The American public discourse on terrorism has been completely transformed since 9/11.¹ Not since the first Gulf War in the early 1990s had the geography of the Middle East and South Asia received such a penetrating look by American media. And not since the fall of the Shah in 1979 had the tenants of Islam been kitchen-table conversations across the United States, and even the world. The transformation of discourse that was taking place on the American main street was also taking place within the intelligence community. However, the transformation within the intelligence community was of a different nature and held significantly different consequences. Today, likely to an unprecedented degree, the way language is used has taken on a crucial role in the description and understanding of modern-day terrorism.

Language is subjective. It is used to convey meaning and ideas among people, and each person applies his or her own enculturated ideas to understand the meaning of words and utterances. How should we deal with the challenge of ethically communicating threat in the national security context?

The way in which the U.S. government communicates threats to the public has been profoundly impacted by the events on and after 9/11. Writers, scholars, and public intellectuals have noted that the use of certain terminology by government officials and politicians has contributed to a polarizing debate on the mere existence and severity of threats to the American public. Social scientists and communication experts both agree that lexicon and usage in the context of modern terrorism can encourage certain interpretations and discourage others. Words and phrases lead to associations and implications that may or may not be factually accurate. This article will review and analyze the modern comprehension, identification, and
the normative discourse of national security threats of terrorism to the United States post 9/11. This review and analysis is particularly important because the nature and scope of national security threats, particularly on U.S. soil, appears to have had a troubling increase in recent years.² This increase carries with it a greater need for government and law enforcement officials to communicate these threats to the American public, both to ensure the public’s safety and to articulate protective measures, policies, and principles.

**Setting the Stage**

First, we need to assess what the measurements of ethical communication are. This is an interdisciplinary process that involves multiple social sciences. Therefore, a baseline measurement in specific fields needs to be established. This assessment needs to also involve technical data of how “ethics” and “communication” are measured.

The centrality of publicly available information related to threats is a key part of the post-9/11 environment. The culture of the intelligence community (and national security environment at large) that currently exists is one that is suspended somewhere between the slightly wavering notions of a country that is currently waging a war abroad with massive troop deployments in Iraq and Afghanistan and the increasing fervor around publicly foiled terrorist plots in the United States.³

Negotiating ethical principles in the context of the communication of national security threats is modern reality for any targeted state or democracy. The benefits to this ethical communication to both internal and external government and security agencies are almost self-fulfilling. Internally, ethical communication of the threat preserves the integrity of analytic units and personnel by shielding them from hasty claims of political motivation and bias. Additionally, ethical communications deepen the relationship with allied countries. These international relationships and alliances are socially, politically, and economically complex. Thus, to communicate a national security threat in such a way shows transparency, precision accuracy, and ethical values/considerations, further strengthening these international alliances.

Debates over semantics plague Washington, D.C., and most political environments worldwide. Words do matter, and how threats are communicated have a range of consequences, both positive and
negative. Specifically, the debate rages over acts of terrorism committed by those of the Muslim faith. For those who purport to be in firm adherence of the Muslim faith, their acts of terrorism and political violence are especially under the microscope. For example, debates over the usage and application of the term *jihad* have been ongoing almost since the day after the 9/11 attacks. These debates in media, at times, attempted to explore the foundational and historical meaning of the term and its application, but it largely failed to do so.⁴

According to John Collins and Ross Glover, authors of *Collateral Language*, the understanding of language becomes especially important when thinking through the developments since 9/11.⁵ They point out that a perceptual system emerged linking up any person who appeared "as if" they are Middle Eastern.⁶ According to Collins and Glover, "[T]he immediate increase in racially motivated crimes after the bombings demonstrates the significance of these perceptions."⁷ Furthermore, according to the website for the Civil Rights Division at the U.S. Department of Justice: "[We have] placed a priority on prosecuting bias crimes and incidents of discrimination against Muslims, Sikhs, and persons of Arab and South-Asian descent, as well as persons perceived to be members of these groups."⁸ The FBI, in conjunction with the U.S. attorney’s offices, have investigated over eight hundred incidents since 9/11 involving "violence, threats, vandalism and arson against Arab-Americans, Muslims, Sikhs, South-Asian Americans and other individuals perceived to be of Middle Eastern origin."⁹ These investigations are of "telephone, internet, mail, and face-to-face threats; minor assaults as well as assaults with dangerous weapons and assaults resulting in serious injury and death; and vandalism, shootings, arson and bombings directed at homes, businesses, and places of worship."¹⁰ Because this post-9/11 perceptual system has been created that links people who are, or are perceived to be, of Middle Eastern descent to terrorism, a rhetorical precedent has been created. Author, academic, and media analyst Noam Chomsky, who has written extensively about the corrosive effect this rhetorical precedent has had on American society in the post-9/11 era, further underscores the point that the manufacturing consent of language and images of terrorism has a tremendous effect on society.¹¹

This current state of ambiguity, compounded with inflammatory remarks from pundits and political figures, is one that when fed to a
massive media campaign can create a volatile mix of public unrest. The need to communicate a national security threat, together with methods and mediums of communicating such threats, comprise a threat communication cycle. This communication cycle is only able to exist when an actual threat and the context in which it is framed are mindful of cultural nuance, terminology, and modern social environments.

Navigating the Landscape

Determining the nature and scope of a national security threat is a difficult challenge. The threat of terrorism to the United States is an issue that occupies more officials in government than ever before in history. National security threats in the twenty-first century take on many forms, including cyber, chemical, biological, and even environmental. The concept of modern threat, defined as acts of terrorism after 9/11 for the purpose of this examination, have been studied extensively by a wide range of experts. Robert Mandel, the chair and professor of International Affairs at Lewis & Clark College in Portland, Oregon, asserts that "[i]dentifying and prioritizing foreign threat have always been fundamental to national security, and this is particularly so in an anarchic world." The anarchic world that Mandel describes is part of the growth and evolution of foreign threats to U.S. national security. Many of the factors involved in defining and measuring threat seem almost fluid, such as government-wide consensus for defining "threat."

The post-9/11 challenge of the government today is narrowing the scope of threat perception, determining the source of the threat, assessing the threat, and having a firmer grasp on the varying understandings of accuracy.

Threat Perception

The nature and scope of a threat depends on who perceives the threat. For example, in the aftermath of the 9/11 attacks, the United States clearly views al Qaeda as posing a threat to the American people. Al Qaeda and its affiliates would argue that their attack was a response to attacks by the West upon Muslim peoples and their lands and, therefore, actions such as suicide bombings and other guerilla-style attacks are justified. U.S. national security and defense infrastructure, like the majority of other industrialized coun-
tries after World War II, was established with the assumption of a clearly defined enemy. In the 2006 book titled *The Starfish and the Spider* by Ori Brafman and Rod Beckstrom, the unstoppable power of leaderless organizations is explained. Brafman and Beckstrom describe the structure and functional nature al Qaeda from its early inception: While al Qaeda as a terrorist organization was expanding and successfully committing acts of terrorism around the world in the 1990s, it remained a largely decentralized organization with a limited command and control structure. Due largely to the antiquated national security intelligence infrastructure in the United States, meticulously detailed in the 9/11 Commission Report, the ability to “perceive threat” from a foreign terrorist organization that seemed more aspirational than operational was a task for which the United States was mostly unprepared.

The scope and nature of nation security threats to the United States has continued to change and evolve into new forms throughout the decades. As threats evolve, so do the ways the United States constructs and depicts the threat image. These images, in a sense, “define the enemy” for the American public. The construction and depiction of the image of “threat” is closely linked. In an article published in 2004 titled “Conglomeration, New Media, and the Cultural Production of the ‘War on Terror,’” James Castonguay takes a unique assessment of post-9/11 imagery associated with America’s “war on terror.” According to Castonguay, Jack Valenti, the head of the Motion Picture Association of America, reminded participants at a meeting with government officials of his industry’s goal by saying: “We are not limited to domestic measures. The American entertainment industry has a unique capacity to reach audiences worldwide with important messages.” Valenti’s statement underscores the vast nature of the creation of imagery in the United States related to the war on terrorism. Not only were government officials creating their own narratives and images of the enemy to help define our national security goals but also Hollywood was enlisted to help deliver that message to not just the American public, but the whole world.

The images of the greatest threats to U.S. national security have always been closely related to the images of our designated enemies. The concept of enemy and threat are nearly inextricable. The image of the “Wanted” poster often comes to mind when one thinks of those who pose a threat. In fact, the history of the Wanted poster is also linked to the establishment of military intelligence over ninety
years ago. In 1919, the FBI first used the Wanted poster to announce a wanted fugitive to as many people as possible. Other than the picture of a wanted felon or fugitive, it seems difficult to project threat in a single still image. During the Cold War era, the image of the red Soviet Union flag depicting a hammer and sickle was a nearly universally understood symbol of Communism. However, the actual threats of the Cold War era from the Soviet Union were more likely nuclear proliferation, espionage, and an overall arms race, not threats to the U.S. political system. Even simple images can carry with them meaning and inference far beyond any symbol or depiction.

Another infamous symbol associated with threat, war, and terror is, of course, the swastika. Its origins possibly date back to ancient India, but it is most commonly known as the official emblem of the Nazi Party. For most of the world, the symbol of the swastika represents the death and destruction that Nazi Germany wrecked throughout Europe. The actual shape of the swastika does not directly stand for Nazi ideology, but it is the common association because it was so closely connected to the horrific actions of Nazi Germany. The swastika was prominently displayed on all Nazi propaganda—much like a logo or brand. Its consistent and ubiquitous use throughout Nazi Germany solidified its connection to Nazi ideology. Similarly to the Soviet flag during the Cold War, the swastika carries with it meaning far beyond its simple shape. Both symbols were ultimately associated with grave threats and acts of terror and oppression.

Accurately capturing the images of threats to the U.S. homeland is indeed a difficult task, and a single such image may not even exist. As a society, we resoundingly return to the infamous Wanted poster. Our emotions point to the need to create an image in times of duress, whether through words or a picture, that resembles the enemy or threat—which thus constitutes our threat. The dimensions of the Wanted poster are loud and clear: that the picture on the poster is someone who should be considered a grave threat. Accurate illustration of threat goes beyond using vocabulary that represents good versus evil. Rather, it entails creating a depiction in the narrative sense of some type of potential, impending physical harm.

Part of depicting a threat involves a play on emotion. Words can indeed generate certain reactions when positioned in certain ways. The image of an enemy allows for the immediate and progressive construction of both offensive and defensive policies as well as operations. The image of an enemy can also greatly increase the rate by
which actions are taken. The high stress and high anxiety associated with incidents of post-9/11 terrorism are fuel to illicit responses that Mandel says are “less likely to take into account the complexity of their environment, more likely to consider fewer policy options, and more likely to choose policy alternatives impulsively.”24 These are emotional reactions, often not well thought out and rationalized, and play directly into the self-perpetuating cycle of threats and terror.

The images of the enemy during WWI, WWII, Vietnam, and the Cold War were varied. For WWI, the dominant images in the American public were those of trench warfare, U.S. soldiers in trenches, and large mechanical tanks on the battlefield. For WWII, the infamous photos of U.S. troops storming the beaches of Normandy were known universally at the time, along with the striking imagery from Nazi Germany marked so poignantly by the swastika. During the Vietnam War, the images that saturated the American public were those of troops shipping out as well as U.S. troops fighting the Vietcong in the jungles of Vietnam. Also, as mentioned earlier, the images of the Cold War were the dominant images of the former Soviet flag on all types of literature, posters, and billboards. This type of imagery, closely paired with the discourse on war and imminent threat, contributed to the depiction and more narrowly defined view of the threat of terrorism to the United States. Mandel asserts that “[d]uring the 1980’s America saw Japan as economic enemy and Soviet Union as political enemy.”25 The post-9/11 era has dwarfed all economic, political, and social encroachments on the “American way of life” and has elevated the threat from violent Islamist extremists to an unprecedented level. This elevation should not be considered inaccurate, or even debatable, but rather a nuanced development that requires careful study and consideration of long-term implications.

**Determining the Source of Threat**

It is difficult to define what is and is not an actual threat to the United States and our interests abroad. It may well be that the answer lies more in art than science; per Mandel, “[T]he great problem is not having a solid comprehension of the dynamics of modern threat.”26 And these dynamics begin with the perception of threat as discussed earlier. From there, the dynamics of modern threat include determining its source and making an accurate assessment on the
severity, and the measurement of this accuracy will help determine what actions, if any, the government or military should take. Further, how we determine "threat" is influenced by the types of threats that are unique to today's national security environment.

Even placing aside the question of who actually instigates a national security threat, there is the issue of where the true source of a threat lies. Mandel argues that our threat theory has been stagnant over the past thirty years and is embedded in the Cold War-era security context. Changes in threat comprehension and response are critical to both disrupting and responding to large-scale foreign attacks such as Pearl Harbor and 9/11. To take the example of the 9/11 attacks, Osama bin Laden and al Qaeda leadership were almost immediately determined to be responsible and soon after, they brazenly admitted their culpability. However, it is difficult to determine if it is the leadership of this nebulous organization or the foot soldiers who physically execute the attacks that pose a greater threat. It is important to acknowledge that rogue states, or "failed-states," as journalist and Newsweek editor Fareed Zakaria points out, provide a safe haven for terrorist organizations pose a serious threat.

At issue is a conceptual shift in the way threat is understood, communicated, and thus acted on. Leaderless and decentralized organizations are part of the challenge to making this conceptual shift. Additional contributing factors are the complexities associated with "failed-states." This set of factors, leaderless and decentralized terrorist organizations, coupled with a growing list of "failed-states" across the globe, are major contributing factors to the way the United States understands, communicates, and responds to nation security threats. Until this conceptual shift in both government and civil society reaches a more serious level of comprehension and maturity, the Cold War-era mentality will continue to play a more dominant role than it should.

Post-Cold War Paradigm

The failed states threat scenario, on the other hand, presents a completely different landscape and operating picture. Fast forward to the post-9/11 era, and a threat environment consisting of designated terrorist groups operating in largely lawless parts of the world seemed to dominate the U.S. worldview. A now-famous headline
featured on the cover of *Newsweek* in October of 2001, only a few weeks after the 9/11 attacks, asked, "Why do they hate us?" In the article, Fareed Zakaria analyzed the political, economic, and cultural landscape of the Middle East and Southeast Asia from the perspective of a national security threat. His conclusion was that complicating factors in the areas of governance, religion, and the cultural concept of idealism were all far lacking the developments the rest of the world had endured in the previous decades. These multiple layers of political, economic, and cultural factors are difficult enough to grasp for a single country or region, but in the new post-9/11 threat environment they are now part of an evolving global environment. This new environment challenges not only the way the United States perceives national security threats but also how we respond.

Post–Cold War threat sources assume several fundamental differences from threat sources during the Cold War. The primary Cold War threat focus remained political-ideological for over nearly three decades. In contrast, post–Cold War threat sources chose tactic and attacked based on more cultural-religious divides. In the post–Cold War era, according to Mandel, "Emerging threats have been typically covert, dispersed, decentralized, adaptable, and fluid, with threat sources relatively difficult to identify, monitor, and target, contain, and destroy, and with these sources' past actions it is not necessarily a sound guide to their future behavior." Examples of state and nonstate actors that exemplify this characterization are the modern-day countries of Somalia and Yemen and nonstate actors such as al Qaeda and Hezbollah. The post–Cold War era presents a menu of complexities that are neither formal nor clearly defined. This fundamental shift is most shockingly apparent in the attacks of 9/11 and in the progression of terrorism-related incidents since. This post–Cold War shift in the nature and origin of threat was indeed not an abrupt one but rather a gradual shift fueled by population shifts, growing international conflict, and, most notably, the escalation of violent Islamist extremism. Mandel claims that "at the level of threat recognition, the end of the Cold War also meant a shift in intelligence’s stock and trade from puzzles or questions that could be answered definitively given the necessary information to mysteries or questions that cannot be answered with certainty no matter what information is received." Mandel’s statement underscores the fact that improving the sources
and methods of national security intelligence practice alone are not absolute safeguards. Rather, a more complete reform from Cold War–style operations are needed.

A side-by-side comparison of Cold War threat versus post–Cold War threat highlights the vast magnitude by which potential threats in the United States have multiplied and evolved. For example, when assessing threat during the Cold War, the primary rival superpower was the Soviet Union. However, in today’s post–Cold War era no one rival superpower remains. There is, instead, an array of rogue states, transnational terrorists, criminals, and so on. Transnational terrorists and rogue states have consumed much of the government’s discourse related to national security in the years following 9/11. The effect of transnational terrorism has come to a full state of maturity for Western governments, and the ambiguity of real or perceived threat is now a matter of exploiting every lead to the point of exhaustion. The differences among one superpower and many rogue actors present a cultural and ideological shift in the way U.S. defense policy and national security strategy had been developed and implemented.

Threat Assessment

The post–Cold War era, combined with post-9/11 security environment, has irrevocably changed our threat analysis and response, and this has happened in a number of ways. The post-9/11 intelligence environment has been mockingly scrutinized in recent years for the overemphasis to “connect the dots.” The most recent example is the attempted bombing of a Northwest airline flight by a Nigerian national who had an explosive device sewn into his underwear on December 25, 2009. A Newsweek article described the incident as “[p]ossibly the worst terrorist strike against the U.S. since 9/11 was averted only by luck and the bravery of other passengers and the airplane’s crew.” This was a frightening thought to many members of Congress and senior administration officials. After the failed attempt, the specific failure of “dots” to connect or pieces in intelligence reporting to be properly analyzed was made apparent. Approximately one month before the incident, the alleged perpetrator’s father, a wealthy banker, visited the U.S. Embassy in Nigeria to express concern that his son had fallen into the company of Yemeni-based extremists. News reporting also indicated that the National Security Agency had intercepted intelligence that al Qaeda in Yemen
was planning an attack against the United States using a Nigerian national. In addition to these two key facts, the alleged perpetrator was also denied a visa to the United Kingdom but maintained a multiple-entry visa to the United States. This case resulted in a thwarted plot, but from the perspective of successfully "connecting the dots," it was a complete failure.

Just prior to the Northwest airline incident, a mass shooting took place on a military base in Fort Hood, Texas. The sole shooter was U.S. Army major and psychiatrist Nidal Hasan. After the shooting, an investigation by the Senate Homeland Security and Government Affairs Committee concluded that "the Army and FBI [missed] warning signs and [failed] to exchange information that could have prevented the massacre." In this example "dots" were not connected. In fact, information between the FBI and the army should have been shared but was not for largely bureaucratic reasons, the Committee found. These two examples of the Fort Hood shooting and thwarted bombing of a U.S. airliner are telling of the fragility of national security intelligence. Even the most minor and seemingly obscure piece of information can have a global impact.

The complexities of modern terrorism are many, but a key issue related to the post-Cold War era is knowing how to classify or label modern threats. Authors Mona Harb and Reinoud Leenders conclude that "caricaturing one's opponent in terms that justify or call for its elimination is as old and common as political conflict itself, yet few notions have provoked as much disagreement as that of 'terrorism.' Modern terrorism is indeed a unique phenomenon, but as Harb and Leenders point out, some fundamental issues such as caricaturing of opponents or threats to security still abound. Labeling a person, organization, or group as a "terrorist" carries with it certain legal, diplomatic, and military ramifications. The Department of State and the Department of Treasury have extensive criteria behind the factors for such a designation, as well as the consequences to such a designation. These criteria are a legal designation and apply to the entire U.S. government.

Specifically related to post-9/11 examination, Harb and Leenders say that "by the rediscovery of the notion in the post-9/11 'war on terrorism,' discursive battles have been fought as intensely as military ones, with all contestants and their sympathizers rejecting and placing their mutual characterizations at the core of their disputes." The "discursive battles" they describe are essentially the
debates marked by analytical reasoning that come with labeling, or classification decisions such as this. With nonstate actors and groups designated as terrorist organizations, such as al Qaeda and Hezbollah, we begin to understand to designate certain groups, but this need does not fully address the subjective nature of our understanding of such a designation.

Overall, global security threats are today "more varied in nature, more numerous in terms of the countries able to project them, above all more capable of being delivered from one side of the globe to another, than at any time in history." Since the conventional wisdom has been turned upside down about the nature and source of threats, we continue to struggle to deal with the looming threat of violent Islamist extremism. The new American foe is often network based, transnational, highly flexible, and able to adapt to vastly different social, political, and economic environments. The challenge that is made clear in this new environment is that the American national security enterprise must remain equally nimble and adaptive.

The national security enterprise has undergone massive reorganization since the attacks on 9/11, and along with the reorganization has come a steep increase in the private sector firms and professionals who support this enterprise. This massive government reorganization, the largest since the creation of the Department of Defense in 1947, has come about for better or worse and seems to be here to stay. The national security enterprise has also seen new management and focus by the Obama administration, but the past strategies of the Cold War seem to still permeate our post-9/11 national security strategy.

**The Role of Accuracy**

The concept of accuracy may seem intuitive in matters of national security intelligence, but like other professions, its practitioners are just as susceptible to error. In a study conducted by the Center for the Study of Intelligence, experimental psychologists examined the relationship among the amount of information available to the intelligence analysts, the accuracy of judgments they make based on this information, and the experts' confidence in the accuracy of these judgments. Key findings from this research are as follows: Once an experienced analyst has the minimum information necessary to make an informed judgment, obtaining additional information generally does not improve the accuracy of his or her estimates.
Additional information does, however, lead the analyst to become more confident in the judgment, to the point of overconfidence. Additionally, experienced analysts have an imperfect understanding of what information they actually use in making judgments. They are unaware of the extent to which their judgments are determined by a few dominant factors, rather than by the systematic integration of all available information. Analysts actually use much less of the available information than they think they do.\(^{55}\)

On the issue of accuracy in intelligence estimates, Glenn Hastedt notes, "In many ways accuracy is a flawed standard for judging intelligence estimates."\(^{56}\) Hastedt argues that the use of accuracy raises the question of how accurate one must be and what is an acceptable level of accuracy. Hastedt points out that accuracy is suspect because of the after-the-fact nature of the evaluative process.\(^{57}\) This concept of accuracy further complicates how to assess national security threats.

The modern developments of terrorism and the perceived rise of post-9/11 violent Islamist extremism led the practitioners of national security intelligence, academics, and thought leaders who study these developments to mostly agree that new, sophisticated, and emerging frameworks are needed to advance the understanding of and response to post-9/11 threats. Commenting on the issue of intelligence failures, Dr. Tamas Meszerics and Dr. Levente Littvay, both professors at Central European University in Budapest, Hungary, note that "[i]n major historical cases, telling apart the otherwise conceptually distinct tasking from collection failure, or both from analytic failure and dissemination failure, has proven to be rather difficult."\(^{58}\) The vantage point from which the authors provide this quote is through the lens of major intelligence failures. Meszerics and Littvay accurately point out that the new millennium in the United States started with two major intelligence failures, the 9/11 attacks and the absence of weapons of mass destruction in Iraq.\(^{59}\)

The nature of threats to the United States has changed radically from the Cold War to the post-Cold War period. The days of predictability of the enemy and its capabilities and next moves are virtually gone. The new era of intelligence collection on cutting-edge mediums has barely arrived and is already evolving. The new post-9/11 security age is filled with new policies, procedures, and protocols, but yet it remains high in both vulnerability and expectation of total security.\(^{60}\) The threat has indeed changed, and Western intelligence
frameworks have changed, but imbedding threat awareness, analysis, and response into a permanent culture is a task that remains.

**Language Use in Context**

Understanding language is a matter of course within context. Former U.S. senator, president of San Francisco State University, and English professor at the University of Wisconsin, S. I. Hayakawa is well known for his work in linguistics and semantics. In 1949 he published *Language in Thought and Action*, which was the first of its kind to examine modern language and its uses. Hayakawa draws many relevant points to an examination of language post 9/11, but of particular note Hayakawa describes that words carry different meanings depending on a person’s perspective. “It would be startling indeed if the word ‘justice,’ for example, were to have the same meaning to each of the nine justices of the United States Supreme Court; then we should get nothing but unanimous decisions.”61 If we accept this principle of meaning variation within context, we also accept the principle that context matters. The context of modern terrorism and its resultant public perception are nothing short of being in a complete state of evolution (and, at many times, confusion). Words—the way we use them and the way we understand them when spoken by others—shape our beliefs, prejudices, ideals, and aspirations.62 Words constitute the moral and intellectual atmosphere in which we live and which coexists within the national security intelligence architecture. This type of coexistence, according to Hayakawa, is a semantic environment.63

After the attacks of 9/11, there began to be an emergence of a new vocabulary with a unique tone and tenor that meshed a historical political-military lexicon with descriptions of the presumed culprits behind the attacks. Because the crimes of 9/11 were perpetrated only a decade ago, the time for serious research and analysis is just beginning. This, however, is not to be confused with the work of criminal and intelligence investigations, which have been nearly continuous since September 12, 2001. The work of intelligence involves making value judgments in writing at every stage of both the intelligence and policy cycles. While the language and lexicon of these value judgments continues to evolve, we must continue to take into serious consideration that multiple readers of intelligence products can take away meanings that were never intended.64 We need to escape the narrow debate of what specific words are correct to describe modern
terrorism and instead ensure that threats are articulated in a manner that captures the events and puts them into the proper context.

According to Hayakawa, an interesting dynamic exists whereby there is not necessarily a connection between a symbol created by language and that which is symbolized. Thus, if language can construct a symbol, this may be independent of that which is represented. Whereas, in Modernist/Platonic thinking, a word or image directly relates to its referent, and accordingly, we know through our reason what the referent is. Thus, many people who are fully involved in the national security intelligence, including intelligence professionals, in various ways may be completely unaware of the impact of the symbolic representations of the language chosen in documents throughout the intelligence cycle. The intelligence cycle is comprised of various stages of evaluation and refinement with strong reinforcement from modern society. The most skilled practitioner or analyst may unwittingly draw on language supportive of ideologies that may be far from accurate. Society is shaped by semantic influences, and the national security environment is as well.

The field of national security intelligence is coded with a complex vocabulary all its own. This field uses a unique array of acronyms and technical terms, which are often used publicly in news, media, and general information sources as well as in controlled or classified government sources. However, since the meanings of words are subjective, it is easy for the general public to misunderstand the government's use of such terms. This is because our society is rooted in Platonic principles. There is a general belief in objectivism, and this belief hinders us from really understanding that language and meaning are subjective. The ultimate challenge is what we as a society assume to be the case (objective language) really does not exist and is actually the opposite (subjective language).

The Case for Ethics

How does this relate to modern terrorism? Or to the national security intelligence field that is supposed to protect us from modern terrorism? The dynamics of modern terrorism and national security intelligence are both of the subjective nature. The reason for a discussion of ethical subjectivism is to underscore that these issues include moral matters. They are not purely action and reaction but include a series of moral judgments made both by the perpetuators of terrorist acts as well as those charged with defending against
them. In the words of philosopher David Hume, morality is a mat­
ter of sentiment rather than fact. To apply this analysis, the au­
thenor of the Elements of Moral Philosophy, James Rachels, provides 
two practical stages.

The first is simple subjectivism. “When a person says that some­
thing is morally good or bad, this means that he or she approves of 
that thing, or disapproves of it, and nothing more.” This theory is 
simple and uncomplicated and provides a basic template to analyze 
many of the statements and expressions around modern terrorism 
and the field of national security intelligence. The problem with this 
theory is that we sometimes make incorrect or inaccurate statements, 
so how does simple subjectivism deal with this? The problem is that 
it doesn’t. You can disagree with a person’s feelings or statements, 
but you can’t take them away from people. Thus, simple subjectiv­
ism might be a great fit for many applications, but not our current 
examination of the language of modern terrorism and national se­
curity intelligence.

The second stage is emotivism. According to Mary Gore Forrester, 
author of Moral Language, “the oldest of the nondescriptivist theo­
ries of the meaning of evaluative terms is emotivism.” Developed 
primarily by American philosopher Charles L. Stevenson (1908– 
1979), emotivism was one of the most influential theories of ethics 
in the twentieth century. Similarly to the growth and expansion of 
the emotivist theory, the national security intelligence enterprise has 
ballooned since the attacks on 9/11. The purpose of stating both 
the influence of a theory of ethics and a social and policy dynamic is 
to demonstrate that we are making a statement that is either true or 
false depending on the perspective of the listener. The purpose of the 
utterance, typically, is only to convey information to the listener.

Realities of threat and the communication of such realities by 
both government officials and perceived persons of authority meet 
at the critical convergence where threat is framed and defined and 
policy making and operations plans begin to take shape. According 
to Hoskins and O’Loughlin, “[T]he issue at hand, then, is to under­
stand how it is that different perceptions of reality emerge, for only 
then can we see why different perceptions of security, threat, and 
terror exist.” The subjective nature of threat after 9/11 is not iso­
lated but rather part of a broader global trend of violent extremism 
of both the religious and nonreligious nature. From the philosophi­
cal point of view this global trend has no true absolute value, but 
instead it is purely subjective and part of the larger philosophical
view of subjectivism. When national security threats have been described through a media outlet or through government officials, the evaluations made are not merely evaluations of approval or disapproval, but the underlying sense is an expression of attitude, thus underscoring the emotivist application. This subjective nature of both post-9/11 national security threats and the way in which they are defined, described, and discussed are seemingly expressions of attitude—emotivism. However, again, our society is fairly grounded in Modernist/Platonic thought. So, these images may be subjective, but people still believe that they can point to a “truth” that we can all know. And therein lies the problem.

**Conclusion**

Communications, in the national security and intelligence context, is far too subjective to draw a narrow application of ethical standards.

The 9/11 attacks have become the de facto framework for nearly an entire body of national security intelligence analysis and threat warning. The intelligence failures and subsequent lessons learned have now become the metric against which every granular piece of intelligence is held for exhausting comparison and probability appraised for similarity or intent of even the most remote reflection to the 9/11 attacks, al Qaeda, or a similar permutation. The 9/11 attacks shined a spotlight on gaping holes and deficiencies in the intelligence community. The subsequent policy decisions to correct these holes and deficiencies established two key deliberation points to all future intelligence analysis. The first point: analyzing each new intelligence collection with the consideration that the information, no matter how seemingly irrelevant, could be part of a larger threat enterprise and is treated with a new sense of interconnectivity to a larger and more ominous threat environment. Second, the renewed concentration on new and emerging national security intelligence and the almost draconian view that every piece of new and emerging intelligence is somehow related to al Qaeda and another potential 9/11 caliber attack.

Throughout the intelligence process selective decisions are routinely, and mandatorily, made about the scope and severity of various threats. There does exist a structured preference to align new or emerging threats into the preestablished frameworks of al Qaeda. This should not be labeled as negative bias or somehow disparate application of analysis, but rather the harsh reality of the relative
immaturity and lack of sheer historical perspective from which to
gauge.

In the narrow context applied in this article, a failure to ethically
communicate threat mirrors the case criteria of analytic intelligence
failures where the major problem is one of comprehension, estima­
tion, evaluation, and prediction. Failure is ascribed to one of these
distinct areas because broad attribution of missing or invalid infor­
mation would be overly simplistic and leave no critical lesson from
which to improve. The need to flush out subsets and conceptual
elements of national security intelligence cycle intake and production
phases can help expose the suspected underlying problems of our
established intellectual capacity of threat related to violent Islamist
extremism post 9/11.

George Selim has spent the past ten years working on issues related to civil
liberties and national security. He holds a graduate degree from Georgetown
University and serves as a guest lecturer on a number of national security, civic
engagement, and community policing initiatives. He currently serves as a senior
policy advisor at the U.S Department of Homeland Security and previously
worked at the U.S Department of Justice.

The views in this article are the author's own and do not necessarily reflect
those of the U.S. Department of Homeland Security or the U.S. government.

Notes

1. Sandra Silberstein, War of Words: Language, Politics and 9/11 (Lon­
Strategic and International Studies, Homeland Security and Counterterror­
3. Nelson and Bodurian, “A Growing Terrorist Threat?”; see also, for
example, this article stating American public opinion has grown weary
of the war in Afghanistan: John Ellis, “The Beginning of the End of U.S.
www.businessinsider.com/the-beginning-of-the-end-of-us-involvement-in­
4. Kenneth Church, “Jihad,” in John Collins and Ross Glover, Collateral
University Press, 2002), ch. 8.
5. Collins and Glover, Collateral Language, 5.
6. Ibid.
7. Ibid.
9. Ibid.
10. Ibid.
13. I am referring to experts such as Robert Mandel, Marc Sageman, Bruce Hoffman, and many others.
15. In an opinion post on Salon.com, political blogger Glenn Greenwald presents a comprehensive look at how the *New York Times*'s coverage of the massacre linked Muslim terrorists to the attacks. He also discusses a column published by *Washington Post*'s Jennifer Rubin based on the same conclusion. Greenwald suggests that the papers' use of the word *terrorism* reveals its meaninglessness in media today. The comment section below his article contains enough material for multiple theses, with many people suggesting that a narrow definition of "terrorism" is as risky as it is bigoted. Available at http://www.salon.com/2011/07/23/nyc17/singleton/ (accessed 31 July 2011).
23. Ibid.
25. Ibid.
26. Ibid., 2.
27. Ibid., 4.
28. Ibid.
32. Ibid.
34. Ibid.
35. Ibid., 11.
36. See, for example, Wright, Sageman, and Zakaria, who have all written extensively on the growth of and evolution of violent Islamist extremism.
39. Ibid., figure 2.1, 12.
40. Silberstein, *War of Words* (selection of speeches throughout the book, including from President Bush and other senior administration officials).
43. Ibid.
45. Ibid.


1. It must be a foreign organization.
2. The organization must engage in terrorist activity, as defined in section 212 (a)(3)(B) of the INA (8 U.S.C. § 1182(a)(3)(B)), or terrorism, as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C. § 2656f(d)(2)), or retain the capability and intent to engage in terrorist activity or terrorism.
3. The organization’s terrorist activity or terrorism must threaten the security of U.S. nationals or the national security (national defense, foreign relations, or the economic interests) of the United States.


50. Robert Harvey, Global Disorder: America and the Threat of World Conflict (New York: Carroll & Graf Publishers, 2003), xiii (as quoted in Mandel, Global Threat, 14).

51. Mandel, Global Threat, 15.


55. Ibid.


57. Ibid., 105–6.


69. Ibid.


72. Priest, "Top Secret America."


77. Ibid.