucius and for humanists. It is, of course, the Golden Rule—the call to love one another; to understand one another; to treat with dignity and respect those with whom we share a brief moment on this Earth."

Many adherents of these, and other, world religions would argue that the moral imperatives of their faiths are not the same. That said, western theological liberalism frequently interprets the religions of the world as cut from the same cloth.

183. Ibid.

184. As of March 29, 2010, the original completion date of this paper, President Obama had published no National Security Strategy.

To access the speeches of President Obama which I have used as sources, see:

President Obama's Inaugural Address, Washington, DC, January 20, 2009, http://www.whitehouse.gov/the_press_office/President_Barack_Obamas_ Inaugural_ Address (accessed February 1, 2010).

President Obama's remarks to the Turkish Parliament, Ankara, Turkey, April 6, 2009, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Obama-To-The-Turkish-Parliament/ (accessed October 18, 2009).

President Obama's "On a New Beginning" speech at Cairo University, Cairo, Egypt, June 4, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-Cairo-University-6-04-09/ (accessed October 18, 2009).

President Obama's "New Moment of Promise" speech to the Ghanaian Parliament in Accra, Ghana, July 11, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-to-the-Ghanaian-Parliament/ (accessed February 1, 2010).

President Obama's remarks at the memorial service at Fort Hood and III Corps, Fort Hood, TX, November 10, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-memorial-service-fort-hood (accessed November 15, 2009).

President Obama's "On the Way Forward in Afghanistan and Pakistan" speech at West Point, NY, December 1, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-address-nation-way-forward-afghanistan-and-pakistan (accessed December 8, 2009).

185. From Ankara, the following quote is representative of President Obama's speech: "The United States is not, and will never be, at war with Islam. In fact, our partnership with the Muslim world is critical not just in rolling back

the violent ideologies that people of all faiths reject, but also to strengthen opportunity for all its people.

"I also want to be clear that America's relationship with the Muslim community, the Muslim world, cannot, and will not, just be based upon opposition to terrorism. We seek broader engagement based on mutual interest and mutual respect. We will listen carefully, we will bridge misunderstandings, and we will seek common ground. We will be respectful, even when we do not agree. We will convey our deep appreciation for the Islamic faith, which has done so much over the centuries to shape the world – including in my own country."

186. From Ankara, while speaking about his support for Turkey's bid to join the European Union (EU), President Obama commented that the EU would stand to gain by the "diversity of ethnicity, tradition and faith" that Turkey would bring. He then proceeded to encourage Turkey in its reforms, for "freedom of religion and expression lead to a strong and vibrant civil society."

187. From Cairo, regarding terrorists: "Their actions are irreconcilable with the rights of human beings, the progress of nations, and with Islam."

188. From Cairo, the full quote runs as follows: "There's one rule that lies at the heart of every religion—that we do unto others as we would have them do unto us. This truth transcends nations and peoples – a belief that isn't new; that isn't black or white or brown; that isn't Christian or Muslim or Jew. It's a belief that pulsed in the cradle of civilization, and that still beats in the hearts of billions around the world. It's a faith in other people, and it's what brought me here today.

"We have the power to make the world we seek, but only if we have the courage to make a new beginning."

189. From Accra, the full quote runs as follows: "Defining oneself in opposition to someone who belongs to a different tribe, or who worships a different prophet, has no place in the 21st century. Africa's diversity should be a source of strength, not a cause for division. We are all God's children."

190. On November 10, 2009 President Obama spoke at a memorial service at Fort Hood, TX, in the wake of the November 5, 2009 terrorist attack. As of the writing of this paper Major Nidal Malik Hasan stands accused of opening fire and killing 13, and wounding 30 others, while shouting *Allahu Akbar*, "God is great" in Arabic. All but one of the casualties were soldiers. These casualty figures are from the official U.S. Army Home Page. Other authorities cite 14 dead, including the unborn infant of one slain pregnant soldier, and 38 wounded. See C. Todd Lopez, "President Says Nation Will Always Remember Fort Hood Casualties," November 11, 2009, at *The United States Army Home Page*, http://www.army.mil/-news/2009/11/11/30179-president-says-nation-will-always-remember-fort-hood-casualties/index.html (accessed 25 March 2010).

191. From West Point, the full quote runs as follows: "We'll have to use diplomacy, because no one nation can meet the challenges of an interconnected world

acting alone. I've spent this year renewing our alliances and forging new partnerships. And we have forged a new beginning between America and the Muslim world – one that recognizes our mutual interest in breaking a cycle of conflict, and that promises a future in which those who kill innocents are isolated by those who stand up for peace and prosperity and human dignity."

192. Here I am leaving aside the added strategic message in the 2006 National Security Strategy, which characterized Islam as a proud religion being twisted by terrorists for evil purposes. Because President Obama has taken this message and more fully developed it, I provide analysis in my discussion of the paradigm suggested by President Obama's policy – the paradigm of Religion as Unity.

193. I am not intending to convey a comprehensive plan that uses all elements of national power to the defeat the adversary, but only a sketch of some of the policy implications of the paradigm of Religion as Freedom.

194. On the answers of various positions within Islam to this decisive question, see part II above, subsection, "The Central Question for Islam – How Islam is to Achieve its Universalization."

195. See discussion above, part II, subsection, "Alignments within Traditionalist Islam."

196. Here I am leaving aside the additional note sounded in President Obama's speeches at Ankara and Cairo, in which he encouraged diversity of religious expression for building strong and vibrant societies. Because President Bush more fully developed this thought, I provide analysis in my discussion of the paradigm suggested by President Bush policy – the paradigm of Religion as Freedom.

197. On the varying faith positions within Islam, see Table 1 of this paper. On demographics which show the level of Muslim support for ever justifying terrorist acts, see Table 8.

198. On the answers of various positions within Islam to this decisive question, see part II above, subsection, "The Central Question for Islam – How Islam is to Achieve its Universalization."

199. The pertinent portion of the First Amendment to the U.S. Constitution reads, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof."

200. I am indebted to Chaplain (Colonel) Micheal Hoyt of the Office of the Army Chief of Chaplains, DACH-3/5/7, for his analysis regarding options for strengthening religion within campaign planning.

A Commander's Strategy for Social Media

1. "'Neda' becomes rallying cry for Iranian protests." *CNN.Com/World*, 22 June 2009.

2. United4Iran, “16 Azar Green Routes,” *Flickr*, December 6, 2009. http://www.flickr.com/photos/united4iran/4165827330/ (accessed October 27, 2010) provides an example of social media tools used to share information among the Iranian protestors.

3. Huda al Saleh, “Al-Qaeda Continues Using Modern Technology to Recruit Youth,” *Asharq Alawsat*, January 5, 2010, http://aawsat.com/english/news.asp?section=3&id=19409 (accessed October 27, 2010).

4. William B. Caldwell IV, Dennis M. Murphy, and Anton Menning, “Learning to Leverage New Media: The Israeli Defense Forces in Recent Conflicts,” *Military Review* 89, Iss. 3 (May-June 2009): 2-10.

5. Ibid.

6. Robert H.Dorff, “A Primer in Strategy Development,” in *U.S. Army War College Guide to Strategy*, eds. Joseph R. Cerami and James F. Holcomb, Jr. (Carlisle, PA: Strategic Studies Institute, 2001), 11-18.

7. See for instance The Social Media Hub, DOS Office of Innovative Engagement, https://www.intelink.gov/communities/state/smp/.

8. David H Petraeus, “Multi-National Force Commander’s Counterinsurgency Guidance,” *Military Review* 88, Iss. 5 (September-October 2008): 210-212.

9. Ibid.

10. Ibid.

11. Dorff, “A Primer in Strategy Development,” 11.

12. Catharine P Taylor, “Eight Ways to Ruin your Social-Media Strategy,” *BNET.com*, November 18, 2009, http://www.bnet.com/2403-13237_23-366324.html?tag=content;btmTier (accessed October 27, 2010).

13. Joint Warfighting Center, *Commander’s Handbook for Strategic Communication* (Norfolk, VA: U.S. Joint Forces Command, Joint Warfighting Center, 2008), III-4.

14. Mark Drapeu and Linton Wells II, *Social Software and National Security: An initial Net Assessment* (Washington DC: National Defense University, Center for Technology and National Security Policy, 2009), 23.

15. Deputy Secretary of Defense, *Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-Based Capabilitie*s (Washington, DC: U.S. Department of Defense, Februrary 25, 2010), 2.

16. Dierdre Collings and Rafal Rohozinsk, *Bullets and Blogs: New Media and the Warfighter* (Carlisle, PA: Center for Strategic Leadership, 2008), 2.

17. Cori E. Dauber, “The Truth is Out There: Responding to Insurgent Disinformation and Deception Operations,” *Military Review* 89, Iss. 1 (January - February 2009): 13-24.

18. Collings and Rohozinski, *Bullets and Blogs: New Media and the Warfighter*, 78.

19. Kimberly Harrington, Department of State, Office of Innovative Engagement, interview by author, Washington DC, November 19, 2009.

20. Collings and Rohozinski, *Bullets and Blogs: New Media and the Warfighter*, 27.

Strategic Communication: A Departmental Transformation

1. Vincent Vitto, "Final Report of the Defense Science Board Task Force on Strategic Communication" in *Report of the Defense Science Board Task Force on Strategic Communication*, (Washington, DC, Department of Defense, January 2008). https://www.intelink.gov/w/images/2/22/2008-01-Strategic_Communication.pdf (accessed January 12, 2010).

2. Defense Science Board, *Report of the Defense Science Board Task Force on Strategic Communication*, (Washington, DC, Department of Defense, January 2008), 21. https://www.intelink.gov/w/images/2/22/2008-01-Strategic_Communication.pdf (accessed January 12, 2010).

3. Richard Wike, "Repairing The U.S. Image In Muslim World: Our Reputation's On The Mend But Challenges Aplenty Remain," *CBS News*, July 29, 2009. http://www.cbsnews.com/stories/2009/07/29/opinion/main5195849.shtml (accessed January 12, 2010).

4. Michael Mullen, "Strategic Communication: Getting Back to Basics," *Joint Forces Quarterly*, issue 55, (4th quarter 2009), 4. http://www.ndu.edu/inss/Press/jfq_pages/ editions/i55/1.pdf (accessed January 15, 2010).

5. Ibid.

6. U.S. Representatives Adam Smith and Mac Thornberry, "Join the new Strategic Communication and Public Diplomacy Caucus," *Memorandum to Congress*, Washington, DC., March 2, 2010. http://mountainrunner.us/files/2010-3-2_SCPD_Caucus_Announcmement.pdf (accessed March 12, 2010).

7. U.S. Representative Mac Thornberry, "Establishing the Strategic Communication and Public Diplomacy Caucus" open posting on Mountainrunner, March 7, 2010, http://mountainrunner.us/2010/03/thornberry.html (accessed March 12, 2010).

8. Vincent Vitto, "Final Report of the Defense Science Board."

9. Mr. Price Floyd, acting ASD (PA) and PDASD (PA), interview with the author, Washington, DC, February 12, 2010.

10. Department of Defense, *Joint Publication 1-02, Dictionary of Military and Associated Terms*,12 April 2001, (As Amended Through 31 October 2009),2006. (Washington D.C.: U.S. Department of Defense, 31 October 2009), 518. http://www.dtic.mil/doctrine/new_pubs/jp1_ 02.pdf (accessed: January 4, 2010).

11. Department of Defense, "DOD Report on Strategic Communication (Section 1055(b))," December 14, 2009. (Washington DC., U.S. Department of

Defense, 14 December 2009), 2. https://www.intelink.gov/wiki/Image:TAB_B-Section_1055%28b%29_report_Dec_14.pdf (accessed January 15, 2010).

12. Ibid., 5-6.

13. Stanley McChrystal, "COMISAF Afghanistan assessment," *Washington Post*, September 21, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/09/21/AR2009092100110.html?hpid=topnews (accessed 11 January 2010).

14. Robert M. Gates, *Speech to the U.S. Global Leadership Campaign*, Washington, D.C., July 15, 2008, http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1262 (accessed March 2, 2010).

15. Defense Science Board, *Report of the Defense Science Boar*d, 11.

16. Since there is not official doctrine for SC, the three key areas described are the most common referenced and most important elements of SC. Some practitioners add Visual Information or Civil Affairs within SC. For the purposes of this paper I am using PA, IO, and DSPD.

17. Department of Defense, *DOD Report on Strategic Communication*, 7.

18. Mr. James Swartout, Director, Joint Communication, Office of Deputy Assistant Secretary of Defense for Joint Communication, interview by author, Washington DC, February 12, 2010.

19. Department of Defense, *DOD Report of Strategic Communication*, 5-6.

20. Ibid., 6.

21. Ibid., 7.

22. Ibid.

23. Ibid., 6-7.

24. Department of Defense., Joint Publication 3-13, Information Operations, (Washington D.C., Department of Defense, 13 February 2006) I-1. http://www.dtic.mil/doctrine/ new_pubs/jp3_13.pdf (accessed January 12, 2010).

25. Department of Defense, *DOD Report of Strategic Communication*, 7-8.

26. Ibid., 8.

27. Defense Science Board, *Report of the Defense Science Board*, xiii.

28. Department of Defense, *DOD Report of Strategic Communication*, 9.

29. Ibid., 9-10.

30. James Swartout, email message to author, March 23, 2010.

31. Hal Pittman, "Strategic Communication and Countering Ideological Support for Terrorism," *Congressional Record*, (November 15, 2007), http://www.carlisle.army.mil/dime/ documents/Pittman_Testimony111507.pdf (accessed December 15, 2009).

32. Ibid., 5.

33. Department of Defense, *2006 Quadrennial Defense Review Report*, (Washington D.C., Department of Defense, February 6, 2006), 92. http://www.comw.org/qdr/06qdr.html (accessed January 18, 2010).

34. Pittman, "Strategic Communication and Countering Ideological Support for Terrorism," 6-8.

35. Ibid., 8.

36. Ibid., 8.

37. Chairman of the Joint Chiefs of Staff Admiral Michael Mullen, "Strategic Communication," *Memorandum for the Deputy Secretary of Defense*, Washington D.C, December 14, 2007), http://www.carlisle.army.mil/DIME/documents/CJCS%20ADM%20Mullins%20memo%20to%20Deputy%20SecDef%20on%20Stategic%20Communication.pdf (accessed 15 Jan 2010).

38. Ibid.

39. Christopher J. Castelli, "Pentagon Terminates the Strategic Communications Integration Group," *Inside the Pentagon*, March 6, 2008. In LexisNexis Academic (accessed March 15, 2010).

40. Ambassador Brian E. Carlson, the State-Defense Strategic Communication Liaison from the Office of the Under Secretary of State for Public Diplomacy and Public Affairs, telephone interview with author, March 15, 2010. Note: Ambassador Carlson's tenure as the DoS-DoD SC Liaison was from September 2006 to December 2009, a total of 39 Months.

41. Various sources, Daniel P. Jordan, *The Demise of the Office of Strategic Influence, The National Security Strategy Process* (Washington D.C., NDU, January 14, 2004), 1. http://ics.leeds.ac.uk/papers/pmt/exhibits/1487/demiseofOSI.pdf (accessed March 10, 2010), Carlson, telephone interview with author, and Floyd, interview with the author.

42. Jordan, *The Demise of the Office of Strategic Influence*, 7.

43. Floyd, interview with the author.

44. Carlson, telephone interview with the author.

45. Swartout, interview with the author.

46. Department of Defense, *DOD Report of Strategic Communication*, 8-9.

47. Ibid., 9.

48. Floyd, interview with the author.

49. Ibid.

50. Ibid.

51. Swartout, interview with the author.

52. Ibid.

53. Christopher Paul, *Whither Strategic Communications? A Survey of Current Proposals and Recommendations*, (Santa Monica, CA., RAND Corp, February 25, 2009), v. http://www.rand.org/pubs/occasional_papers/2009/RAND_OP250.pdf (accessed (20 January 2010).

54. Ibid., 4.

55. Department of Defense, *2010 Defense Quadrennial Defense Review Report*, (Washington, DC, Department of Defense, February 2010), 25-26 and Department of Defense, 2006 Defense Quadrennial Defense Review Report, 91-92.

56. Department of Defense, *2006 Defense Quadrennial Defense Review Report*, 91-92.

57. Defense Science Board, *Report of the Defense Science Board*, xi.

58. U.S. Congress, Duncan Hunter, *National Defense Authorization Act for Fiscal Year 2009*, (Washington, DC, U.S. Congress, October 14, 2008) Section 1055. http://www.dod.mil/dodgc/olc/docs/2009NDAA_PL110-417.pdf (accessed February 15, 2010).

59. President of the United States Barack Obama, "Report on the Administration's Comprehensive Interagency Strategy for Public Diplomacy and Strategic Communication of the Federal Government." *Report to Congress* (section 1055), Washington DC, March 19, 2010.

60. Ibid., 7.

61. U.S. Congress, *National Defense Authorization Act for FY 2010*, (Washington, DC, U.S. Congress, June 18, 2009), 374. http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr 166&db name=111& (accessed February 15, 2010).

62. Carlson, telephone interview with the author.

63. Floyd, interview with the Author.

Section Two: Information Effects in the Cyberspace Domain

Russian Cyberspace Strategy and a Proposed U.S. Response

1. Cyber Security Strategy, Cyber Security Strategy Committee, Ministry of Defence, Estonia, Tallinn 2008, 3.

2. The inconsistent usage of cyber and related cyber terminology may be due to the relative newness of cyber as a domain. Therefore, unless using a direct quote, this paper will use cyber, along with its related term as one word (no space). For example, the author uses cyberspace, cyberattack, cyberdefense, and cyberdeterrence vice cyber space, cyber attack, cyber defense, and cyber deterrence.

3. Russians use the term "near abroad" in reference to the other fourteen former Soviet republics that declared independence when the Soviet Union was dismantled in 1991. "Russia The Near Abroad," http://www.photius.com/countries/russia/government/russia_government_the_near_abroad.html (accessed January 13, 2010).

4. *Cyber attacks disrupt Kyrgyzstan's networks*, January 30, 2009, http://www.securityfocus.com/brief/896 (accessed January 21, 2010).

5. U.S. Deputy Secretary of Defense Gordon England, "The Definition of Cyberspace'," memorandum for Secretaries of Military Departments, Washington, DC, dated 12 May 2008.

6. Deputy Secretary of Defense Memorandum, dated 15 Oct 2008.

7. Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," 12 April 2001, (As Amended Through 31 October 2009), 111.

8. Ibid.

9. Libicki, Martin C., "Cyberdeterrence and Cyberwar," 2009, linked from the RAND homepage at http://www.rand.org (accessed December 17, 2009).

10. *Joint Publication 1-02*, 374.

11. Ibid., 159.

12. Libicki, Martin C., "Cyberdeterrence and Cyberwar."

13. Ibid., 1.

14. Steven Blank, *Web War I: Is Europe's First Information War a New Kind of War?* (Carlisle Barracks, PA: Strategic Studies Institute, September 2008), 227.

15. Ibid., 227.

16. Libicki, "Cyberdeterrence and Cyberwar," 1.

17. Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," August 27, 2008, http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ (accessed January 8, 2010).

18. Blank, *Web War I*, 227.

19. James A. Hughes, "Cyber Attacks Explained," CSIS Commentary, Center for Strategic and International Studies, Washington, D.C., June 15, 2007, http://csis.org/files/media/csis/ pubs/070615_cyber_attacks.pdf (accessed December 28, 2009).

20. Geers, "Cyberspace and the Changing Nature of Warfare."

21. Blank, *Web War I*, 227.

22. Ibid., 228.

23. Ahto Lobjakas, "News Analysis: How Vulnerable Are Countries To Cyberattacks? Ask Estonia!," April 29 2008, http://www.rferl.org/content/article/1109653.html (accessed December 28, 2009).

24. Ibid.

25. Ibid.

26. NATO News, "NATO opens new centre of excellence on cyber defence", May 14, 2008, http://www.nato.int/docu/update/2008/05-may/e0514a.html (accessed December 28, 2009).

27. Kevin Coleman, "Cyber War 2.0 – Russia v. Georgia," August 13, 2008, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/ (accessed December 28, 2009).

28. Ibid.

29. Kesavan Unnikrishnan, "Google helps Georgia get back online after Russian cyber attack," August 12, 2008 http://www.digitaljournal.com/article/258508 (accessed January 12, 2010).

30. U.S. Cyber Consequences Unit. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," (U.S. Cyber Consequences Unit: August 2009), 5.

31. Benton Foundation, "Georgia States Computers Hit By Cyberattack", August 18, 2008, http://www.benton.org/node/16036 (accessed December 28, 2009).

32. Marcus H. Sachs, "Russian Business Network - Additional Analysis", November 22, 2007, http://isc.sans.org/diary.html?storyid=3681 (accessed January 8, 2010).

33. Jeremy Kirk, "Georgia cyberattacks linked to Russian organized crime," August 17, 2009, http://www.computerworld.com/s/article/9136719/Georgia_cyberattacks_linked_to_Russian_organized_crime?source=rss_news (accessed January 8, 2010).

34. John Markoff, "Before the Gunfire, Cyberattacks," August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed December 28, 2009).

35. Ibid.

36. Ibid.

37. Ibid.

38. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, (Washington, D.C.: National Defense University Press, 2009), 476.

39. Ibid., 477.

40. Geers, "Cyberspace and the Changing Nature of Warfare."

41. Ibid.

42. Kramer, *Cyberpower and National Security*, 476.

43. "Hitachi Data Systems Partners with Lenovo Group to Address Storage Needs in China," May 24, 2004, http://www.hds.com/corporate/press-analyst-center/press-releases/2004/gl040526a.html (accessed January 12, 2010).

44. Steve LeVine, "Cyber-Attack Strategy: Part of Russian Attack on Georgian Pipelines, Report Finds", August 24, 2009, http://www.energybulletin.net/node/49938 (accessed January 13, 2010).

45. Kramer, *Cyberpower and National Security*, 486-487.

46. Center for Strategic and International Studies, "Securing Cyberspace for the 44th Presidency," (Washington, D.C., December 2008), 1.

47. Ibid.

48. Ibid.

49. Michael G. Mullen, *Chairman of the Joint Staff Guidance for 2009-2010* (Washington, DC: December 21, 2009), 4.

50. The North Atlantic Treaty (Washington, DC, April 4, 1949), http://www.nato.int/cps/ en/natolive/official_texts_17120.htm (accessed December 28, 2009).

51. Bruce D. Caulkins, *Proactive Self-Defense in Cyberspace, Strategy Research Project* (Arlington, VA: Institute of Land Warfare, 2009), 9.

52. Ibid.

53. Susan Brenner, "Networks and Nationalization," Jul 21, 2009, http://www.circleid.com/posts/networks_and_nationalization/ (accessed January 13, 2010).

54. Ibid.

55. Ibid.

56. Shane Harris, “The Cyberwar Plan,” November 14, 2009, linked from *National Journal Magazine* Home Page at http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (accessed January 13, 2010).

57. There are numerous cyberstrategists that will argue for and against cyberspace as a new common.

58. Kramer, et al, eds., *Cyberpower and National Security*, 313.

59. Libicki, “Cyberdeterrence and Cyberwar,” 7.

60. Ibid.

61. Ibid., 18.

62. Howard F. Lipson, “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,” (Pittsburgh, PA: Carnegie Mellon Software Engineering Institute November 2002).

63. George W. Bush, *The National Security Strategy to Secure Cyberspace*, (Washington, D.C.: The White House, February 2003), x.

64. Kramer, et al., eds., *Cyberpower and National Security*, 328.

65. Ibid.

66. Ibid., 486.

67. U.S. CCU. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008,” 8.

68. Kramer, et al, eds., *Cyberpower and National Security*, 332.

69. Ibid., 106.

70. Brian Prince, “Cyber-attacks on Georgia Show Need for International Cooperation, Report States,” August 18, 2009, http://www.eweek.com/c/a/Security/Cyber-Attacks-on-Georgia-Show-Need-for-International-Cooperation-Report-States-294120/ (accessed January 12, 2010).

71. U.S. CCU. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008,” 7.

72. Stephen Korns, “Botnets Outmaneuvered,” January 2009, linked from The *Armed Forces Journal* home page at http://www.armedforcesjournal.com/2009/01/3801084/ (accessed December 29, 2009).

73. U.S. CCU. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008,” 7.

74. Center for Strategic and International Studies, “Securing Cyberspace for the 44th Presidency,” 43.

75. Caulkins, *Proactive Self-Defense in Cyberspace*, 11.

76. Libicki, “Cyberdeterrence and Cyberwar,” 137.

77. Kramer, et al, eds., *Cyberpower and National Security*, 476.

78. Geers, "Cyberspace and the Changing Nature of Warfare."

79. Barack Obama, "Remarks by the President on Securing our Nation's Infrastructure," May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed January 13, 2010).

Keeping Up with the Drones: Is Just War Theory Obsolete?

1. General Omar Nelson Bradley, http://www.quotes.net/quote/11181 (accessed January 4, 2010).

2. "The Drone War," *The American Legion Magazine*, 4, http://www.tagyouitonline.com (accessed August 27, 2009).

3. Dan Murphy, "Drones as Weapons of War," *The Christian Science Monitor*, May 17, 2009: 12, in ProQuest (accessed October 20, 2009).

4. John J. Kruzel, "Official Hails Effect of Unmanned Aircraft on Warfare," *American Forces Press Service*, May 25, 2010, http://www.defense.gov (accessed March 30, 2010).

5. "Just War Theory," *The Internet Encyclopedia of Philosophy*, http://www.utm.edu/research/iep/j/justwar.htm (accessed September 5, 2009).

6. Brian Orend, *The Morality of War* (Ontario: Broadview Press, 2006), 10.

7. "ACLU Requests Information on Predator Drone Program," January 13, 2010, http://www.aclu.org (accessed April 1, 2010).

8. Ari Shapiro, "Official Makes Case for Deadly Drone Strikes," March 26, 2010, http://www.npr.org/templates/story (accessed April 1, 2010).

9. David Drayden, "Harold Koh Tries to Rationalize Legality for Drone Attacks," March 26, 2010, http://news.firedoglake.com (accessed April 1, 2010).

10. Shapiro, "Official makes Case for Deadly Drone Strikes," (accessed April 1, 2010).

11. Drayden, "Harold Koh Tries to Rationalize Legality for Drone Attacks."

12. Kruzel, "Official Hails Effect of Unmanned Aircraft on Warfare."

13. www.japcc.org, presentation on *Unmanned Aircraft Systems in NATO*, datrd 11 June 2009, authored by Lieutenant Colonel Jens Fehler, C4ISTAR Branch, Joint Air Power Competence Center, Kalkar, Germany, accessed 1 April 2010

14. Murphy, "Drones as Weapons of War," 12.

15. P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: The Penguin Press, 2009), 33.

16. Ibid, 36.

17. Ibid, 32.

18. Murphy, "Drones as Weapons of War," 12.

19. Ibid.

20. Robert Sparrow, "Killer Robots," *Journal of Applied Philosophy* 24, no. 1 (2007): 63.

21. Fred Kaplan, "Attack of the Drones; Now that Congress has Killed the F-22, the Air Force is Facing Another Shock to the System: Planes without Pilots," *Newsweek* 154, iss. 13 (September 28, 2009): 4, in ProQuest (accessed October 20, 2009).

22. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 194.

23. Kaplan, "Attack of the Drones; Now that Congress has Killed the F-22, the Air Force is Facing Another Shock to the System: Planes without Pilots," 4.

24. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 37.

25. Karl A. Kaszuba, "Military Technology: Has it Changed the Rules of Warfare?," (Maxwell Air Force Base, Alabama), 2, http://www.au.af.mil/au/awc/awcgate/awc/97-103.pdf (accessed January 10, 2010).

26. Eric Patterson, "Just War in the 21st Century: Reconceptualizing Just War Theory after September 11," *International Politics* 42 (2005): 117.

27. "Just War Theory," *The Internet Encyclopedia of Philosophy*, 2.

28. "War," *Stanford Encyclopedia of Philosophy*, 4, http://plato.stanford.edu/entries/war (accessed September 5, 2009).

29. Orend, *The Morality of War*, 21.

30. "Just War Theory," *The Internet Encyclopedia of Philosophy*, 8.

31. Orend, *The Morality of War*, 105.

32. "Just War Theory," *The Internet Encyclopedia of Philosophy*, 8.

33. Ibid.

34. Orend, *The Morality of War*, 107.

35. Patterson, "Just War in the 21st Century: Reconceptualizing Just War Theory after September 11," 119.

36. Doyle McManus, "The Cost of Killing by Remote Control," *Los Angeles Times* (May 3, 2009): 38, in ProQuest (accessed October 20, 2009).

37. Jerrold Kessel and Pierre Klochendler, "Mideast: When Drones Become Indiscriminate," *Global Information Network* (July 1, 2009), in ProQuest (accessed October 20, 2009).

38. Human Rights Watch, "Precisely Wrong," June 30, 2009, 24, http://www.hrw.org/en/reports/2009/06/30/precisely-wrong?print (accessed October 20, 2009).

39. "Just War Theory," *The Internet Encyclopedia of Philosophy*, 8.
40. Patterson, "Just War in the 21st Century: Reconceptualizing Just War Theory after September 11," 119.
41. Ibid., 357.
42. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 128.
43. Ibid., 356.
44. Ibid., 11.
45. Suzy Killmister, "Remote Weaponry: The Ethical Implications," *Journal of Applied Philosophy* 25, no. 2 (2008): 129.
46. "Just War Theory," *The Internet Encyclopedia of Philosophy*, 11.
47. Killmister, "Remote Weaponry: The Ethical Implications," 129.
48. Ibid.
49. Ibid., 130.
50. The New Yorker, *The Predator War*, by Jane Mayer p. 4
51. "War," *Stanford Encyclopedia of Philosophy*, 10.
52. Killmister, "Remote Weaponry: The Ethical Implications," 122.
53. Orend, *The Morality of War*, 107.
54. Sparrow, "Killer Robots," 67.
55. Ibid.
56. Orend, *The Morality of War*, 117.
57. Karl A. Kaszuba, "Military Technology: Has it Changed the Rules of Warfare?," 7.
58. "Just War Theory," *The Internet Encyclopedia of Philosophy*, 2.
59. Patterson, "Just War in the 21st Century: Reconceptualizing Just War Theory after September 11," 121.
60. Ibid.
61. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 2.
62. McManus, "The Cost of Killing by Remote Control," 38.
63. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 331.
64. Ibid., 332.
65. Ibid.
66. Sparrow, "Killer Robots," 70.

67. Human Rights Watch, “Precisely Wrong,” 4.

68. Ibid., 10.

69. Ibid.

70. Ibid.

71. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 395.

72. Susan Leigh Anderson, “Asimov’s ‘three laws of robotics’ and Machine Metaethics,” February 2, 2007, 483, http://www.springerlink.com/content/771k1181268772p1 (accessed November 17, 2009).

73. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 394.

74. Ibid., 59.

75. LandWarNet Conference Remarks by the Secretary of the Army in Fort Lauderdale, FL, August 21, 2007, http://www.army.mil/-speeches/2007/08/21/4547-landwarnet-conference-remarks (accessed July 23, 2009).

76. Ibid.

77. Ibid.

78. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 386.

79. Ibid., 385.

80. Ibid.

81. Ibid., 411.

82. Ibid., 396.

83. Kevin Clarke, “The Drone Wars,” *U.S. Catholic* 74, iss. 6 (June 2009): 46, in ProQuest (accessed September 27, 2009).

84. Ibid.

85. “War,” *Stanford Encyclopedia of Philosophy*, 14.

86. Orend, *The Morality of War*, 223.

87. Fred Reed, “Remote Weapons Could Backfire,” *The Washington Times* (February 3, 2007): 11, in LexisNexis Academic (accessed October 27, 2009).

88. Ibid.

Reflections on a Strategic Vision for Computer Network Operations

1. Bible.com Homepage, “King James Bible,” http://bibleresources.bible.com/passagesearchresults2.php?passage1=Proverbs+29&book_id=24&version1=9&tp=31&c=29 (accessed 7 May 2010).

2. For background on the requirements of the Military Departments to "develop and procure weapons, equipment, and supplies essential to the fulfillment of the functions assigned," see U.S. Department of Defense, *Functions of the Department of Defense and its Major Components*, Department of Defense Directive (DODD) 5100.1 (Washington, DC: Department of Defense, November 21, 2003), 13.

3. For unclassified background on the role of the GCC's, see U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, May 2, 2007 Incorporating Change 1 dated March 20, 2009), I-14. Generally, GCC authority is limited to the creation of effects contained within the geographic boundaries of the commander's area of responsibility (AOR). The global nature of cyberspace causes a concern that GCC-initiated CNA will cause trans-regional effects. For unclassified, official use only background on the role of combatant commanders to plan and conduct cyberspace operations, see George W. Bush, *The Unified Command Plan*, (Washington, DC: The White House, December 2008).

4. U.S. Joint Chiefs of Staff, *Joint Communication Systems*, Joint Publication 6-0, (Washington, DC: U.S. Joint Chiefs of Staff, 10 June 2010), xi. For additional unclassified, but official use only background on the role of combatant commanders to plan and conduct cyberspace operations, see George W. Bush, *The Unified Command Plan*, (Washington, DC: The White House, December 2008). Also see U.S. Strategic Command, *USCYBERCOM Announcement Message*, J3 Director of Global Operations Record Message DTG 212106Z May 2010 (Offutt AFB, NE: U.S. Strategic Command, May 21, 2010).

5. David Jablonsky, "Strategic Vision and Presidential Authority in the Post Cold-War Era," *Parameters* XXI, no. 4 (Winter 1991-92): 2.

6. Glenda Y. Nogami, *What is This Thing called Strategic Vision?*, U.S. Army War College paper presented at the International Military Testing Association Annual Convention in Rotterdam, The Netherlands, 1994 (Carlisle Barracks, PA: U.S. Army War College, 1994), 4.

7. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret, (Princeton, NJ: Princeton University Press, 1989), 608.

8. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: U.S. Joint Chiefs of Staff, 12 April 2001, as Amended Through 13 June 2007). There is no definition for "cyberspace war" or "cyberwar" in this authoritative DOD publication.

9. A general description of cyberwar developed by the author.

10. Martin C. Libicki, "Cyberdeterrence and Cyberwar," RAND Project Air Force, (2009): 117.

11. Libicki, "Cyberdeterrence and Cyberwar," 1119.

12. The 2007 cyberattack against the country of Estonia is an example of strategic level cyberwar that failed to be decisive. When the government of Estonia, a member of NATO, decided to move an historic statue that memorialized Soviet war dead to a less prominent location in its capital city, Russian patriots objected. Continued Estonian recalcitrance resulted in a massive distributed denial of service (DDOS) cyberattack against various government, financial, police, and emergency response websites. While not proven, these strategic level attacks presumably originated from within Russia and by Russian operatives around the world. This campaign of cyber attacks did not have an accompanying Russian physical attack. Consequently, the Estonians continued to move the statue. For more information on this ultimately indecisive cyberwar, see Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 29, 2007.

13. Libicki, "Cyberdeterrence and Cyberwar," 122.

14. Ibid., 139.

15. Ibid., 117.

16. Ibid., 140.

17. The 2008 cyberattack against the country of Georgia is an example of operational cyberwar conducted in a manner supportive of a successful Russian physical attack against Georgian forces. South Ossetia, a relatively autonomous and demilitarized region of Georgia on the Georgian-Russian border, sought independence from Georgia. An independent South Ossetia served the strategic interests of Russia but not those of Georgia. As the Georgian government moved forces into South Ossetia to restore its territory, it experienced a significant campaign of cyber attacks, presumably of Russian origin. While this cyber attack was ongoing, Russian forces entered South Ossetia and moved against those of Georgia. Georgian forces were successfully defeated. For more background on how this operational cyberwar proved to be decisive in support of operational maneuver rather than directly achieve the Russian strategic end state, see Eneken Tikk, et al, *Cyber Attacks against Georgia: Legal Lessons Learned*, (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, November 2008).

18. Ibid., 142.

19. Ibid., 156. Libicki's argument that military operators are better suited to plan military operations is consistent with the premise underscoring a broader role for the GCC's in planning and executing CNO. Military operators are the most capable of creating the military advantages necessary to win battles. The IC is better suited to informing operational decision-makers about enemy capabilities and intentions.

20. Ibid., Libicki, 6. Libicki writes, "operational cyberwar – cyber attacks to support warfighting, may have far greater purchase than strategic cyberwar – cyber attacks to affect state policy." This paper addresses many of the national

and strategic policy documents that describe the preponderant U.S. focus on strategic cyber concerns. For a good reference on the current lack of similar emphasis at the operational and tactical levels, see Andre Abadie, www.kasserinepass.com: *Determining the U.S. Army's Readiness for Tactical Operations in Cyberspace*, Master's Thesis, (Fort Leavenworth, KS: Army Command and General Staff College, December 6, 2009).

21. Christopher J. Castelli, "Defense Department Adopts New Definition of Cyberspace," *Inside the Air Force*, 23 May 2008, http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm (accessed 1 May 2010).

22. U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, (Washington, DC: U.S. Joint Chiefs of Staff, September 17, 2006 incorporating change 1 dated February 13, 2008), III-1.

23. Ibid., II-2.

24. Dr. Lani Kass, "Cyberspace: A Warfighting Domain," briefing slides, Headquarters, U.S. Air Force, Washington, DC, September 2006, slide 14.

25. Vice Chairman of the Joint Chiefs of Staff, General James E. Cartwright, "Definition of Cyberspace Operations," action memo for Deputy Secretary of Defense, (Washington, DC: September 29, 2008).

26. U.S. Joint Chiefs of Staff, *Joint Communication Systems*, Joint Publication 6-0, (Washington, DC: U.S. Joint Chiefs of Staff, 20 March 2006), GL-11.

27. Ibid., II-1.

28. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, 111.

29. U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: U.S. Joint Chiefs of Staff, 13 February 2006), GL-6.

30. Ibid.

31. Ibid., GL-5.

32. Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006) GL-1. An unclassified, publically accessible, redacted copy of the classified NMS-CO, accessed at http://www.carlisle.army.mil/DIME/documents/National%20Military%20Strategy%20for%20Cyberspace%20Operations.pdf. The redacted NMS-CO presents an unclassified definition of CNA-OPE. For the purpose of this research paper, however, the author has chosen not to quote it verbatim to avoid confusion with its classified counterpart. The author's description intends to capture the essence of the activity at the unclassified level.

33. U.S. Joint Chiefs of Staff, *Information Operations*, GL-5.

34. Chairman of the Joint Chiefs of Staff, *Information Assurance (IA and Computer Network Defense (CND)*, Chairman of the Joint Chiefs of Staff Instruction

6510.01, (Washington, DC: Chairman of the Joint Chiefs of Staff, 15 August 2007), GL-7.

35. John Mense, *Basic Computer Network Operations Planners Course (BCNOPC) Manager*, Army 1st Information Operations Command (LAND), interview by author, Ft. Belvoir, VA, 24 May 2010.

36. George W. Bush, *The National Security Strategy of the United States of America*, (Washington, DC: The White House, March 2006), 43.

37. Ibid., 43-44.

38. George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), v.

39. Catherine A. Theohary and John Rollins, *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*, CRS Report for Congress (Washington, DC: Congressional Research Service, 30 September 30, 2009), 4. (accessed at http://www.crs.gov)

40. Executive Office of the President, *Cyberspace Policy Review*, (Washington, DC: The White House, May 2009), Executive Summary. (accessed at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA501541&Location=U2&doc=GetTRDoc.pdf).

41. DefenseLink-Unified Command Plan Homepage, accessed at http://www.defense.gov/specials/unifiedcommand/ on 1 May 2010.

42. USSTRATCOM Homepage, accessed at http://www.stratcom.mil/mission/ on 1 May 2010.

43. George W. Bush, *The Unified Command Plan*, (Washington, DC: The White House, May 2006), 13-14. An unclassified, publically accessible, redacted copy of Unclassified//For Official Use Only 2006 UCP, accessed at http://www.dod.gov/pubs/foi/ojcs/08-F-0518.pdf.

44. Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, 10. Reference from the unclassified, redacted version.

45. Ibid., 11.

46. Ibid., F-3.

47. Ibid., F-1.

48. Ibid., 11.

49. Joint Electronic Library Webpage, *Joint Doctrine Hierarchy*, accessed at http://www.dtic.mil/doctrine/doctrine/status.pdf on 3 May 2010.

50. Joint Chiefs of Staff, *Joint Communication Systems*, XIII.

51. Ibid., I-11.

52. U.S. Joint Chiefs of Staff, *Information Operations*, IX.

53. "Dual-hatted" in this instance means that the same officer commands both JFCC-NW and NSA.

54. U.S. Secretary of Defense Robert M. Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under US Strategic Command for Military Cyberspace Operations," *Memorandum for Secretaries of the Military Departments*, Washington, DC, June 23, 2009. Accessed at http://docs.govinfosecurity.com/files/external/OSD-05914-09.pdf on 10 June 2010.

55. U.S. Department of Defense, "Petraeus Cites Need for Critical Warfighting Specialties," *Defense and Security News*, 28 September 2009, accessed at http://www.defencetalk.com/critical-warfighting-specialties-22207/on 20 May 2010.

56. Ellen Nakashima, "Cyber Warfare: Challenges of the Unknown," *Washington Post*, 19 March 2010, accessed at http://www.cbsnews.com/stories/2010/03/19/politics/washingtonpost/main6313925.shtml on 20 May 2010.

57. Major M. Bodine Birdwell, USAF, *If You Don't Know Where You are Going, You Probably Will End Up Somewhere Else: Computer Network Operations Force Presentation*, Graduate Research Project, (Wright Patterson Air Force Base, OH: Air Force Institute of Technology, June 2009), 37.

58. Eneken Tikk et al, *Cyber Attacks against Georgia: Legal Lessons Learned*, (Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence, November 2008), 4-5. This is an excellent case study of the cyberattacks against the country of Georgia that coincided with a Russian ground force operation.

Strategic Impact of Cyberwarfare Rules for the United States

1. Barack H. Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House, Washington, DC, May 29, 2009.

2. U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, *Cybersecurity and Science and Technology, Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action*, 110th Cong., 1st sess., April 25, 2007.

3. Amber Corrin, "Cyber warfare: Sound the alarm or move ahead in stride?" *Federal Computer Week*, October 15, 2009, http://fcw.com/Articles/2009/10/19/FEAT-DOD-cyber-warfare.aspx?Page=5&p-1 (accessed October 23, 2009).

4. "Leaders: Battle is joined; Cyberwar," *The Economist*, April 25, 2009, 20.

5. U.S. Congress, Senate, Senate Select Committee on Intelligence's 15th Annual World-Wide Threat Hearing, *Current and Projected National Security Threats to the United States*; 111th Cong., 1st sess., February 12, 2009: 8.

6. Corrin, "Cyber warfare."

7. "Leaders," 20.

8. U.S. Congress, Senate, *Current and Projected National Security Threats*, 8-9.

9. Ibid.

10. U.S. Congress, House of Representatives, House Subcommittee on Emerging Threats, *Cybersecurity and Science and Technology, Securing the Modern Electric Grid from Physical and Cyber Attacks*, 111th Cong. 1st sess., July 21, 2009.

11. Gen Kevin Chilton, U.S. Air Force, "U.S. Strategic Command – Cyber and Space Defense," interview by Lynn Neary, National Public Radio, August 11, 2009.

12. U.S. Congress, House of Representatives, *Securing the Modern Electric Grid*.

13. Gen. Chilton, "U.S. Strategic Command."

14. Corrin, "Cyber warfare."

15. Kevin Coleman, "The 2010 Cyber Threat Environment," January 11, 2010, http://defensetech.org/category/cyber-warfare/ (accessed on January 12, 2010).

16. Gen. Chilton, "U.S. Strategic Command."

17. U.S. Congress, Senate, *Current and Projected National Security Threats to the United States*.

18. U.S. Congress, House of Representatives, *Securing the Modern Electric Grid*.

19. Maj Arie J. Schaap, U.S. Air Force, "Cyber Warfare Operations: Development and Use Under International Law," *The Air Force Law Review*, 2009; 64, Military Module, 123.

20. Duncan B. Hollis, "Rules of Cyberwar?" *Los Angeles Times*, October 8, 2007.

21. Col Jeffrey Caton, *What do Senior Leaders Need to Know about Cyberspace?* (Carlisle Barracks, PA: U.S. Army War College), 4.

22. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, (Washington DC: U.S. Department of Defense, 12 April 2001, as amended through 17 October 2008), 141.

23. Computer network attack (and counter attack) is action taken to destroy nodes or links or disrupt transactions in cyberspace that may or may not have intended second order effects in other domains (i.e. land, sea, air and space). Computer network exploitation is action taken to gather intelligence in cyberspace.

24. United Nations, "Charter of the United Nations," http://www.un.org/en/documents/charter/chapter1.shtml (accessed January 6, 2010).

25. United Nations, General Assembly Resolution 3314, "Definition of Aggression," December 14, 1974, http://www.un-documents.net/a29r3314.htm (accessed January 6, 2010).

26. United Nations, "Charter of the United Nations."

27. United Nations, "Definition of Aggression." Note that the complete Article 3 lists seven acts of aggression, all of which apply to State actors.

28. Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009, 179.

29. Hollis, "Rules of Cyberwar?"

30. Libicki, *Cyberdeterrence and Cyberwar*, iii.

31. Webster's New World College Dictionary

32. Hollis, "Rules of Cyberwar?"

33. Thomas C. Wingfield, "The Law of Information Conflict: National Security Law in Cyberspace" (Aegis Research Corp., 2000), 352-3.

34. "U.S. Joins Council of Europe Convention on Cybercrime," *U.S. Federal News Service*, Washington D.C., September 29, 2006.

35. Kristin Archick, "Cybercrime: The Council of Europe Convention," *CRS Report for Congress* RS21208, September 28, 2006, 1.

36. Council of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001, 2.

37. Ibid., 4-5.

38. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (accessed February 12, 2010).

39. Stephen W. Korns, and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, (Winter 2008-09): 60.

40. Schaap, "Cyber Warfare Operations,"147.

41. John Markoff and Andrew E. Kramer, "U.S., Russia disagree on cyberspace treaty; Nations to address handling growing threat of attacks," *The Boston Globe*, June 28, 2009.

42. U.S. Congress, Senate, *Current and Projected National Security Threats*, 72.

43. Ibid.

44. Schaap, "Cyber Warfare Operations,"149–53.

45. Korns and Kastenberg, "Georgia's Cyber Left Hook," 61.

46. Jeffrey T. G. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," *Michigan Law Review*, 106 (May 2008): 1444.

47. Korns and Kastenberg, "Georgia's Cyber Left Hook," 63.

48. Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review*, 11:4, 1023-24.

49. When two or more laws contradict, the more specific law has precedence over the general law.

50. Hollis, "Why States Need an International Law." 1023-24.

51. Ibid, 1028.

52. Schaap, "Cyber Warfare Operations," 146.

53. Tony Bradley, "Pandora's Box," http://netsecurity.about.com/library/weekly/aa031703b.htm (accessed on 11 February 2010).

54. Clay Wilson, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress," CRS Report for Congress, October 17, 2003, http://www.fas.org/irp/crs/RL32114.pdf (accessed 11 February 2010).

55. Rita Roland, "Government Works to Stop Actual Bad Guys in the Virtual Realm," *Signal*, March 2009, 57-60.

56. Paul Ames, "NATO allies sign agreement to fund center to boost defenses against cyberattacks," *Associated Press Worldstream*, May 14, 2008.

57. Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*, Vol. 8, No. 1, October 2008, 43.

58. Siobhan Gorman, "World News: Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs," *Wall Street Journal*, August 17, 2009, A.5.

59. Hollis, "Why States Need an International Law," 1024.

60. Amber Corrin, "Some key events in the history of cyber warfare," *Federal Computer Week*, October 15, 2009, http://fcw.com/Articles/2009/10/19/FEAT-DOD-cyber-timeline.aspx?p=1 (accessed October 23, 2009).

61. Ibid.

62. Ibid.

63. Ibid.

64. Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," *New York Times*, July 9, 2009, http://www.nytimes.com//2009/09/10/technology/10cyber.html (accessed January 7, 2010).

65. Gorman, "World News," A5.

66. Korns and Kastenberg, "Georgia's Cyber Left Hook," 65.

67. Eneken Tikk et al, "Cyber Attacks Against Georgia: Legal Lessons Identified," http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (accessed January 11, 2010).

68. Gorman, "World News," A.5.

69. Korns and Kastenberg, "Georgia's Cyber Left Hook," 65, and "War, redefined; Even before Russian troops arrived, Georgian government websites were under cyber attack," *Los Angeles Times*, August 17, 2008, A25.

70. Korns and Kastenberg, "Georgia's Cyber Left Hook," 67.

71. Peter Svenson, "Georgian President's Web Site Moves to Atlanta," *Associated Press News*, August 11, 2008, http://www.usatoday.com/tech/products/2008-08-11-2416394828_x.htm (access January 11, 2010).

72. Steven Adair, "Website for the President of Georgia Under Distributed Denial of Service Attack," *CyberInsecure.com*, July 20, 2008, http://cyberinsecure.com/website-for-the-president-of-georgia-under-distributed-denial-of-service-attack/ (accessed January 17, 2010).

73. Svenson, "Georgian President's."

74. Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *The Washington Post*, October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/ report_russian_hacker_forums_f.html (accessed January 12, 2010).

75. Gorman, "World News," A.5.

76. Hollis, "Why States Need an International Law," 1025.

77. Gorman, "World News," A.5.

78. Ibid.

79. Amber Corrin, "Cyber Warfare: Sound the alarm or move ahead in stride?" *Federal Computer Week* online, October 15, 2009, http://fcw.com/Articles/2009/10/19/FEAT-DOD-cyber-warfare.aspx?sc_lang=en&Page=1 (accessed January 12, 2010).

80. "War, redefined; Even before Russian troops arrived, Georgian government websites were under cyber attack," *Los Angeles Times*, A25.

81. Katie Paine, "Reputation Redux: Russia Invades Georgia by Land and by Server," *PR News*, August 25, 2008, Vol. 64, Issue 33.

82. Korns and Kastenberg, "Georgia's Cyber Left Hook," 70.

83. Gorman, "World News."

84. William J. Lynn, Deputy Secretary of Defense, Cyber Security, *Speech at the Center for Strategic and International Studies*, June 15, 2009 (Washington D.C.).

85. Maryann Lawlor, "Launching stealth warfare; Attacks in cyberspace may be prelude to future conventional conflicts," *Signal*, March 2009, 63, 7, 47-50.

86. U.S. Congress, House of Representatives, *Securing the Modern Electric Grid*.

87. Kevin Coleman, "McAfee's Take on the Cyber War," November 23, 2009, http://defensetech.org/category/cyber-warfare/ (accessed January 12, 2010).

88. Lawlor, "Launching Stealth Warfare," 47-50.

89. Gen Robert Keller, "Military must look at cyberspace as an 'urban environment,'" *Inside the Air Force*, July 17, 2009, http://www.insideddefense.com/secure/display.asp?docnum=AIRFORCE-20-28-6&f=defense (accessed October 1, 2009).

90. U.S. Secretary of Defense Robert M. Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for military

Cyberspace Operations," *Memorandum for Secretaries of the Military Departments*, Washington D.C., June 23, 2009.

91. Charles Billo & Welton Change, "Cyber Warfare Analysis of the Means and Motivations of Selected Nation States," http://ists.dartmough.edu/docs/execsum.pdf (accessed January 12, 2010).

92. Kevin Coleman, "Russia's Cyber Forces," *Defensetech.org*, http://www.defensetech.org/archives/cat_cayberwarfare.html (accessed January 10, 2010).

93. Schaap, "Cyber Warfare Operations," 133.

94. Corrin, "Cyber warfare."

95. U.S. Congress, House of Representatives, *Securing the Modern Electric Grid.*

96. Lynn, *Cyber Security.*

97. Corrin, "Cyber warfare."

98. Richard Mereand, "Securing Cyberspace: Guarding the New Frontier," *National Security Watch*, The Institute of Land Warfare, August 25, 2009, 2.

99. Gen Chilton, "U.S. Strategic Command."

100. Renata Goldirova, "NATO picks Estonia for high-tech crime centre," May 15, 2008, http://euobserver.com/?aid=26138 (accessed February 12, 2010).

101. Corrin, "Cyber warfare."

102. Lynn, *Cyber Security.*

103. Ibid.

104. Korns and Kastenberg, "Georgia's Cyber Left Hook," 70.

105. Schaap, 173.

106. Coleman, "McAfee's Take."

107. Korns and Kastenberg, "Georgia's Cyber Left Hook," 72.

108. John Lister, "Are cyber-attacks an act of war?" August 16, 2008, http://tech.blorge.com/Structure:%20/2008/08/16/are-cyber-attacks-an-act-of-war/ (accessed January 12, 2010.)

109. Korns and Kastenberg, "Georgia's Cyber Left Hook," 72.

110. Lister, "Are cyber-attacks an act of war?"

111. Kevin Coleman, "A Thaw in the Cyber Cold War," December 14, 2009, http://defensetech.org/category/cyber-warfare/ (accessed January 12, 2010).

112. Korns and Kastenberg, "Georgia's Cyber Left Hook," 62.

113. Lynn, *Cyber Security.*

114. Coleman, "A Thaw in the Cyber Cold War."

115. Kevin Coleman, "The Time for Preemptive Cyber Strikes Has Come," January 4, 2010, http://defensetech.org/category/cyber-warfare/ (accessed January 12, 2010).

116. Gen Chilton, “U.S. Strategic Command.”

117. Bradley, “Pandora’s Box.”

Prudens Futuri

Prudens Futuri

CSL
CENTER *for*
STRATEGIC
LEADERSHIP