ASSESSING PERCEIVED CREDIBILITY OF WEB SITES IN A TERRORISM

CONTEXT: THE PFLP, TAMIL TIGERS, HAMAS, AND HEZBOLLAH

Brandon Todd Spinks, M.A.

Dissertation Prepared for the Degree of

DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

May 2009

APPROVED:

Emile Sahliyeh, Major Professor
Linda Schamber, Committee Member
David McEntire, Committee Member
Herman L. Totten, Dean of the College of
    Information
Michael Monticino, Interim Dean of the
    Robert B. Toulouse School of
    Graduate Studies

Spinks, Brandon Todd. *Assessing Perceived Credibility of Web Sites in a Terrorism Context: The PFLP, Tamil Tigers, Hamas, and Hezbollah.* Doctor of Philosophy (Information Science), May 2009, 137 pp., 24 tables, 5 figures, references, 119 titles.

The purpose of the study was to contribute to the overall understanding of terrorist organizations' use of the Internet and to increase researchers' knowledge of Web site effectiveness. The methodological approach was evaluation of the perceived credibility of Web sites based on existing criteria derived from information users. The Web sites of four terrorist organizations were assessed: two secular nationalist groups, the People's Front for the Liberation of Palestine (PFLP) and Liberation Tigers of Tamil Elam (LTTE or Tamil Tigers); and two religious nationalist groups, Hamas and Hezbollah.

The findings of this analysis showed differences in perceived credibility factors among terrorist organizations' Web sites and positive levels of perceived credibility for the Web sites. These findings indicate the potential for positive impressions of the organizations' Web sites by information users, which would help empower the organizations with the capacity to reach their objectives. By using Web sites, these groups can effectively increase their support base through disseminating information, improving recruiting, and attracting monetary contributions, and can establish themselves as legitimate components of society.

TABLE OF CONTENTS

Chapters

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Terrorists increasingly employ the use of the Internet to reach many of their objectives. They have become technologically sophisticated at developing Web sites to garner support, disseminate information, and communicate to members. But, how effective are these Web sites? And, what does terrorists' effectiveness at using Web sites signify for those who study terrorism or attempt to thwart terrorist activity? This study moves toward answering these questions.

Numerous scholars, policy-makers, and counterterrorism experts have investigated thousands of Web sites and Web pages linked to terrorist organizations all over the world to improve understanding of possible effects of terrorist organizations' use of Web sites. However, such investigations have generally focused on why these organizations have shifted toward a more technologically based approach to information dissemination. And regrettably, these studies have primarily looked at the benefits to a terrorist organization using the Internet from the perspective of the terrorist organization, not the information user.

Because it can be assumed that credibility is important to terrorist organizations, this study looked at perceived credibility of Web sites. It did from the information user's perspective. Furthermore, it investigated terrorist organizations' use of Web sites for information dissemination.

This approach contributes to the overall understanding of terrorist organizations' use of the Internet, increasing the knowledge of Web site effectiveness. At the same time, the methodological approach employed here enables researchers to perform

investigations of perceived credibility of terrorist organizations' Web sites without interacting with members of a group.

Problem Statement

Terrorists have become evermore dangerous and difficult to stop, not because of their numbers or the types of activities they conduct, but because of their profound ability to remain fluid and impermanent (Hoffman, 2005). In fact, in his testimony to the U.S. Congress concerning the al Qaeda movement, Hoffman (2005) said that when faced with the might of the U.S. military, al Qaeda simply adapted by fleeing to neighboring Pakistan and going underground. However, its presence continued to be felt around the world as it presented video and audio messages calling for a mobilization of Muslims to rise up as one, to expand and increase violence toward the "enemies of Islam" (Hoffman, 2005). Indeed, to some (Hoffman, 2005), the al Qaeda movement has actually grown. How did this organization overcome the challenges resulting from the West's Global War on Terrorism? It increased its use of the Internet (Hoffman, 2005).

There are problematic issues related to understanding this phenomenon. This study identified and addressed several. First, terrorist organizations continuously seek tools to securely, effectively, and efficiently communicate a message (Hoffman, 2005, 2006; Schmid & de Graf, 1982). Whether the objective is to provide members with confidential information, incite actions of others against a common adversary, or strengthen constituent support, terrorists are challenged with how to get information to information seekers without jeopardizing their own security.

2

Second, those who study terrorism are faced with many obstacles to advance understanding of terrorist strategies, actions, or intentions. Due to the extreme secrecy of most terrorist organizations, as well as the relative risk associated with personally investigating these groups, scholars are limited in their analytical methods.

Third, throughout the information science literature, a vast amount of research attends to the World Wide Web as a tool for information dissemination and as a resource for information seekers. The design and sustainment of a Web site that is valued highly enough by consumers to attract their interest is also a point of concentration in contemporary research. However, the literature focuses on how Web sites are employed in an electronic commerce (e-commerce) context. It does not address the use of Web sites by organizations to reach varying objectives such as selling an ideology, as do terrorist organizations, to build internal and external support for a movement. Additionally, given the large amount of attention on computing sources of information, the literature that covers general Web site credibility is relatively small and underdeveloped (Fogg & Tseng, 1999; Fogg et al., 2001). Consequently, the information science literature can benefit from a better understanding of the potential effectiveness of Web sites of terrorist and other organizations that promote ideologies.

Finally, the body of literature on terrorism similarly suffers from its general approach to Web site-oriented research. That is, it largely looks at the increased use of the Internet by terrorists, but generally concentrates on the theoretical and practical assumptions as to why the Internet is chosen as a more efficient method of information distribution. It does not look at perceived Web site credibility, and thus it fails to move toward determining possible Web site effectiveness.

Purpose

This study had multiple intentions. First, it aimed to contribute to the information science and terrorism literature to improve the understanding of terrorist organizations' use of Web sites. Second, the study was conducted in order to advance information science and terrorism-related research toward establishing the means to accurately assess the effectiveness of terrorist organizations' Web sites. To this end, modifications were made to a model commonly used to measure perceived credibility of e-commerce Web sites. The modified version adequately assesses terrorist organizations' Web sites. This model is also applicable for future studies of Web site credibility where selling an ideology is paramount. Finally, this study sought to provide researchers a mechanism to assess perceived credibility of terrorist organizations' Web sites without placing the researcher at personal risk.

Accordingly, this study analyzed several established terrorist groups' Web sites and gauged their level of perceived credibility of the information user according to commonly accepted indicators. The main research question for this investigation was:

To what extent are there perceived credibility differences between terrorist organizations' Web sites?

More specifically the study asked:

1. What are the perceived credibility differences between the Web sites of each religious nationalist terrorist organization?

2. What are the perceived credibility differences between the Web sites of each secular nationalist terrorist organization?

3. What are the perceived credibility differences between the Web sites of the religious nationalist groups and the secular nationalist groups?

The questions above present those who study the credibility of Web sites, as well as students of terrorism, a unique venue for novel research. By answering these

4

questions, this study, and future research, can contribute significantly to the understanding of such phenomena.

Significance

With such considerable growth in the use of the Internet by terrorist organizations, increased attention must be given to how effective Web sites are at contributing to a group's success, and thus, its survival. This investigation advances scholarship toward this end, offering an feasible method for scholars and anti-terrorist organizations to assess Web site effectiveness.

By studying terrorist organizations' Web sites, researchers can enhance understanding of what possible objectives an organization may have for the Web site, what type of information is disseminated, or who are the specific target populations for the information. Due to the advancements in Web design capabilities by terrorist organizations, understanding can also be improved regarding who integrates additional means to disseminate information and/or receive support.

Terrorist organizations and movements are increasingly attractive to the disenfranchised, disillusioned or discontented (Benard, 2005). At the same time, there is an upsurge in Web site use to foster support as well as spread terror. By examining perceived credibility of terrorist organizations' Web sites, researchers can augment the understanding of potential Web site effectiveness. In other words, by assessing perceived credibility from the perspective of the constituent, the member, the adversary, or the supporter, investigators can increase understanding of how effective a particular Web site might be with a specific population.

Methodology

Numerous studies address Web site credibility in the literature. They discuss methodological approaches, offer theoretical arguments, or expound on Web site effectiveness. Generally, it is assumed that certain factors affect the level of credibility an individual applies to a Web site and that effectiveness is directly correlated with credibility. Moreover, research is commonly conducted through multiple interviews or surveys from a sample of the population. Such methodological approaches were not applicable for this investigation due to the potential risk to researchers. Consequently, this study employed an adapted model to assess perceived credibility from a Web site user's perspective .

To answer the research questions, the model evaluated potential differences in perceived credibility between different types of terrorist organization's Web sites. The four organizations assessed were categorized into two groups: secular nationalist and religious nationalist. The groups included the People's Front for the Liberation of Palestine (PFLP) and the Liberation Tigers of Tamil Elam (LTTE or Tamil Tigers) for the secular nationalist category, and Hamas and Hezbollah for the religious nationalist category.

The study collected ten individual records for each Web site. Records were created by downloading and capturing the first two levels of the Web site using Adobe Acrobat Professional and MHTML format respectively. Individual records were then assessed with the model to measure factors affecting perceived credibility. To overcome significant risk to the validity and reliability of this study, an intercoder reliability test was conducted. A more in-depth discussion on the methodological

approach used for this study is in Chapter 3.

Scope and Limitations

The scope of this project is limited to the assessment of perceived credibility of four terrorist organizations' Web sites. As a consequence, the generalizability of the findings may be restricted. However, the purpose of this analysis was to advance the study of credibility and the effectiveness of terrorist organizations' Web sites through an interdisciplinary approach and by establishing a model that researchers can utilize in the future.

There were a few limitations identified in the course of the study such as language challenges and variable application. As such, some information presented on Web pages was either not evaluated due to language barriers or not assessed as fully as this study intended. The consequences and proposed solutions to each of these issues are discussed more in Chapters 3, 4, and 5.

Expected Outcomes

It is assumed here that credibility is important to terrorist organizations. Therefore, the Web sites investigated in this study are expected to show high levels of attention and effort by the organization to ensure they are attractive to the information seeker. In addition, it is expected that little difference will be found between the religious and secular nationalist organizations.

Important to note is that the Web sites investigated here are those of organizations that have operated for considerable time periods and are accordingly well positioned in their respective communities. Thus, the findings should be considered in

this context, as similarities might be present as a result. However, by investigating organizations both within a particular struggle and contrasting them with organizations that operate in two disparate environments, significant threats to validity are overcome. Finally, the findings will disconfirm the literary arguments that terrorist organizations appear to place importance on the application of credibility to their Web sites if significant quantities of incidents are found.

Summary

The research question posited here is to what extent are there perceived credibility differences between terrorist organizations Web sites? This investigation focuses on two problems. First, because terrorist organizations seek to utilize methods to reach their goals, it is uncertain as to a Web site's effectiveness. Second, researchers are confronted with numerous challenges when investigating terrorist organizations. This study offers an adapted model to adequately assess Web site effectiveness without placing the researcher at undue risk.

The study is presented in the following format. Chapter 2 provides a literature review related to perceived credibility and multiple factors affecting perceived credibility such as context, relevance, and novelty. It also reviews the literature on the importance of Web site credibility and information dissemination to terrorist organizations, as well as contemporary models that assess perceived credibility. Chapter 3 presents the methodological approach. Chapter 4 offers a discussion on data analysis and the findings. The final chapter provides recommendations for future research, policy implications, and concluding remarks.

CHAPTER 2

LITERATURE REVIEW

Introduction

Schmid and de Graf (1982, 9) stated that "Without communication there can be no terrorism." Similarly, Hoffman (2006) suggested that effective communication tools are pivotal in a terrorist movement's longevity. In other words, terrorist organizations must have an effective, credible means to disseminate their message in order to survive. Martha Crenshaw (1981, 379) maintained that "the study of terrorism can be organized around three questions: why terrorism occurs, how the process of terrorism works, and what its social and political effects are."

By studying the relevant aspects of terrorist organizations' Web sites on the Internet, these problems may be overcome. Moreover, by investigating terrorist organizations´ Web sites, researchers will increase understanding of what varying purposes terrorists use Web sites, what types of information terrorists disseminate, and how effective a Web site may be. Consequently, counterterrorism policy can be adjusted to focus more intensely on specific areas found to be effectively utilized by the terrorist organization. As a result, strategic targeting of these areas can undermine the ability of the terrorist organization to sustain support, inevitably threatening the survival of the organization.

This chapter provides a literature review on several relevant areas that contribute to the general understanding of terrorist organizations, their use of the Internet, perceived credibility and Web site effectiveness. First, it is necessary to establish a general understanding of what terrorism is as it provides important parameters for the

type of organization being investigated, the various activities it may undertake, strategies employed, and plausible intentions. Thus, the first section of this chapter presents several definitions for terrorism that are widely used throughout the literature.

Second, many scholars claim that terrorism is a means to communicate a message and that a primary aim of terrorists is to maximize the publicity of that message throughout the global community. Accordingly, the literature suggesting terrorism as communication is reviewed.

Third, terrorist organizations historically utilize media as a means to disseminate a message. Therefore, the literature related to the importance of the media to terrorist organizations is reviewed.

Fourth, terrorist organizations increasingly employ the Internet and develop Web sites as mechanisms for information dissemination. Consequently, the literature related to terrorist organizations and Web site credibility is reviewed.

Finally, a method is needed for researchers to accurately investigate terrorist Web sites to increase understanding of their effectiveness without placing the researcher in a potentially dangerous situation. Accordingly, the last section of this chapter discusses the literature related to various models that assess Web site credibility, as well as the model utilized for this project.

What is Terrorism?

Multiple definitions exist in the literature attempting to classify terrorism. The review here is by no means exhaustive, but intends only to provide a fundamental reference point for the many perspectives of terrorism. Schmid (1983, 110) analyzed

over one-hundred definitions and concluded that no "true or correct definition" exists. Understandably, how terrorism is ultimately defined is determined by the agent doing the defining. More specifically, a definition can be influenced by the underlying objectives of the individual or group committed to defining the term and presenting the definition. Additional cognitive factors may also affect how the term is defined.

The U.S. State Department and CIA use the same politically oriented definition. This definition is also used by many other agencies in the U.S. intelligence community. It suggests that terrorism is premeditated and politically motivated violence, intended to influence an audience (U.S. State Department, 2004).

The FBI's definition is oriented around the criminality of terrorism. It portrays terrorism as an illegal activity. It also entails two components of the phenomenon - domestic and international terrorism.

According to the FBI Policy and Guidelines (USDOJ 2000/2001, iii) domestic terrorism is

> activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States. International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; or affect the conduct of a government by mass destruction, assassination or kidnapping and occur primarily outside the territorial jurisdiction of the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.

The United Nations (2007, 1) employs Schmid and Jongman's (1988) definition

of terrorism. It states that terrorism is,

> an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), (imperiled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.

Terrorism definitions vary among scholars too. Crenshaw (1981, 379) claimed

that

> Terrorism occurs both in the context of violent resistance to the state as well as in the service of state interests. If we focus on terrorism directed against governments for purposes of political change, we are considering the premeditated use or threat of symbolic, low-level violence by conspiratorial organizations. Terrorist violence communicates a political message; its ends go beyond damaging an enemy's material resources.

Crenshaw (2005) also declared that "terrorism" is a type of political behavior.

Similarly, some (Russell et al., 1979; Sandler and Enders, 2003) have defined terrorism

as a premeditated, use of force that is threatened or actual, to achieve a political goal

through fear, coercion, or intimidation. Gurr (2005, 19) posits that terrorism "is a tactic,

sometimes a strategy, chosen by groups waging conflict." Others (Eubank and

Weinberg, 2001) reaffirmed the U.S. State Department's definition of terrorism claiming

that it is usually characterized as small-scale violence planned and carried out by small

groups or individuals in order to send a message to a specified audience.

Hoffman (2001, 420) claimed that "Terrorism is fundamentally the use (or

threatened use) of violence in order to achieve psychological effects in a particular

target audience." Pape (2005, 9) suggested that terrorism "involves the use of violence

by an organization other than a national government to intimidate or frighten a target audience. In general, terrorism has two broad purposes: to gain supporters and to coerce opponents." So why did he not allow for state sponsored terrorism in his definition? In his notes, Pape (2005, 298) stated that terrorism "still signifies, principally, violent acts against innocents that are committed by nongovernmental actors – such as revolutionaries, nationalists, or ethnic groups – and are intended to challenge the existing political order." He (Pape 2005, 298) added that

> Although one could broaden the definition of "terrorism" to include the actions of a national government intended to cause terror among an opposing population, use of such a broad definition would distract attention from what policy makers would most like to know: how to combat the threat posed by non-state actors to the national security of the United States and our allies. Further, it could also create analytic confusion. Terrorist organizations and state governments have different levels of resources, face different kinds of incentives, and are susceptible to different types of pressures. Accordingly, the determinants of their behavior are not likely to be the same, and thus the two require separate theoretical investigations.

As is evident, no comprehensively agreed upon definition of terrorism exists. Nevertheless, this study uses Schmid and Jongman's (1988) version because this definition shares many nuances with numerous others. In particular, it states that "the direct targets are not the main targets." Instead, the victims "serve as message generators." Furthermore, it claims terrorism is a "threat- and violence-based" process. In other words, terrorism is a process of communication where the victims are used as mechanisms or catalysts to disseminate a message. The following section will look at this characterization more closely.

Terrorism as Communication

The world has been compelled toward improving its understanding of terrorism.

Essentially, terrorism is a message conveyed to an audience. "Terrorists seek to further their political aims by publicly broadcasting their (often political) message" (Goodman et al., 2006, 197). Some scholars suggest that terrorism is a means of communication between the colonizer and the colonized, albeit as a last resort (Fanon, 1965; Dale, 1988; Eubank and Weinberg, 2001). Others (Crenshaw, 1981; Russell et al., 1979; Sandler and Enders, 2003; Gurr, 2005; Ross and Gurr, 1989; Pape, 2005; Rapoport, 1984) similarly state that terrorism is used symbolically and strategically to convey a message when all other means of communication seem to be ineffective. In fact, violence and counter violence might be the most accurate way of exchanging information between parties (Fanon, 1965).

Indeed, during the 1500s terrorists in eastern Asia took on a violent approach to communicate their demands for liberation from colonial influence. Dale (1988, 47) asserted that even suicidal attacks that occurred in the early sixteenth century represented "protests against western hegemony or colonial rule by Muslims who felt they had no other means of fighting against superior European or American power."

Thus, terrorism is characterized by some as a means to communicate and by others as a message. I suggest that terrorism is not, nor can it be defined as a message itself. A terrorist action is simply an agent, transmitting a message from one group to another. In other words, terrorism and terrorist acts are nothing more than catalysts, used to convey a message in order to bring about change. However, what mechanisms do terrorists use to get their message across to targeted populations? Historically, the primary means has been media.

Terrorist Organizations and the Media

Terrorists depend on the media to get their message to the masses (Hoffman, 2006; Schmid & de Graf, 1982). In his testimony to the U.S. Congress, Hoffman (2005) discussed the importance of the Internet to groups such as al Qaeda. He suggested that the future success of counterterrorism efforts depends upon the recognition of the significance of the Internet to terrorist organizations (Hoffman, 2005). Hoffman (2005, 18) additionally summarized the current situation stating that

> In particular, special efforts must be devoted to effectively countering the messages of hate and intolerance and the calls for violence and bloodshed that now permeate the Internet. The coarsest most base conspiracy theories are regularly peddled with frequency that has endowed them with a veracity through repetition and ubiquity that is divorced from reality. Accordingly, this 'war of words' needs to be fought most critically on and through the Internet – an arena where American efforts have been particularly anemic while those of our enemies have been active, voluminous and indeed effective. Before 9/11, for example, al Qaeda had only one Web site: www.alneda.com. Today, the movement is present on more that 50 different sites (Weimann, 2006). 'The more Web sites, the better it is for us,' a jihadist statement posted on azzam.com in 2002 (Kelley 2002, 27) proclaimed. 'We must make the Internet our tool." For al Qaeda, the Internet therefore has become something of a virtual sanctuary: providing an effective, expeditious and anonymous means through which the movement can continue to communicate with its fighters, followers, sympathizers and supporters worldwide.

Terrorist organizations share this dependency because they want and need to maximize the amount of publicity they receive from an event or activity. The greater the publicity a group receives following a terrorist act, the greater amount of people who will receive their message. Goodman et al. (2007, 198) insisted that "the reaction of the media further publicizes terrorist intentions to the international arena, thus satisfying and potentially fuelling the terrorists appetite for more attention."

Hoffman (2006, 174) similarly stated that

Indeed, without the media's coverage the act's impact is arguably wasted, remaining narrowly confined to the immediate victim(s) of the attack rather than reaching the wider "target audience" at whom the terrorists' violence is actually aimed. Only by spreading the terror and outrage to a much larger audience can the terrorists gain the maximum potential leverage that they need to effect fundamental political change.

Jenkins (1975, 16) as well suggested that "Terrorism is theatre; terrorist attacks are often carefully choreographed to attract the attention of the electronic media and the international press." Meyer (1991, 2) determined that

Propaganda grants authority to its makers. In the first place, simply by demonstrating its ability to disseminate information that the government has banned, a guerilla group proves that it is a viable force. Second, once a group has the people's ears it can manipulate their minds, causing them to act as they might not otherwise; or if it does not work as effectively as this, its messages at least command the attention of those who read, hear or see them. In words and pictures, those whose plans are hidden from public view can portray themselves any way they please. Furthermore, if appearing to play a particular role can win support, propaganda will help these guerillas to become in fact the powerful forces that they claim to be.

Through the propagation of information, a terrorist organization seeks to accomplish a variety of goals (Goodman et al., 2007). The exact objectives, however, depend upon the group, the act, the message, the target audience, or any number of other factors within a specific context. They may be to inform, instruct, garner financial, material, or spiritual support, mobilize the masses, gain sympathy, recruit, threaten, intimidate, coerce, unify, legitimize, or influence policy (Denning, 2002; Denning, 2000; Gunaratna, 2007; Weinberg, 2007; Goodman et al., 2007; Hoffman, 2006).

New communication tools such as the Internet have permitted Islamists to go further and become increasingly effective at disseminating their message than ever before (Goodman et al., 2007). In fact, "The mass media and the Internet seem to play a role in sparking terrorism in locales where we might not expect it to occur" (Weinberg

2007, 39). The Internet also provides a means for a terrorist organization to appear larger or more influential than it really is (Thomas, 2003, Goodman et al., 2006). Thus, the Internet "acts as a 'force multiplier', as it is able to reach large audiences and in turn amplify the effect of communication without increasing the number of attackers" (Goodman et al., 2006, 198).

Jenkins (2007) stated that many groups, such as al Qaeda, communicate their message publicly more than any other group previously. He (Jenkins 2007, 8) claimed that "No previous clandestine leaders have ever issued so many video and audio tapes, backed up by a vast array of statements from local leaders and spokesmen, strategic documents, recruiting material, field manuals, memoirs, and recorded testaments by suicide attackers."

Technology can also play a crucial role in the expansion of terrorist activity (Weinberg, 2007; Lia, 2005). Jenkins stated that

> While, in part, this extensive outreach reflects the rich oral traditions of Arab culture, the jihadists also exploit the latest communications technology. This is not new; earlier groups used press releases, tapes cassettes, and underground press conferences with hooded spokesmen to proselytize on behalf of their cause. But jihadists have done it better, and this is perhaps their most important achievement. The rise of Al Qaeda coincided with the spread of the Internet, and the jihadists were quick to exploit the opportunities it offered for direct, unmediated communications with constituents. The Internet enabled the jihadists to create a virtual terrorist community without an intervening and vulnerable hierarchy.

Indeed, utilizing the media to publicize a message or distribute information has been a significant component in the overall strategies of terrorist organizations for generations (Qin et al., 2007). In the past, terrorists distributed propaganda through flyers, newspapers, and posters. Terrorist organizations have also launched radio and television stations to broadcast information to a broader range of the public. Importantly,

many of these methods were effective, contingent upon the control and overall influence the terrorists had over the media (Hoffman, 2006).

With the development of the Internet and the World Wide Web, terrorists are now endowed with a media tool that has revolutionized communications in relation to speed, content, audience, and purpose (Hoffman, 2006; Gunaratna, 2007). Indeed, in many cases, terrorists have complete authority and control over the amount and type of information they can disseminate.

Crenshaw (2007) suggested that the methods terrorist organizations employ depend on electronic media. She stated that "Communication via the Internet has become essential. Organizations and small cells are thus able to access both technical information and inspirational tracts, share information among themselves, and publicize their activities to the outside world" (Crenshaw 2007, 19).

Others (Coll & Glasser, 2005; Weimann, 2004; Qin et al., 2007) agree. Qin et al. (2007, 72) stated that

> Terrorist/extremist groups have sought to replicate or supplement the communication, fundraising, propaganda, recruitment, and training functions on the Internet by building Web sites with massive and dynamic online libraries of speeches, training manuals, and multimedia resources that are hyperlinked to other sites that share similar beliefs. The Web sites are designed to communicate with diverse global audiences of members, sympathizers, media, enemies, and the public.

Weinmann (2006, 118) also suggested that

> The Internet can be used to recruit and mobilize supporters to play a more active role in terrorist activities or causes. In addition to seeking converts by using the full panoply of Web site technologies to enhance the presentation of their message, terrorist organizations capture information about users who browse their Web sites. Users who seem most interested in the organization's cause or who seem well-suited to carrying out the organization's work are then contacted.

Ultimately, the technology (as well as its use) will not only improve, but will promote even more sophisticated advancements of exploitation by terrorist organizations (Lia, 2005). Therefore, not only will more terrorist organizations begin using the Internet for information dissemination purposes, but terrorist organizations currently on the Internet will increase and diversify the use of the Internet through technological advances to increase effectiveness. However, for such a strategy to be successful, the terrorist organizations will depend upon establishing credibility with the information user.

Terrorist Organizations and Web Site Credibility

As stated earlier, Schmid and de Graf (1982, 9) declared that "Without communication there can be no terrorism." Hoffman (2006) posited that effective communication tools are pivotal in a terrorist movement's longevity. For Goodman et al. (2007, 194) and White (1991), "Terrorists use three primary tools to amplify their force: media, support networks, and technology." Consequently, terrorist organizations must have an effective, credible means to disseminate their message in order to persist.

Terrorist organizations increasingly utilize the Internet to expand their influence around the globe (Qin et al., 2007; Goodman et al., 2006). Zanini and Edwards (2001, 43) state that "almost without exception, all major (and many minor) terrorist and insurgent groups have Web sites." The use of Web sites has presented terrorist organizations with an extraordinary tool to meet their information and communication needs. As importantly, it does so by providing anonymity, extreme speed, and a global

19

reach. No other tool has empowered these organizations with so much (Goodman et al., 2007).

Much like a corporation involved in e-commerce, terrorist organizations use Web sites to improve their position/situation. In fact, "The jihadist enterprise seems to have patterned itself along modern business lines. This underscores the observation that al Qaeda was never a military organization: it is much more a missionary enterprise that employs violence to sell its ideology" (Jenkins 2007, 9). In fact, groups such as al Qaeda are comparable to "a franchise, venture capital, or grant-making organization" (Crenshaw 2007, 20).

Indeed, "The worldwide spread of technology has increased access to the outside world, essentially 'flattening' the globe by increasing communications" (Goodman et al., 2006, 198). Friedman (2005) reasoned that converging factors such as wide-spread production of Web-based tools, an increase in the ubiquity of computers, and an expansion of global markets resulting from societies becoming more open (in countries such as China, Russia, and in Eastern Europe), promote cross-cultural communication and collaboration vis-à-vis greater access to the Internet (Goodman et al., 2006). More importantly, "Just as the Internet and the spread of technology enable increased communication for the purposes of industry, civilian, and government relations, this technology enables terrorists to increase their communication, productivity, and collaboration" (Goodman et al., 2006, 197). Additionally, increased connectivity not only allows for "more efficient business transactions, it also allows for fast and direct communication among terrorists" (Goodman et al., 2006, 198).

However, because of the nature of the business, terrorist Web sites are also different from e-commerce sites. Fundamentally, terrorist sites sell an ideology. Furthermore, the ideology is presented in a contextually relevant narrative. That is, terrorist organizations sell a lifeway or way of being. Moreover, the lifeway is expressed as under threat from an external source. As a consequence, the lifeway must be protected by any means necessary and the terrorist group has risen to that challenge, providing resistance for those who are incapable of doing so.

Terrorist organizations present the narrative through dissemination of information of many different types. Information on Web site's therefore often describe the group's history, its overall objectives, its successes, the damage inflicted by the enemy on its constituency, news, biographies, videos of speeches, protests, actual terrorist actions, communiqués, etc. (Hoffman, 2006). Many also provide the means for users to contribute monies, download literature or 'how-to-guides', or communicate with members. Several organizations have multiple sites to increase visibility and/or design sites in numerous languages for broader information distribution (Whine, 1999). Moreover, terrorists use Web sites to target others' emotions by conveying a salient message in order to support specific objectives.

Many terrorist organizations excel in the mastery of Web site design. The "Middle East Arab terrorist organizations in particular are seen as being on the 'cutting edge of organizational networking', having demonstrated an ability to harness information technology for offensive operations, as well as using the more typical propaganda, fund-raising, and recruiting purposes of other groups" (Hoffman 2006, 207). Notably, the levels of technological sophistication reached by terrorist organizations in recent times

have impacted the image they are able to portray on the Internet. Qin et al. (2006, 80) found that "Multimedia content is more attractive and tends to leave a stronger impression on people than pure textual content. While the terrorist/extremist groups are not as good as the US government in terms of organizing their Web functionalities, they employed a significantly higher level of embedded multimedia techniques, especially images and audio/video clips, to catch the interests of their target audience." In concurrence, Hoffman (2006, 226) stated that the Web sites administered by terrorist organizations and their supporters increasingly present a "compelling and indeed accepted point of view."

The aspiration to reach an audience faster and with a greater amount of perceived high quality information is apparently prominent in most terrorist organizations. Furthermore, the abilities of terrorist organizations to produce sophisticated Web sites will only improve. However, the implications of such improvements are not clearly understood beyond the point "that as terrorist communications continue to change and evolve, so will the nature of terrorism itself" (Hoffman 2006, 228). Similarly, Gunaratna (2007) pointed out that increasingly sophisticated employment of the Internet by terrorist organizations must be the primary concern of counterterrorist agencies. Further, "…the counterterrorism technical community has no option but to develop a robust understanding of the Internet and develop the tools to surveil and track individuals on the Internet" (Gunaratna 2007, 69). Unfortunately, "This is the forgotten dimension of counterterrorism" (Gunaratna 2007, 70). In fact, as Qin et al. (2007, 71) point out, "our empirical understanding of (terrorists') Internet usage is still limited." Thus, a strong need exists for research that

investigates effects of Internet use by terrorists such as possible correlations between terrorist organizations' Web sites and their actual organizational success.

As this section has illustrated, credibility is, and will be increasingly important to terrorist organizations. Essentially, they must receive 'buy in' from their constituencies in order to survive. But what is meant by credibility? And what is the difference between credibility and perceived credibility? Indeed, several questions arise when discussing credibility, perceived credibility, or factors affecting credibility. The following sections address these inquiries.

What is Credibility?

The literature on credibility dates back to the 1930s and addressed this concept in a sophisticated manner. However, contemporary scholars state simply that credibility is believability (Fogg & Tseng, 1999; Tseng & Fogg, 1999; Fogg et al. 2001, Metzger, 2007; Wathen & Burkell, 2002), or that "credibility is a political phenomenon" and it "is the extent to which something is believable" (Cioffi 1983, 74, 75) Sources are believed credible based on a perception of competence, character, composure, dynamism, and sociability (Wathen & Burkell, 2002; Burgoon et al., 2000). In other words, if an information seeker locates information that they determine is believable, then credibility is applied to that information.

Others (Fogg & Tseng, 1999; Fogg et al., 2001; Petty & Cacioppo, 1981; Self, 1996) suggested that credibility can be characterized as a perceived quality – made up of multiple dimensions such as trustworthiness and expertise. Perceptions of credibility also come from individuals "evaluating multiple dimensions simultaneously" (Fogg, et

al., 2001, 62; Buller & Burgoon, 1996; Gatignon & Robertson, 1991; Petty & Cacioppo, 1981; Self, 1996; Stiff, 1994). Although no comprehensive agreement exists in the literature on how many dimensions are considered by the information user, agreement does exist that trustworthiness and expertise are two components of credibility (Fogg et al., 2001).

Importantly, trust and credibility should not be considered synonymous. Rather, trustworthiness and expertise in aggregate are used by consumers to determine levels of credibility (Fogg et al., 2001; Fogg et al., 2002a,b; Fogg & Tseng, 1999; Metzger, 2007). Trustworthiness is defined as "well-intentioned, truthfulness, (or) unbiased" and integrates the "goodness or morality of the source" (Fogg et al., 2001, 62).

Expertise is another dimension of trustworthiness and is defined as "knowledgeable, experienced, (or) competent," or taking into account the "perceived knowledge and skill of the source" (Fogg et al., 2001, 62). Wilson and Sherrell (1993, 102) suggested that "a communication source possesses credibility if his/her statements are considered truthful and valid…and thus worthy of serious consideration. A member of a target audience may accept (internalize) the influence of the communication source because the advocated behavior is congruent with his/her own value system."

Fundamentally, credibility is all about perspective. It is believability in something, not trust. Accordingly, if a person perceives something or someone to be credible, then, to that person, it is. Therefore, perceived credibility is a viable conception to consider.

What is Perceived Credibility?

Numerous studies (Fogg et al., 2001; Fogg et al., 2002b; Metzger, 2007) have

been conducted to ascertain what factors influence one's perceived credibility of Web sites. These studies used Web sites previously constructed by the researcher. Many factors were tested by varying the errors, contrast (the difference in color between the text and the background), type of information, and media. Researchers then surveyed information users through a simple questionnaire to rate Web sites based upon multiple criteria. They subsequently determined what factors play a role in the information user's perception of a credible Web site as well as the relative significance of those factors. The result was the creation of several models that are used in the literature to measure perceived credibility.

Future researchers can assess a Web site's perceived credibility of the information user by examining the Web site using an applicable model. The information provided can more easily be measured to illustrate impacts of ambience, functionality, or information reliability on credibility. This is the approach taken with this study.

Types of Credibility

Tseng and Fogg (1999) suggested four types of credibility for consideration. The first type was "presumed credibility." This form of credibility is applied by an information seeker to a Web site when that seeker is from a culture that, for a variety of reasons (Andrews & Gutkin, 1991; Bauhs & Cooke, 1994; Muir & Moray, 1996; Waern & Ramberg, 1996; Sheridan et al., 1983; Lerch & Prietula, 1989), presumes computers as flawless or unbiased. Thus, the information seeker may have a preconceived notion of credibility toward the computer and the information it provides prior to using it.

The second type was "reputed credibility." Generally, this type of credibility is

perceived by the information seeker because of what a third party has said. Reputed credibility can also be perceived when Web sites have links to other Web sites.

"Surface credibility" was the third type. With this type of credibility, information seekers simply judge the book by its cover, or in other words apply credibility based on the initial presentation of that information. Regarding Web site credibility, visual design is most important, particularly design features such as color tones, page layout, and visual aids.

The fourth and final was "experienced credibility." Here, information seekers apply credibility to the interface contingent upon their previous experience with it. This is perhaps the most complex of the four types of credibility and deserves further research.

Fundamentally, credibility is a perceived conception applied to a Web site and/or the information it presents. Without applied credibility, an organization will experience difficulty selling its product or service. Consequently, how the information is presented is as important as what information is being presented. This is even more crucial in a terrorism context where organizations attempt to sell an ideology. Furthermore, credibility is dynamic, constantly under threat of change. A discussion of the dynamics of credibility follows.

Dynamics of Credibility

Other research on digitally based information sources focuses on the dynamics of credibility (Fogg & Tseng, 1999; Tseng & Fogg, 1999), or how credibility is gained, lost, and regained again. Researchers found that information that users deemed as correct or accurate led to credibility gain (Hanowski et al., 1994; Kantowitz et al., 1997;

26

Muir & Moray, 1996). Conversely, credibility was lost when users found the information false or inaccurate (Kantowitz et al., 1997; Lee, 1991; Muir & Moray, 1996).

Self (1996, 423) presented three ideas about credibility: "First, sources are credible because their message's rightness is perceived by the audience. Second, sources are credible because they rightly read how to reveal themselves to particular audiences. And third, sources are perceived to be credible because of audience characteristics." Thus, as Self explains, the message, the source, and the audience each contribute to credibility and he indicates how each receives credibility. However, what if credibility is lost?

Regaining credibility is somewhat difficult (Lee & Moray, 1992). The literature suggested two ways this may be done. First, a Web site can provide good information over a certain period of time (Hanowski et al., 1994; Kantowitz et al., 1997) or if an error is made, but is consistent over time allowing the user to anticipate and compensate for it, credibility might be regained (Muir & Moray, 1996). However, once a user perceives the Web site has no credibility, he/she will discontinue using it. Consequently, credibility is unlikely to be regained (Muir & Moray, 1996).

This discussion underscores the value of credibility to the general information provider. Because credibility can be gained or lost quite easily and quickly, the constant challenge for terrorist organizations is to establish and sustain credibility with information users. Moreover, they must do so in an emotionally laden context while at the same time, presenting information perceived as credible in many different languages. However, this assumes that credibility may be important to the terrorist organization. The following sections address the integrity of this assumption.

Does Credibility Matter?

In many cases credibility does not matter to the user (Tseng & Fogg, 1999; Fogg & Tseng, 1999). For example, studies (Tseng & Fogg, 1999; Fogg & Tseng, 1999) show that computer credibility is not a factor when users are not aware that a computer is operating certain tasks (such as in a vehicle's fuel system), users do not perceive the possible bias or incompetent influence of a computer (such as in a calculator), users apply no saliency to the interaction with the computer (such as when casually searching the Internet), or when the computer is acting as a transmittal device (such as in a video conference).

However, in other instances, computer credibility is quite important, such as when the source is used for knowledge, instruction, decision aids, and metric, performance, or status reporting (Fogg & Tseng, 1999). For knowledge repositories, credibility is critical when data or other information is being sought, stored, or organized. When information seekers receive instruction or advice from a computer, credibility is also important. Such instruction can be subtle, such as default buttons on dialogue boxes, or they can be quite apparent, such as online help systems. Credibility also has an impact on scientists' use of computers as measurement tools or storage devices. Indeed, context contributes significantly to the degree of credibility and as a result, will be further discussed below.

Credibility is also important for Web site designers, but for a different reason. For those persons providing information to information seekers, it is their message that they want "attended to, recalled, or acted upon. If a user rejects new information as not credible, that information will not be learned, nor can it have any other impact" (Wathen

& Burkell 2002, 134). In fact, the literature agrees that credibility is a significant factor to consider when designing a Web site or when seeking information on a particular issue. Moreover, within an e-commerce context, if a Web site has little perceived credibility among its users, it will not enjoy success (Fogg et al., 2002). Consequently, the organization employing the Web site in an e-commerce context may become economically disadvantaged relative to its competition. Potential results may be a decrease in demand for goods and/or services produced and perhaps even a loss of market share. Ultimately, an organization with a profit motive may cease to exist if it is overly dependent upon an ineffective computer-based interface.

Such concerns in an e-commerce setting are not too dissimilar from the concerns of terrorist organizations. Although this relationship will be more deeply discussed below, it is sufficient to say here that terrorist organizations also need the support of consumers. That is, for a terrorist organization to survive over the long term, it must receive enough support from the people to overcome the many challenges it faces, such as monetary, secrecy, security, or recruitment (Hoffman, 2006; Gunaratna, 2007). Consequently, it can be assumed that credibility is important for terrorist organizations in order to reach many of their objectives. Accordingly, factors affecting the level of credibility perceived by the information user might possibly be a concern.

What Affects Credibility?

It is assumed here that credibility has as much influence on the objectives of a terrorist organization's Web site as one sponsored by an international corporation. At the same time, other factors might be considered when evaluating the credibility of a

Web site and the information it provides, such as the type of information source, errors on the Web site, information complexity, and user demographics. Because credibility can have such a significant influence on a message, it is essential that researchers have a greater understanding of how users decide what is credible and what is not (Wathen & Burkell, 2002). Moreover, it is important to discuss these factors as many of them are employed in models measuring perceived credibility.

Human vs. Digital Sources of Information

Some scholars (Cioffi, 1983; Dennis, 1996; Morley & Walker, 1987; Petty & Cacioppo, 1986) suggest that a vital factor affecting information acceptance is how credible the information is perceived to be. When it comes to Web-based information, some researchers suggest that people perceive digital sources of information as objective or infallible, consequently applying greater credibility than to humans (Andrews & Gutkin, 1991; Bauhs & Cooke, 1994; Honaker & Harrel, 1986; Kerber, 1983; Pancer et al., 1992; Sheridan et al., 1983).

Conversely, some empirical studies show that people do not perceive digital sources of information as being more credible than humans (Andrews & Gutkin, 1991; Honaker et al., 1986; Matarazzo, 1986; Pancer et al., 1992; Lerch & Prietula, 1989; Waern & Ramber, 1996). In fact, in certain instances they are seen as less credible than humans. Nevertheless, although it may be intuitive for people to perceive digital sources of information as more credible than humans, "no solid empirical evidence supports this notion" (Fogg & Tseng 1999, 81).

Although little research exists in this area in relation to terrorists' Web sites, I

offer that information seekers are likely to deem these types of Web sites as credible

based upon the context. That is, whether credibility was applied to a particular type of

information source might be contingent upon the context. In a terrorism context, terrorist

organizations' Web sites may generally receive high credibility from constituents due to

their awareness that terrorists emphasize secrecy when disseminating information.

Conversely, for the terrorists' adversary, the Web sites may receive little to no

credibility.

Errors

Errors in the interface have varying impacts on credibility. These might be

spelling, typographical, functional, contextual, or other type of error. However, the

literature is undecided as to the specific influence from small or large errors (Kantowitz

et al., 1997; Lee, 1991; Lee & Moray, 1992; Muir & Moray, 1996), but consensus does

exist that small errors "have disproportionately large effects on perceptions of credibility"

(Fogg & Tseng 1999, 82; Fogg et al., 2001). For example, I propose that small errors

will likely have a significant effect on perceived credibility particularly when they are

found on a page where little information is presented. However, the true effect of errors

on perceived credibility of terrorist organizations' Web sites may not be as the literature

suggests. In fact, it is likely that errors will have little to no effect on perceived credibility

of terrorist organizations' Web sites where errors occur in information that has been

translated. Here, context plays a significant role and its importance is addressed below.

Information Complexity and Source

Cioffi (1983) found that the credibility of information or its sources is unstable. He suggested that the complexity of an issue and the overall complexity of the information being received on that issue can impact credibility. His research found that credibility suffers as complexity increases. In addition, he concluded that credibility "can be related to estimated likelihood" (Cioffi 1983, 80). That is, the level of credibility applied to information is based upon the perceived likelihood that the information is as it is presented.

Dennis (1996) found that if a source is not challengeable, the credibility of the information is likely to decrease. In other words, if one cannot investigate and determine the source of the information in question, the credibility of that information will suffer. Similarly, a message and its source can be formatted to match consumer interests to increase overall credibility (Wathen & Burkell, 2002). This is particularly relevant to terrorist organizations' Web sites where the overall appearance and the types of issues addressed are primarily most salient to the constituents of the organization.

Research has also shown that the manner in which a message was conveyed was lost by the consumer over time. Consequently, "It may be, therefore, that the primary influence of credibility factors is at the point of 'first contact' between the receiver and the message: the mean by which the message is made persuasive might not matter in the long run, only that it was persuasive in the first place" (Wathen & Burkell 2002, 136).

Interestingly, Wilson and Sherrell (1993) found that "if a message is high in discrepancy, low in incongruity, and if the source is identified early in the message, then

high-credibility sources will tend to have a greater impact on knowledge/attitudes/ behaviors than low credibility sources" (Wathen & Burkell 2002, 136). Other scholars (Slater & Rouner, 1996) posit that credibility assessments are related to three areas related to the information source: "knowledge and attitudes about the source specifically, attitudes about credentials, and quality of the message, including its presentation, plausibility, and whether it is supported by data or good examples" (Wathen & Burkell 2002, 136). Such research demonstrates that the manner in which a message is conveyed can impact how it is perceived (Wathen & Burkell, 2002).

User Demographics and Credibility

User demographics also impact credibility (Gatignon & Robertson, 1991; Self, 1996; Zajonc, 1980). For instance, if users are familiar with the content they are more likely to find the information less credible (Honaker et al., 1986; Kantowitz et al., 1997; Lerch & Prietula, 1989; Tseng & Fogg, 1999). That is, if one perceives one's self as knowledgeable in a certain area or field, it is quite likely that the information surveyed will be critically evaluated. Consequently, errors or inaccuracies in the information are likely to be found. On the other hand, those persons not familiar with the information are not as critical and thus more likely to find the information credible (Gatignon & Robertson, 1991; Self, 1996; Zajonc, 1980). Conversely, Self (1996) found that an information seeker's familiarity level of a message directly correlates with the level of credibility.

Users' knowledge of computer systems also plays a role. For example, if an information user is proficient in a certain computer system, flaws are likelier to be found,

thus discounting the credibility of the information being presented. However, the literature is undecided as to the exact relationship (Bauhs & Cooke, 1994; Lee, 1991; Lerch & Prietula, 1989; Miller & Larson, 1992; Muir, 1988; Waern et al., 1992).

Credibility can also be affected by other factors such as Web site design and use of color and layout (Kim & Moon, 1997). Here the literature suggested that the more a Web site appears as professionally developed, the likelier credibility will be applied. In addition, users tend to apply greater amounts of credibility to Web sites that have complimentary colors and layout designs.

Human credibility factors such as communal homogeneity also affect levels of credibility (Mackie et al., 1990). That is, perceived credibility increases where people are exposed to Internet based information that is distributed by a group based out of the same community. Additionally, geographical proximity to similar groups providing information via a Web site has been argued to increase credibility (Byrne, 1971; Cialdini, 1993; Zimbardo & Leippe, 1991).

A need for information also affects perceived credibility (Tseng & Fogg, 1999). That is, "People with a greater need are generally more likely to accept information from the technology. Specifically, people in unfamiliar situations or who have already failed at the task when relying only on themselves perceive computing technology as more credible" (Tseng & Fogg 1999, 43; Kantowitz et al., 1997).

Some scholars (Wathen & Burkell, 2002) claimed that when people lack expertise in an area and thus perceive information as being credible they might suffer from a 'gullibility-error'. This occurs because users are less willing or capable of determining credibility and consequently deem information credible from a source that is

not credible. Conversely, when experts in certain fields view information with a skeptical approach they can suffer from an 'incredulity error'. In this case, experts might discount credibility because of hyper-skepticism when in fact the information may be credible.

Fogg et al. (2001) found other demographic factors that have an influence on how individuals apply credibility to Web sites. Their study surveyed over 1400 individuals and looked at several demographic variables including age, gender, country of origin, education level, income level, and personal experience on the Web. Their findings concluded that younger persons are likelier to be more critical of signs of amateurism than are older persons. In other words, younger persons graded Web sites more harshly when it contained errors or glitches such as broken links or even a single typographical error. In contrast, older respondents reacted positively toward elements of expertise and trustworthiness. In addition, they graded Web sites higher when some degree of tailoring to the consumer appeared.

When it came to gender, men reacted more negatively overall than women. Here Fogg et al. (2001) found that men generally answered questions regarding credibility with a greater tendency to be critical or skeptical of a Web site's credibility. This may be evidence that men have higher standards regarding credibility and are more leery of information received via the Web than women or it perhaps it is that women are not quite as critical in responding to the sample questions.

The survey also applied a cross-cultural component as it accounted for country of origin of respondent. However, it should be noted that, although differences were identified between the respondents, questionnaires were answered by only two countries, Finland and the United States. Furthermore, these two countries are both

western and have different perspectives of the Internet relative to those within other communities around the globe. Nevertheless, Fogg et al. did find some interesting disparities of statistical significance. The findings showed that Finns are much more critical of commercially related Web sites or those that show signs of amateurism than persons in the U.S. Conversely, persons from the U.S. generally applied higher levels of credibility to Web sites that appeared to have some level of tailoring and that conveyed expertise and trustworthiness.

Finally, Fogg et al. (2001) found little to no dissimilarities between some demographic variables. Concerning education levels, Fogg et al. found that those individuals with higher levels of education (graduate level), in contrast to those with no college education, applied greater credibility to those sites that showed more trustworthiness. Interestingly, they found no other statistically significant differences. Similarly, they discovered that in relation to levels of income, individuals with higher levels of income applied greater credibility to sites that tailored information to the user. Here again, no other disparities of statistical significance were noted. Interestingly, when it came to a person's level of experience on the Web, no statistical evidence was found to show that differences exist.

Relevance

Relevance has been defined by many as a contributing factor in information acceptance. Benbasat and Zmud (1999) stated that to be relevant, information must be implementable. They claimed that relevant information must be palpable, it must provide real value, it must be pragmatic, and it must be timely (Benbasat & Zmud, 1999). Herz

(1971) claimed that "only that which has a potential bearing on the future can be considered as relevant" (Sullivan 1973, 314). Sullivan (1973) maintained three definitions (or perhaps more aptly put, three characteristics) for relevance. First, information "may be relevant if it simply aids us in 'understanding' a given phenomenon; it may provide information without which we might draw erroneous conclusions" (Sullivan 1973, 316). Second, information is relevant when it is "pertinent in a very specific way to a given problem or situation" (Sullivan 1973, 316), that is, when it is timely. And finally, information is relevant when it is utilizable or useful. Further, he suggested that analysts must evaluate "who the information will be relevant to and what type would be relevant" (Sullivan 1973, 323).

Barry and Schamber (1998) asserted that several factors have been suggested by scholars as affecting relevance judgments. These include an individual's level of knowledge and their cognitive state, "perceptions and beliefs of the user, qualities of information such as topical appropriateness, recency, accuracy, and clarity, and situational factors such as time constraints and the effort and cost involved in obtaining information" (Barry & Schamber 1998, 220). According to Taylor (1962, 1968, 1985, 1988) "factors such as educational background, familiarity with the subject area, and the user's intuitive sense of analogy all affect the user's state of readiness" (Barry & Schamber 1998, 220).

Additionally, Barry and Schamber (1998, 221) suggested that relevance is "(a) cognitive and subjective, depending on a user's knowledge and perceptions; (b) situational; (c) complex and multidimensional, influenced by many factors; (d) dynamic, constantly changing over time; and (e) yet systematic, observable and measurable at a

single point in time." They also maintained that "information seekers must make judgments in order to predict or determine whether information at hand will help resolve their information problems" (Barry & Schamber 1998, 221).

Indeed, a person's evaluations of whether information is relevant depends on "their individual perceptions of their problem situations and the information environment as a whole, and that their perceptions encompass many factors beyond information content" (Barry & Schamber 1998, 234). Furthermore, Barry (1993, 1994) found that "relevance was conceptualized as any connection that existed between the information contained within the documents and the user's information need situations" (Barry & Schamber 1998, 223).

For Dennis (1996), relevance is contingent upon how well the information matches the topic under evaluation. In his research, he discovered that the acceptance or rejection of information is based on how relevant participants assess it to be and the social implications of its acceptance or rejection. In other words, two factors to consider when determining the impact of relevance are an individual's assessment of the information's relevancy and the perceived societal responses to accepting or rejecting the information. Initially when individuals are exposed to new information they first analyze it in contrast to information they already possess. In other words, they consider this information in contrast to the communal belief system that correlates with the situation (Dennis, 1996; Burnstein & Vinokur, 1973).

Lord et al. (1979) similarly claimed that the relevancy of information also affects the acceptance/rejection process when it is in contrast to the prevailing communal perspective. Benbasat and Zmud (1999) concured. They maintained that "when

presented with messages containing information supporting both sides of an issue, individuals tend to focus on the information supporting their preference and discount the information opposing it" (Dennis 1996, 437). Therefore, information in opposition to a communally accepted belief system is more likely to be found irrelevant or less relevant than if it were in correlation.

It has also been concluded that issue saliency determines the degree to which relevance impacts the process. Baker and Wagner (1987) concluded in their research that people do not always look into the accuracy of information or for its general truthfulness or even with it being consistent with what they already know (Allen, 1996). Information can also be inaccurate, but still considered relevant if it is continuously disseminated verbally over time. Indeed, information continuously circulated among the masses can be considered as relevant and have a significant impact on the collective (Dennis, 1996). Such a claim is not a novelty.

In the late 19th century, Peirce (1877, 66) claimed that

> as soon as a firm belief is reached we are entirely satisfied, whether the belief be true or false…we seek for a belief that we shall think to be true. But we think each one of our beliefs to be true, and indeed, it is a mere tautology to say so.

Finally, when an issue requires a certain type of information, that is theoretical or practical, but the alternative is provided, the information may be considered less relevant or perhaps even irrelevant (Benbasat & Zmud, 1999). Consequently, the information deemed less relevant or irrelevant may be discarded.

Novelty

Another prominent factor affecting the information acceptance/rejection process

is the novelty of the information. Dennis (1996) and Morley and Walker (1987) posited that for a perspective to change or be changed, particularly when related to a specific issue, information must be important, novel, and credible. For Allen (1996, 197), certain factors "such as novelty, are specifically associated with users" of information. However, "assessments of the novelty of the information presented depend on what else the user has seen" (Allen 1996, 197). That is, knowledge levels and education, as well as many other factors have a significant contribution on whether an individual considers a piece of information novel or not.

Similarly, past life experiences which have created individual and communal perspectives are likely to play a leading role in establishing information as credible. Osgood and Tannenbaum's (1955) presentation of *Congruity Theory* seems to confirm this. They asserted that the individual is assumed to have preconceived perspectives and attitudes on the source of information as well as the issue. Consequently, on the cognitive level, when these perspectives or attitudes are not in agreement, incongruity occurs (Osgood & Tannenbaum, 1955).

The literature on Web site credibility illustrates that the perception of a Web site impacts an individual's trust in that site as well as its sponsor. This in turn affects the consumer's intent on purchasing a product or service via that Web site. However, what about the effects of a Web site's credibility on a terrorist organization? More specifically, can the credibility of a terrorist organization's Web site correlate with its overall success?

Context

It is important to reiterate that many factors have an impact on credibility. The previous section discussed several including human vs. digital sources of information, errors, information complexity and source, user demographics, relevance, and novelty. Research on terrorist organizations' Web sites will further clarify the extent to which they impact credibility perceived by the information user. I suggest that it all depends upon context. That is, the contexts that information is created, distributed, and received in, impact all other contributing factors.

The literature suggested that credibility was an important factor when designing and using Web sites for information dissemination. However, situational aspects do exist that significantly contribute to information seekers' perceptions of credibility, particularly context.

Some scholars suggested that when persons are positioned in unfamiliar situations, increased levels of credibility are applied to the interface (Muir, 1988). Others maintained that when individuals are unsuccessful at solving a particular problem, the information sought from digitally-based information sources is deemed more credible (Tseng & Fogg, 1999). Still others claimed that when people exhibit a strong information need, Web-based resources will be perceived as highly credible (Hanowski et al., 1994; Kantowitz et al., 1997).

Goffman (1974, 116) defined context as "immediately available events which are compatible with one frame of understanding and incompatible with others." Glassie (1979) claimed that "the particularistic context is the observable environment of an expression of culture" (Young 1985, 117). For Hall (1977), "Contexting probably

involves at least two entirely different but interrelated processes – one inside the

organism and the other outside. The first takes place in the brain and is a function of

either past experience (programmed, internalized contexting) or the structure of the

nervous system (innate contexting), or both. External contexting comprises the situation

and/or setting in which an event occurs (situational or environmental contexting)"

(Young 1985, 120).

Young (1985, 116) defined context as "whatever bears on the event whether it is

contiguous or not." She further stated that a complete integration occurs between

information and the context it is located in, information and context are interdependent,

and a context is multiple in character (Young, 1985).

Similarly, Goldstein's (1964) criteria for context included a "Physical setting,

interactions among participants, performance, time and duration, sentiments expressed,

miscellaneous observation, and the observer. Also, personal history of informants,

aesthetics of informants, knowledge, feelings, and meanings, the transmission of

folklore materials, descriptions of folklore situations collectors are unable to observe,

and informant's repertories" (Young 1985, 116).

Cohen (1986) suggested that aspects of knowledge and information are context

sensitive. Furthermore, knowledge has a social component. That is, "The level to which

knowledge can be undermined by environmental factors is socially determined" (Cohen

1986, 578). This occurs from the influence of what Cohen terms 'defeaters'. He

asserted that "The ability of a defeater to undermine knowledge is determined in part by

intersubjective standards" (Cohen 1986, 578). Moreover, the social groups that we live

in set standards of acceptance. "Thus it is important to evaluate what social group is the

most relevant or influential on a given issue. Is it the immediate familial group or society at large" (Cohen 1986, 579)? In other words, standards for accepting information are structured – perhaps constructed within the community. He suggested that "A particular standard for a piece of information is provided by context" (Cohen 1986, 581). Additionally, during every-day activities and functions, skepticism is not an issue. The norms and standards previously established find that skeptical opposition to accepting information is not relevant. In fact, "relevance is governed by a context-sensitive standard" or perspective (Cohen 1986, 583).

Young (1985, 117) further suggested that the "Number of possible contexts for an event are limitless, but number of relevant contexts for understanding an event is limited." According to her, events are context specific. She posited two designs for how contexts apply to information behavior. First, "Contexts are contexts of events. Each context brings a different perspective to bear on the event and the event presents itself in a different perspective to each context" (Young 1985, 117). Second, "Contexts are also contexts for perceivers. They shift with shifts in the mode of attention of perceivers and from one perceiver to another" (Young 1985, 117). Consequently, "The same event seen in a different context is, in a sense, a different event" (Young 1985, 117). Young continued by contending that contexts are not only multiple, they are also constitutive. Therefore, contexts impact a way of thinking about an event. In other words, they significantly influence a person who creates a perspective or perhaps more logically, they affect an already existing one.

Context plays a prominent role in Web site credibility. Accordingly, it is imperative that researchers consider the context when studying terrorist organizations' Web sites.

The source and complexity of the information, quantity and type of errors, overall relevance and novelty are all notable considerations, but they are all situated in varying contexts. That is, these factors all exist in a separate context when and where the information is created, distributed, and received. Cultural attributes, historical experiences, religious beliefs, and traditional lifeways are all context specific and their importance cannot be discounted. Disregard to contextual differences may bring about enormous misconceptions of a perceived reality. This is particularly true when evaluating a social practice of a population which is starkly different than one's own.

Indeed, measuring numerous factors is difficult and requires an applicable, viable model. Accordingly, the next section provides a discussion on models used in the literature to assess perceived credibility.

Toward Assessing Perceived Credibility

The body of literature devoted to the study of the World Wide Web is growing. Scholarship has been presented on a wide array of topics from how individuals seek information on the Internet to what factors affect Web site design (Wathen & Burkell, 2002). With the Internet becoming the predominant source of information for users over the last two decades, issues of information credibility are on the rise (Metzger, 2007; Wathen & Burkell, 2002).

However, assuming that an intended objective of terrorist organizations is the attainment of perceived credibility, are there credibility differences between terrorist organizations' Web sites? Several scholars (Everard & Galletta, 2005; Corritore et al., 2003; Grabner-Krauter & Kaluscha, 2003; Hoffman et al., 1999; McKnight et al., 2003;

Sivasailam et al., 2002) declared that a Web site can have a significant impact on an organization's proliferation and even survival. It should be noted that this scholarship however, is conducted in an e-commerce context. I found no research that determines whether a Web site, as a form of media, can have an impact on an organization's potential effectiveness where that organization's primary objective is committing violent acts toward persons or other physical interests of a state or other social or political entities.

The terrorism literature does not provide much clarity either. The research related to the use of the Internet by terrorist organizations in this discipline (Qin et al., 2007; Zhou et al., 2005; Chen et al., 2004; ISTS, 2004; Thomas, 2003; Tsfati & Weimann, 2002; Weimann, 2004) is limited to link, content, and technology analyses. That is, what information the Web site is providing to consumers, what benefits the organization hopes to receive, or the advances in technology used on Web sites. No research has been undertaken to move toward determination of the potential effectiveness of these Web sites. In order to reach such a determination, research must first be conducted on the perceived credibility of different terrorist organizations' Web sites.

Web Site Credibility Models

One central consideration for new research is to utilize a comprehensive, relevant, applicable, and accurate model to test hypotheses and/or evaluate relationships between variables. Assessing perceived credibility of Web sites is no different.

Several models are discussed throughout the literature on Web site credibility

and were considered for this project. One important caveat is that although many criticisms might be posited regarding the usefulness of the models presented here, only the primary concerns related to a few models are addressed. The intent is to initiate a substantive dialogue related to the need for the development of applicable models that can accurately assess perceived Web site credibility in a terrorism context.

The quest for a model brought about two questions. First, are the models presented in the literature applicable to research that assesses perceived Web site credibility in a terrorism context? That is, do they incorporate appropriate variables to measure perceived credibility in such a unique context? Second, does a model exist that can aid researchers in studies conducted on perceived credibility without the researcher making physical contact with group members or its supporters? Because of the nature of terrorism and the activities of terrorist organizations, it became clear that face-to-face contact between researcher and participant or supporter might be extremely complicated, if not unsafe. Therefore, variables measuring trustworthiness may not be feasible. Consequently, a need for a model that can be employed without such contact existed.

It was discovered early on that many models suffer from applicability issues related to their metrics. That is, many of the metrics measured attributes not relevant in a terrorism context. Furthermore, many of the models required data be acquired from the primary information users, in other words the supporters or members of the organization under investigation. Undoubtedly, this presented several problematic issues that needed to be overcome in order to conduct this study. A few of those are addressed in the following section.

Applicability

One issue that arose in the search for an acceptable model was inapplicable

metrics. In some cases, models included variables that measured the impact of

personal or corporate associations with the organization or the information presented on

the Web site. In other cases, models had variables that measured the effects of

information provided on the organization's physical location.

Table 1 shows the Fogg et al. (2001) model. It includes several variables that

were inappropriate for this study. They were *Physical Address, Phone Number, Photos*

of Members, Email Address, Domain Name and Company Name Do Not Match, and

Lists Author's Credentials. These variables were not suitable for this context because of

the nature of the organizations' activities.

That is, these organizations operate under extreme secrecy in many cases and

thus much of the information assessed by these variables may likely be highly guarded

by the organization and consequently not disseminated. *Lists Author's Credentials* was

also rejected due to the likelihood that the display of credentials relevant to terrorists is

not necessary to garner constituent support.

Other models presented similar concerns. Table 2 displays the metrics used in

the Fogg et al. (2002b) model. In this example, *URL Address* was not an acceptable

variable because of potential intent by the terrorist organization to remain unidentifiable.

Table 1: Fogg et al. (2001a) Model Assessing Web Site Credibility

Real-World Feel	Ease of Use	Expertise	Trustworthiness	Tailoring	Commercial Implications	Amateurism
Quick Response Time	Can Search Past Content	Operated by External News Organization	Has Believable Links	Sends Confirmation Emails	Advertises on Radio etc.	Recently Updated
Physical Address	Looks Professional	Lists Authors' Credentials	States Policy Content	Preferential News Coverage	Has Relevant Advertisements	Multiple Languages
Phone Number	Coherent Arrangement	Lists Citations and References	Links to Outside Materials & Sources	Recognizes Return Users	Has a Commercial Purpose	Has <5 Pages
Email Address	Download Time	Has Detailed Info on News Stories	Has Links to Competitors	Requires a Log-In	Requires a Paid Subscription	Hosted by Third Party
Photos of Members	Navigability	Claims it is Official Site	Recommended by Friend		Has >1 Ad per Page	Domain & Company Name Do Not Match
		Has Content Reviews/ Ratings	Represents a Non-Profit Org		Has Pop-Ups	Has Typographical Errors
		Shows Awards it has Won	Lists Well-Known Corporate Customers		Difficulty Distinguishing Between Ads & Text	Is Unexpectedly Unavailable
			URL Ends with ".org"			Has Non-working Link(s)
						Has Non-Credible Links
						Rarely Updated

Table 2: Fogg et al. (2002b) Model Assessing Web Site Credibility

Expertise	Trustworthiness	Other
Site Response Time	Repeated Usefulness	Novel Information
Onsite Search Capabilities	Site Links	Professional Appearance
Multiple Languages	Related Links	Coherent Information
Visitor Recognition	URL Address	Appropriate Design
Typographical Errors		Printer-Friendly
Availability		Live-Chat
Bad Links		Third-Party Hosting
		Log in Requirements
		Download Time

In Table 3, the Wathen and Burkell (2002) model employed *Credentials* as a metric. This variable suffers from similar issues as in the Fogg et al. (2001) model.

Table 3: Wathen and Burkell (2002)

Model Assessing Influences on Print and Interpersonal Media

Source	Receiver	Message	Medium	Context
Expertise/ Knowledge	Issue Relevance	Topic/Content	Organization	Distraction/ "Noise"
Trustworthiness	Motivation (Need)	Internal Validity/ Consistency	Usability	Time since message seen
Credentials	Prior Knowledge of Issue	Plausibility of Arguments	Presentation	
Attractiveness	Issue Involvement	Supported by Data or Examples	Vividness	
Similarity to Receiver Beliefs/ Context	Values / Beliefs / Situation	Framing		
Likeability Goodwill Dynamism	Stereotypes of Source or Topic	Repetition/ Familiarity		
	Social Location	Ordering		

Finally, the Metzger (2007) model, shown in Table 4, used *Who Is The Author*, *Contact Information*, and *Author's Qualifications* to assess perceived credibility. Again, such variables were unbefitting for this study. Intuitively, in a terrorism context, it is unlikely that this information would be available in such an open forum due to the covertness of the organization's activities.

Table 4: Metzger (2007) Model Assessing Web Site Credibility.

Accuracy	*Authority*	*Objectivity*	*Currency*	*Coverage/Scope*
External Confirmation	Who is the Author?	Facts/Opinions	Current Information	Completeness
	Official Stamp	Consider Objectives		User Friendliness
	Contact Info			
	Author's Qualifications			

Because the terrorist organization is incessantly under threat of attack by authorities, both electronically and physically, it must be continuously discreet in its activities and location. This includes its location in cyber space. It must also safeguard the identity of supporting entities. Presumably, any information that identifies persons and/or the location of members or supporters is likely to be protected by the organization.

In contrast to the e-commerce Web sites however, the absence of such information on a terrorist organization's Web site may increase legitimacy of the organization, not decrease it. That is, constituent perceptions can be influenced toward providing increased support for the organization if it appears its activities are such a threat to its adversary that the organization must entail a high degree of secrecy in all

that it does. This is directly associated with the narrative, or context, that the organizations operates in.

Other variables were simply not suited to assess terrorists' Web sites. Table 1 includes *Has Content Reviews/Ratings* and *Shows Awards It Has Won*, while the Fogg et al. model in Table 2 uses *Provides Free Financial News*.

Feasibility

Other variables were identified that could not be used because of feasibility issues concerning face-to-face contact with organizational participants or supporters. Many of these variables were related to trustworthiness or specific attributes of an information user.

Tables 1 and 2 include variables that focused on trustworthiness, thus further challenging these models' appropriateness. That is, in order to utilize these metrics, it may be necessary for the researcher to communicate directly with an organization's support base. Such an activity might be extremely difficult and perhaps include significant risk. The variables included *Has Believable Links, Recommended By A Friend, Is an Organization You Respect,* and *Information that Contrasts With One's Own Opinion* in Table 1 and *Repeated Usefulness* in Table 2.

Tables 3 and 5 have several problematic areas. The models presented in these two tables are Wathen and Burkell's (2002) model assessing influences on print and interpersonal media and their model assessing influences on computer media respectively.

Table 5: Wathen and Burkell's (2002)

Model Assessing Influences on Computer Media.

Source / Message / Medium	Receiver
Expertise / Knowledge / Competence	Source / Topic Assumptions
Trustworthiness	Motivation
Content / Relevance / Currency / Accuracy / Tailoring	Issue Knowledge / Expertise
Attractiveness / Format	Technology Expertise
Interface Design	Social Location
Loading Speed	
Usability / Accessibility	
Interactivity / Flexibility	

The tables show that these models have variables directly intended to measure trustworthiness. In addition, they have separate categories with numerous variables that measure technical, intellectual, and psychological attributes of an information user. Such foci make it near impossible to use these models in a study such as the one presented here due to the inability to initiate face-to-face contact with members or supporters of the organization under investigation.

Consequently, the models mentioned above were found to be inappropriate for assessing perceived credibility of terrorist organizations' Web sites. However, one model was identified that presented a solid foundation to build upon. This model and the slight modifications made to it are discussed in the next section.

A Model to Assess Terrorists' Web Sites

The literature review conducted for this study presented several models in recent research that measured perceived credibility of Web sites. However, most were

determined to be unusable in a terrorism context. One model that exhibited potential was identified. It provided a strong base useful to develop a suitable metric of perceived credibility of a terrorist organization's Web site. This model was developed by Everard and Galletta (2005) in their research on impression formation. To ensure an accurate application of the model to the Web sites under investigation here, several improvements were made and are discussed below.

Everard and Galletta's (2005) study on impression formation claimed that flaws are inversely related to credibility. They stated that "Flaws of concern include any features of the system that may degrade the system's ambience, functionality, or information reliability" (Everard & Galletta 2005, 61). Impression formation as they defined it is "the manner in which information presented serves to form users' perceptions of a Web site" (Everard & Galletta 2005, 57).

Table 6: Everard and Galletta (2005) Model Assessing Web Site Credibility

Style	Completeness	Language Errors
Contrast	"Under Construction"	Spelling Errors
Consistent Font	Obsolete Content	Typographical Errors
Crooked Columns	Obsolete Links	Grammatical Errors
Word Spacing	Non-Loading Pictures	Factual Errors
Line Spacing		

Their study examined various types of flaws or imperfections in an experimental context in order to measure hypothesized damage to a Web site's perceived credibility. Their model hypothesized that "errors, poor style, and incompleteness are inversely related to the users' level of perceived quality" (Everard & Galletta 2005, 55). In addition, they found that the perception of flaws rather than flaws themselves impacted

perceived credibility of the Web site. Their model looked at flaws in three types or categories: style, completeness, and language errors. Table 6 displays their model.

Everard and Galletta suggested that style, completeness, and language errors all combine to influence an individual's perception of the online store. As a result, if a potential consumer applies a high level of quality (or credibility) to the online store, they will have trust in it and the products or services it markets. The consumer then makes a purchase. In other words, the consumer seeks a product or service and once an online store is perceived as high quality (or credible), trust is placed in it and a purchase is made. In many ways, this is not too dissimilar from the interactions between terrorist organization and terrorist organization supporter.

In essence, a terrorist organization is "selling" an ideology. For the organization to survive it must have support. To gain support it must build trust in its constituent base through the dissemination of information related to its existence, purpose, and activities. Although a Web site can be used for many reasons, information dissemination is one of its primary functions for terrorist groups. Thus, terrorist organizations "sell" their ideology to the people who in turn "buy in" to the services the organization provides. After necessary adaptations to Everard and Galletta's model, a metric was created that could assess perceived credibility of such an organization's Web site.

A Research Model

Because of the similarities between the fundamental objectives of e-commerce stores and Web sites of terrorist organizations, Everard and Galletta's model was only slightly modified.

Table 7: Research Model Assessing Perceived Credibility of Web Sites

Ambience	Functionality	Information Reliability
Contrast	"Under Construction"	More Than 12 Errors
Consistent Font	Obsolete Content	>1 Error, but <12 Errors
Crooked Columns	Obsolete Links	Spelling Errors
Word Spacing	Non-Loading Media	Typographical Errors
Line Spacing	Onsite Searching	Grammatical Errors
	Multiple Languages	
	Donating Functions	
	Repeat Visitor Recognition	
	Multiple Site Offerings	
	Offers "How To" Guides	
	Uses Multiple Media (Video, RSS Feeds, Blogs, Mail Lists)	

Table 7 shows the resulting research model. Similar to the Everard and Galletta model, the model presented here incorporates an assortment of variables that are categorized into three groups: ambience, functionality, and information reliability. The metrics presented in the model meet the two criteria for this study. That is, each variable is viable and applicable for measuring perceived credibility of Web sites in a terrorism context and they do not require physical contact be made by the researcher with members or supporters of the group.

It is important to reiterate that these metrics do not measure credibility as no person is interviewed or surveyed to determine the amount of credibility one might apply toward a particular Web site. Accordingly, the metrics only assess perceived credibility. In other words, they are metrics that have been shown to accurately illustrate the amount of credibility a person may potentially apply to a Web site.

Applying Credibility

Importantly, credibility is not perceived by the information user in an instant. In fact, credibility is likely perceived in stages. That is, credibility is not only affected by certain factors, but these factors vary in influence at different levels of a Web site and their importance is likely correlated to the depth of the user's movement through the different levels of a Web site.

Within 7 seconds a user is turned on or off from a Web site (Everard & Galletta, 2005). This is due to the user's impression of the Web site based on what he/she initially sees. Consequently, the appearance, or ambience of the homepage, or first level of a Web site, is critical to preserve the interest of the user and maintain the objective of the organization to foster perceived credibility. Ambience of the supporting pages (second, third, fourth levels etc.) of the Web site is also important to establish credibility, but function and information reliability become increasingly more important. Accordingly, factors related to *ambience* are significant influences at the first level. This is the first stage of perceiving credibility. Factors related to functionality and information reliability are more significant at subsequent levels (second, third, fourth, or deeper levels).

If the user perceives the Web site as credible based on impressions of ambience, he/she moves on to look deeper into the Web site, maneuvering through the pages, clicking on links, and viewing the media. The user's approach can be deliberate or inadvertent. Throughout the user's movement, mechanical functions of the Web site become more important. At this point, the second level of the Web site, factors affecting *function* become important. This is the second stage of perceiving credibility.

Finally, if the user has moved through the first two stages of applying credibility he/she begins to evaluate the credibility of the *information* presented. Intuitively, the user starts to focus on specific pieces of information and evaluates them against his/her own cognitively retained and organized information constructs.

During the final stage, information is evaluated for its quality and trusted when it is deemed reliable. Indeed, trust in information is critical to establish perceived credibility of a Web site among information users. In fact, trust "is a reflection of credibility" (Everard & Galletta 2005, 60). To articulate, trust is an attribute of an information user and applied to a Web site. Credibility is an attribute of the Web site and perceived by the information user. Without the information user trusting the information provided by a Web site, the user will not perceive the Web site as credible. Therefore, information reliability is critical to establish perceived credibility of a Web site amongst its users. Consequently, flaws, or errors, can have a significant impact on how reliable presented information will be perceived. Information reliability is the third and final stage of perceiving credibility.

Web sites, more often than not, have several levels in their design. Importantly, the suggestion posited here does not infer that the stages of perceiving credibility correlate directly with the level of the Web site. For example, the second stage of perceiving credibility does not necessarily have to be bound to the second level of the Web site and so on. Multiple levels may be evaluated by the information user in the seven second time period. Consequently, factors related to ambience on the deeper levels may be considered by the user to perceive credibility. Nevertheless, for research

purposes, this study assumes a direct correlation between the stages of perceiving

credibility and the respective levels of the Web site.

Considering this assumption and looking at this process holistically and in a

linear manner, as the user moves through the levels of a Web site seeking information,

the significance of the factors already experienced by the user decline. This continues

until a novel page or piece of information is found. For example, when a user assesses

the credibility of the *information* presented (during the third stage), contrast or word

spacing will have less of an impact than in the user's initial review of the Web site. Over

time, during the user's interaction with the Web site, all factors continue to affect the

user's decision to apply overall credibility to the Web site. However, the amount each

factor impacts the process of perceiving credibility continues to fluctuate, particularly as

the user moves from level to level of the Web site. This is an area that deems further

research.

Summary

In summary, this chapter met several objectives. First, it outlined the two

significant problems that this study focuses on: a) terrorists continuously face

challenges to effectively and efficiently disseminate information and b) scholars face

challenges assessing Web site effectiveness because of the danger of physically

interacting with members and/or supporters of terrorist organizations. Second, it

reviewed the literature to articulate the relationship between terrorist organizations' Web

sites and perceived credibility. The literary review provided a snapshot of some of the

more widely-used definitions of terrorism to establish a foundational understanding of

what type of group this study examined. It also provided literary explanation on why

terrorism is considered by many as a means to communicate a message and how it

does so through mechanisms such as the media to maximize publicity of that message.

Next, it linked that objective to the increased use of the Internet as well as the

technological advancements of terrorist organizations. Additionally, it discussed the

difference between credibility and perceived credibility. Finally, it evaluated several

models to assess perceived credibility and presented the original model developed for

this study. In Chapter 3, the methodological approach used in this study is discussed.

CHAPTER 3

RESEARCH METHODS

Introduction

The literature review suggested that perceived credibility of a Web site is critical to its effectiveness. Accordingly, this study assumed that an objective of terrorist organizations' dissemination of information through their Web sites is to establish perceived credibility. The research question posited here was: *To what extent are there perceived credibility differences between terrorist organizations' Web sites?* An improved understanding of Web site effectiveness was achieved by identifying and illustrating the differences and similarities between terrorists' Web sites.

Research Design

To assess perceived credibility, this study was a comparative content analysis. Although inferences are not made from the textual content, the techniques used to valuate and assess the information presented on each Web site are similar. In other words, this study quantitatively assessed the textual content of each Web site and the method in which it was presented. It applied value to the method to which information was presented and the quantity and quality of information located on each Web site through the use of a coding frame. As a result, it gauged the probability a user may apply credibility to a particular Web site.

The study focused on three main areas: ambience, functionality, and information reliability. One objective was to articulate the differences of perceived credibility in Web sites between two types of terrorist organizations, religious nationalist and secular nationalist. An additional goal was to illustrate the differences in Web sites between the

two organizations of each group. Descriptive statistics A Future for the Young: Options for Helping Middle Eastern Youth Escape the Trap of Radicalization were used to illustrate similarities and dissimilarities in the findings.

Data Collection

Four terrorist organizations' Web sites were chosen for this investigation. The organizations were Hamas, Hezbollah, Popular Front for the Liberation of Palestine, and Tamil Tigers.

Hamas is a religious nationalist group based in the Gaza Strip. Founded in 1987, Hamas initially sought the destruction of Israel and the return of occupied territories to Palestinian inhabitants. In recent years, Hamas has ceased demanding the destruction of the Israeli state and instead, has accepted a two-state solution to the Palestinian-Israeli conflict. That is, the establishment of a Palestinian state, existing alongside Israel. Since its creation, Hamas has committed numerous terrorist actions toward Israel and its interests. Additionally, Hamas has provided social-welfare programs for Palestinian Arabs and has become a influential political force in Palestinian politics, currently holding a majority within the Palestinian parliament.

Hezbollah, or the Party of God, is based in southern Lebanon and is also a religious nationalist organization. It was formed in 1982, during the Israeli invasion of Lebanon. Accordingly, it is an active force within the Arab-Israeli conflict, calling for the destruction of the Israeli state. It has political, social, and military influence in Lebanon. The group holds seats in the Lebanese parliament, manages multiple social programs to improve conditions of its Shi'a constituents, and maintains a strong military presence

in Lebanon. Its military forces' primary aim is to thwart any and all aggressive action of Israel. Syria and Iran are the main financial supporters of the organization.

The Popular Front for the Liberation of Palestine (PFLP) also resists Israeli occupation of Palestinian lands. Established in 1967, the PFLP advocated the elimination of Israel. However, in the late 1990s, the organization accepted a two-state solution to the Palestinian-Israeli conflict. The group follows a Marxist-Leninist philosophy and thus can be defined as a secular nationalist organization. Unlike Hamas, the PFLP membership base is comprised of non-Muslims as well as many highly educated individuals.

The Liberation Tigers of Tamil Elam (LTTE or Tamil Tigers) is a secular nationalist terrorist organization located in the Sri Lankan territory of Tamil. Founded in 1976, its primary aim is for the Tamil region to secede from Sri Lanka to form an independent state. The Tamil Tigers are well known for their military tactics, particularly suicide bombings. Members are highly motivated and extremely loyal to the group to the extent that group members are known to wear a cyanide capsule around their neck, ultimately choosing death over capture. The organization also maintains a considerable fighting force with varying divisions, including the Sea Tigers and the Air Tigers. Similar to the other organizations mentioned here, the Tamil Tigers are deeply involved in local politics and provide social-welfare programs.

These organizations and their Web sites were chosen for several reasons. First, their objectives and means to reach those objectives are founded on different principles. Consequently, each organization was placed into one of two groups: religious nationalist or secular nationalist. The religious nationalist group emphasizes religion in

its strategy and ultimate objective as the establishment of a theocratic system of governance. In contrast, the secular nationalist organizations aim to establish an independent state where the political system would be based on more secular principles. Hamas and Hezbollah were categorized as religious nationalist and the PFLP and Tamil Tigers were categorized as secular nationalist. Due to the contrast, this study was able to identify and articulate variances in a common method utilized to reach organizational objectives.

Second, three of the organizations operate within the Arab-Israeli conflict. Thus, a comparison was made between two groups (Hamas and Hezbollah) founded on similar principles and between groups (Hamas/Hezbollah and PFLP) founded on dissimilar principles.

Finally, the four organizations chosen provided two groups (PFLP and Tamil Tigers) founded on similar principles, but operating in different contexts, as well as two groups (Hamas/Hezbollah and Tamil Tigers) founded on different principles and operating in two different contexts.

The Web sites chosen for this investigation were those of Hamas (2009), Hezbollah (2009), the PFLP (2009) and the Tamil Tigers (2009).

Data Analysis

This study recorded each terrorist organization's Web site on 10 separate dates. The homepage of each terrorist organization's Web site was recorded in MHTML format. This method provided a frozen image of the Web site for future analysis. The captured image was chiefly used to gauge ambience qualities.

The first and second levels of each Web site were recorded using Adobe Acrobat 8.0 Professional. It was determined early on through preliminary reviews of these Web sites that the first two levels were necessary and sufficient to provide an accurate assessment of perceived credibility primarily because the third level of a Web site generally consists of external Web site pages and not pages controlled by the organization under investigation.

The focus of the combined levels was *Functionality* and *Information Reliability*. It is suggested here that factors associated with *Ambience* lose their overall effectiveness as the information user progresses from the first to the second level. Accordingly, the PDF record of the second level was sufficient to identify incidents associated with *Functionality* and *Information Reliability*. The use of Adobe also provided a succinct list of errors related to images, font use, server connection, format, and links. A more in-depth review of the errors found is below. The operationalization of variables is discussed in the next section.

Ambience

This category evaluated overall style of the Web site or specific Web page under investigation. (See Appendix A for more information on the operationalization and coding rules of the variables in Ambience, Functionality, and Information Reliability.) Ambience was defined as cosmetic factors that interfere with an information user's interaction with a Web site.

Ambience factors have the greatest impact on one's perception of credibility during the first few seconds a user reviews a page (Everard & Galletta, 2005). After this

brief period, functionality and information reliability increase in importance while ambience decreases. Correspondingly, factors in this category were only assessed at the first level. Metrics considered for *Ambience* were similar to the Everard and Galletta (2005) model. They consisted of *Contrast, Consistent Font, Crooked Columns, Word Spacing*, and *Line Spacing*.

Contrast was assessed as either good or poor. The contrast of a page was poor if the contrast between background and text made it difficult to identify and read information quickly. An incident was defined as a section of information that presented poor contrast. *Contrast* was only evaluated at the first level.

Consistent Font was defined as inconsistencies in the font style and/or font size that made it difficult to determine headings from supportive text. *Consistent Font* was delineated by the quantity of incidents per level. An incident was defined as a section of information that presented poor font use. *Consistent Font* was only evaluated at the first level.

Crooked Columns was defined as inconsistencies in the column alignment of an individual section that made it difficult to identify and read information quickly. *Crooked Columns* was delineated by the quantity of incidents per level. An incident was defined as a section of information that presented crooked columns. This factor was only evaluated at the first level.

Word Spacing was defined as the white spacing between words. Consistency in white spacing throughout the section was examined, for example, single or double spaces between words. *Word Spacing* was delineated by the quantity of inconsistencies found. This factor was only evaluated at the first level.

Line Spacing was defined as the spacing between lines. Line spacing should be consistent throughout the section examined, for example, single or double spaced. *Line Spacing* was delineated by the quantity of inconsistencies found. This factor was only evaluated at the first level.

Functionality

The next category assessed was *Functionality*. This category evaluated the mechanical factors that interfere with an information user's interaction with a Web site. It is suggested here that factors related to *Functionality* receive their greatest influence during the second stage of perceiving credibility. That is, during the information user's transition from the first level to the second level of the Web site. Consequently, these factors were assessed at the first and second levels of the Web site.

Similar to the Everard and Galletta model, this study looked at factors related to "completeness" such as *"Under Construction" Pages*, *Obsolete Content,* and *Obsolete Links.* However, to assess media functions of a Web site, Everard and Galletta's variable, *Non-Loading Pictures,* was replaced by *Non-Loading Media*. This allowed for a more comprehensive assessment of the full range of media assets integrated onto Web sites by terrorist organizations. Furthermore, this factor was examined along with the variable *Uses of Multiple Media* (Video, RSS Feeds, Blogs, Mail Lists, etc.) to articulate the various types of media assets used, assorted combinations of media assets utilized, and for what purpose various media assets were employed.

Due to the advancements in Web design capabilities by terrorist organizations, one purpose of this study was to improve understanding of who integrates additional

means to disseminate information and/or receive support. Therefore, additional metrics were included for *Functionality.* Such an assessment goes beyond contemporary Web site analyses, thus providing a valuable contribution to the literature. The metrics used were *Onsite Searching, Multiple Languages, Donating Functions, Repeat Visitor Recognition, Multiple Site Offerings*, and *Offers 'How To' Guides*.

Under Construction Pages was defined as pages that displayed an "Under Construction" declaration. These types of pages did not include linked pages that did not upload or display a "File Not Found" statement. *Under Construction Pages* were delineated by the quantity of links examined on each page and by the quantity of incidents found from each level. This factor was evaluated at both the first and second levels.

Obsolete Content was defined as information on a page that was presented as recent, but was greater than thirty days old, was incomplete, or was absent. Purposely archived information was not considered as obsolete. *Obsolete Content* was delineated by the quantity of incidents per page or if the entire page was obsolete. This metric required qualification of the obsolete information by describing how old the information appeared to be and for what purpose it appeared to be used for on the page. This factor was evaluated at both the first and second levels.

Obsolete Links was defined as links that connected to a separate, system default page that displayed "File Not Found" or a similar statement. *Obsolete Links* was delineated by the quantity of incidents per level. This factor was evaluated at both the first and second levels.

Non-Loading Media was defined as pictures, RSS feeds, video, or other non-text

sources of information that did not load. *Non-Loading Media* was delineated by the quantity and type of incidents per level. This factor was evaluated at both the first and second levels.

Uses of Multiple Media was defined as video, RSS feeds, blogs, or mail lists used to support the Web site's objective of disseminating information. *Uses of Multiple Media* was delineated by the quantity and type of incidents per level. This factor was evaluated at both the first and second levels.

Onsite Searching was defined as a tool offered by the Web site's designer to search the organization's Web site for specific information. Search capabilities linked to external search engines were not considered. *Onsite Searching* was delineated by either the site having the capabilities or not. This factor was evaluated at both the first and second levels.

Multiple Languages was defined as the use of various languages for information dissemination. This metric considered uses on the entire Web site or pages/sections that were in more than one language. *Multiple Languages* was delineated by the total quantity of languages offered and by the type of languages offered. This factor was evaluated at both the first and second levels.

Donating Functions was defined as methods provided by the Web site designer for direct revenue generation. *Donating Functions* was delineated by determining if the site offered the user the ability to directly donate funds, if it provided information on how to directly donate funds, the quantity of methods employed by the Web site, and the types of methods used for direct fund raising. This factor was evaluated at both the first and second levels.

68

Repeat Visitor Recognition was defined as a Web site that recognized returning users. *Repeat Visitor Recognition* was delineated by determining if the Web site recognized repeat visitors. A determination was made by visiting the Web site multiple times. This factor was evaluated at both the first and second levels.

Multiple Site Offerings was defined as a Web site that offered links to other pages sponsored or designed by the same terrorist organization under review. These sites may be in the same language or not. For example, as is the case with multiple Islamist organizations, Web sites are designed in Arabic and English or French for greater exposure. Some sites were identical copies with translations instituted. Others were completely different due to the composition of the intended audience.

Multiple Site Offerings was delineated by the quantity of additional sites the organization offered and in what languages they were designed. This factor was evaluated at both the first and second levels.

Offers "How To" Guides was defined as instructional materials or "How To" guides that provided guidance and/or instruction on activities related to the organization's endeavors on a Web site. *Offers "How To" Guides* was delineated by the quantity of "How To" guides offered and the type/purpose of materials offered on the site. This factor was evaluated at both the first and second levels.

Information Reliability

The final category assessed was *Information Reliability*. This project looked at errors that impacted perceived credibility such as spelling, typographical, and grammatical errors. The average quantity of errors per level and the average quantity of

errors per page were determined. This approach was adequate due to the speed at which users scan Web pages and the related quantity of errors that need to be present in order for one error to be identified by the information user.

Number of Errors was defined as language errors such as spelling, typographical, or grammatical. Studies have shown that it generally takes twelve errors per page for the information user to identify one error. Thus, *Number of Errors* was delineated by the average quantity of incidents per page and whether 1 to 11 errors, or 12 or more errors per page were found. This variable was evaluated at the first and second levels of the Web site.

Spelling Errors, Typographical Errors, and *Grammatical Errors* are those identified in the English version of the information presented. These metrics were delineated by the quantity and type of incidents per level. Consideration was made for information that had been translated and for correlations between translated material and consistency in errors made. These types of errors were evaluated at the first and second levels of the Web site.

Terrorists constantly seek effective and efficient means to disseminate information. Increasingly they have turned to the Internet, designing their own Web sites for this purpose. Those who study terrorism are challenged with factors that many times prevent intimate contact with an organization's members and/or supporters. The model presented above will overcome these two problems. It will illustrate the potential effectiveness of a terrorist organization's Web site by assessing perceived credibility and it will provide researchers with a mechanism to assess potential effectiveness

without requiring physical contact between researcher and terrorist. The model will be applied to four terrorist organizations' Web sites in the following chapter.

Methodological Issues

Several issues related to assumptions, validity, and reliability of the data and findings were addressed in the study. The sections below discuss perceived credibility, a viable model, and intercoder reliability.

Perceived Credibility

This study adapted and employed metrics used in Everard and Galletta's (2005) model that evaluated Web site credibility along with additional metrics relevant to the context. It is important to note that the metrics employed in this study do not measure data collected directly from information users. In fact, they are indicators of perceptions of credibility derived from users in previous studies. Thus, this study assumed that certain factors affect the degree of credibility applied to a Web site. Furthermore, it assumed that by assessing those factors on Web sites, an accurate measurement can be made as to the level of perceived credibility a Web site might receive.

A Viable Model

In order to reach a model that was applicable and feasible to use, some variables were removed while others were added. First, the categories used in this study were *Ambience*, *Functionality*, and *Information Reliability*. These differ from Everard and Galletta's categories of *Style*, *Completeness*, and *Language Errors* respectively.

71

Second, Everard and Galletta's metric *Non-Loading Pictures* was changed to *Non-Loading Media* in order to incorporate all types of media employed on Web sites. Third, other metrics were included in order to more fully assess the functioning capabilities of the terrorist organizations' Web sites. These included *Onsite Searching, Multiple Languages, Donating Functions, Repeat Visitor Recognition, Multiple Site Offerings, Offers "How to" Guides,* and *Uses Multiple Media (Video, RSS Feeds, Blogs, Mail Lists).* Finally, to assess the reliability of the information presented, *Factual Errors* was removed while *More Than 12 Errors* and *>1 Error, but <12 Errors* were added. *Factual Errors* was simply not a feasible variable for this study as it requires physical contact be made with members or supporters of the group. *More Than 12 Errors* and *>1 Error, but <12 Errors* were added to more fully investigate the effects of the quantity of errors on a page. Descriptive statistics are used in the following chapter to illustrate similarities and differences that were found.

Intercoder Reliability

The immense quantity of information collected afforded clarity to the possibility of any differences in perceived credibility between organizations' Web sites, but it presented an enormous amount of data that needed to be appraised and coded by multiple coders. As a result, an intercoder reliability test was conducted. The intercoder reliability test essentially defines "the extent to which independent coders evaluate a characteristic of a message or artifact and reach the same conclusion" (Lombard et al., 2005). Three individuals, not including the researcher, were chosen for coding. Coding

samples used for preliminary tests were one record for each Web site, or 10 percent of the total records. The test included coding of all variables.

Each coder was instructed on the operationalization of the metrics used in this study and the related methods required to evaluate each page of each Web site. Preliminary tests were conducted to ensure intercoder reliability. For these tests, several individual records were chosen arbitrarily to conduct the preliminary test. After review of a test further training and adjustments were made until it was determined that 75 to 80 percent reliability had been reached. In other words, the data received intercoder agreement 75 to 80 percent of the time, depending upon the coder. According to Lombard et al. (2005), this was an acceptable rate and thus no adjustments were made to the coding scheme. Each coder analyzed approximately one-third of the overall data. (For a more detailed review of the coding scheme created for this study, see Appendix A.) The coders spent approximately 14 hours training on the coding scheme with the primary investigator to reach these levels. Disagreements over coding were generally resolved by adjusting the operationalization of the variable.

Summary

In this chapter, the basic methodological approach was outlined and discussed. Although not exactly a comparative content analysis, this study used similar techniques to valuate and assess information of four terrorist organizations' Web sites. The chapter also described the organizations and their Web sites. Four organizations' Web sites were studied. Two of these were religious nationalist groups and the other two were secular nationalist groups. Methodologically, the information was recorded using readily

available software and common techniques. A new model was also constructed by

taking a model used for evaluating perceived credibility of e-commerce Web sites and

adapting it to be more applicable to a terrorism context. Finally, this chapter addressed

potential concerns with the data and coding scheme by discussing the intercoder

reliability test conducted prior to analyzing the data. The next chapter presents the

findings of this investigation.

CHAPTER 4

RESULTS

Introduction

The research question for this study was: *To what extent are there perceived credibility differences between terrorist organizations' Web sites?* The previous chapters provided a broad review of the literature in both the information science and terrorism-related fields to articulate the importance of perceived credibility to Web site designers, particularly those in a terrorist organization. Additionally, problematic issues were discussed related to models used in the literature to assess perceived credibility in more contemporary Web site analyses. A new model was constructed to gauge perceived credibility in a unique context such as terrorism.

The first section of this chapter discusses the sample and unitization of the study. The second section provides a general overview of the findings. It focuses on the three primary areas of *Ambience, Functionality*, and *Information Reliability*. The third section presents the findings of each religious nationalist organizations' Web site and offers a discussion on the similarities between the two. It addresses the sub-question: *What are the perceived credibility differences between the Web sites of each religious nationalist terrorist organization?* Similarly, the fourth section reviews the findings related to the two secular nationalist organizations' Web sites and offers a discussion on the similarities between these two Web sites. It addresses the research sub-question: *What are the perceived credibility differences between the Web sites of each secular nationalist terrorist organization?*

Finally, the last section contrasts the findings between the two groups of Web

sites, addressing the research question: *What are the perceived credibility differences between the Web sites of the religious nationalist groups and the secular nationalist groups?*

Sample and Unitization

Although the model used in this study was not constructed to define information changes on Web sites over time, it did provide a valid assessment of each Web site's perceived credibility by accurately illustrating problematic areas outlined in the literature.

Each Web site was downloaded and saved ten separate times. Similarities between Web sites were assessed by evaluating each Web site's ten records to determine the average quantity of incidents over time. The average incidents of a particular Web site were then contrasted with the means of the other Web sites. As Table 8 shows, this equated to 40 homepages and 3960 pages at the second level (n=4000). In total, 136,160 links were examined (n=136,160). The sample sizes are discussed in greater depth below.

These amounts illustrate the vast quantity of information that potentially exists on four Web sites when assessing only two levels. To include a third or even fourth level for assessment might create a daunting task. Moreover, this study found that, generally, the third level and beyond were external pages to the Web site. Some links at the third level did send the information user elsewhere internally, deeper into the original Web site. However, a high percentage of the links transferred the information user to a Web site not directly associated with the original Web site. Thus, the quantity of links at one level did not correlate with the quantity of pages at the next level. As a result, it was

justifiable to assess only the first two levels of each terrorist organization's Web site.

Credibility Metrics

In this section, general findings of the study are discussed focusing on the three primary areas: *Ambience, Functionality*, and *Information Reliability*.

Ambience

Appearance, or ambience, is critical during the initial seconds of an information user's experience with a Web site (Everard & Galletta, 2005). Upon arriving at a Web site, the information user previews the homepage, or first level, and establishes a certain amount of perceived credibility. Although this occurs in only a few short seconds, it has a significant impact on determining the information user's next steps. However, as time goes on and the user travels through the pages of a Web site, ambience decreases in its influence on perceived credibility.

Figure 1 illustrates a breakdown of the factors affecting *Ambience.* (All values presented are means only.) Incidents recorded for *Ambience* increased the difficulty to find and/or review and/or interpret information. Each metric in Figure 1 is associated with a value that represents the percentage of incidents recorded for that specific metric.

The first level consisted of four pages. On this level the incident mean was 21. This equated to 5.25 incidents per homepage. Of these, *Consistent Font* received the highest value with 52% of all incidents being poor font use. In most cases, poor use of font size and/or style made it difficult to differentiate headings from supportive text.
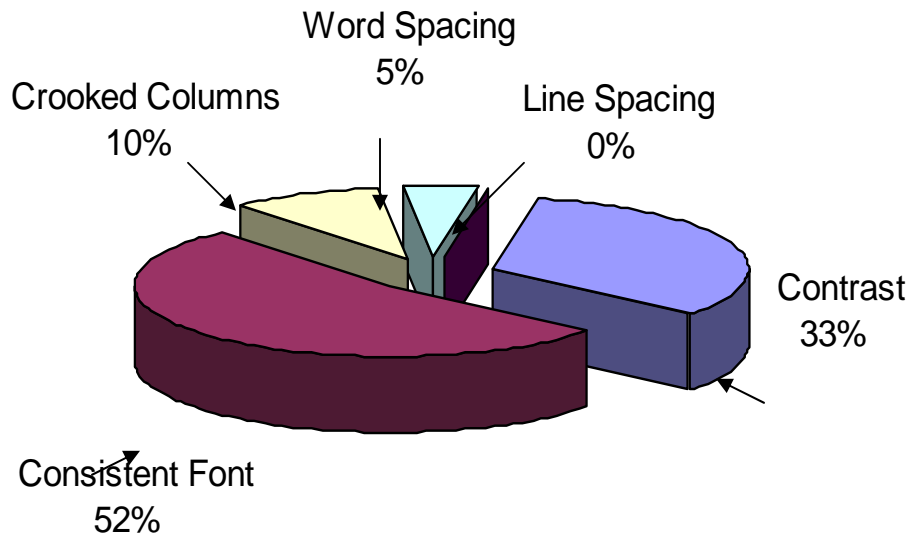
Figure 1: Metrics Related to Ambience

Contrast received the second highest value with 7 incidents, or 33%. These occurrences were largely related to various types of menus or banners. More specifically, background colors were similar to the font color, making the information difficult to identify and read. The remaining metrics received lesser values with *Crooked Columns* recording 2 incidents, or 10%, *Word Spacing* recording 1 incident, or 5%, and *Line Spacing* recording no incidents.

Overall, the ambience of the Web sites assessed was good as defined by this study. However, substantial differences were found between the Web sites of the two types of organizations and between the organizations in each group. An explanation of these differences is presented below.

Functionality

Table 8 illustrates the overall findings related to *Functionality*. At the first level, 4

pages with 423 links were found. On average, this equates to 105.75 links per page. At the second level, an average of 396 pages and 13,193 links were examined.

Accordingly, the quantity of links per page declines considerably to 33.32 links per page and only increases to 34.04 links per page when the levels are combined.

Interestingly, when several of the factors related to *Functionality* were assessed, evidence was discovered to support the theory that the homepage is most important to the sponsoring organization. First, the amount of information presented on the homepage was proportionately far greater than anywhere else in the Web site.

Table 8: Average Number of Incidents Related to Functionality

	1st Level	2nd Level	Total
Number of Pages	4	396	400
Number of Links	423	13193	13616
Number of Links Per Page	105.75	33.32	34.04
Obsolete Content	0	42	42
Obsolete Content Per Page	0	0.106	0.105
Obsolete Links	7	28	35
Obsolete Links Per Page	1.75	0.071	0.088
Percentage of Obsolete Links Per Level	1.655	0.212	0.257
Non-Loading Media	2	4	6
"Under Construction" Pages	0	0	0
Donating Functions (Direct)	0	0	0
Repeat Visitor Recognition	0	0	0
Offers "How To" Guides	0	0	0

This is a strong indicator that a designer understands the importance of the homepage, the small amount of time to gain the user's attention, and the resulting necessity to provide as much information as possible at this level. In fact, it was revealed that designers generally placed a substantial amount of information on the

homepage through various types of menus, extensive lists of archived articles, and links to photos, video, audio, or supporting pages, to name just a few. As a consequence, this study presupposes that the designer attempts to present enough information to the user to increase the likelihood that the user might be attracted to some aspect of the Web site and thus continue exploring its pages.

Table 8 also shows evidence that obsolete content was more likely to be on the second level rather than the first. Indeed, at the first level, obsolete content was not found to be presented as current information. All of the Web sites investigated for this study consistently placed dated information within an archive located on the homepage or elsewhere in the Web site. This finding further supports the argument that the homepage is critical to gain the attention of the user. Additionally, it demonstrates the intent of the organization to provide up-to-date information to its constituents.

Conversely, data in Table 8 seems to challenge the argument that a designer seeks to establish perceived credibility at subsequent levels. As the table illustrates, at the second level 42 incidents were identified, or .106 incidents per page, where obsolete content was presented as current information. The average value for *Obsolete Content* for both the first and second levels was only .105 incidents per page. This value indicates that the chances of the user coming across obsolete information are slim. Overall, these data further support arguments in the literature that designers attempt to produce an excellent product by keeping their Web sites current.

The data for *Obsolete Links* appear to reinforce the arguments posited here regarding the importance of *Functionality* and intent to establish perceived credibility. This metric also illustrates the decreased likelihood that an obsolete link will be

discovered as the user progresses through the Web site. Looking at Table 8, an average of 7 obsolete links, or 1.75 nonfunctioning links per homepage, was found at the first level. With 423 total links presented on average at the first level, only 1.655 percent were nonfunctioning. These values dropped significantly when moving to the second level. Here, the quantity of nonfunctioning links was 28 on average, with less than 1, or .071, nonfunctioning links per page. With 13,193 links presented in total at the second level, only .212 percent was determined to be nonfunctioning. Overall, as Table 8 shows, 35 nonfunctioning links on average, or .088 bad links per page were found. This equates to .257 percent of the links on the first and second levels as nonfunctioning.

Many of the remaining factors presented in Table 8 also support the intent of Web site designers for terrorist organizations to establish and maintain a high level of perceived credibility. Of the 400 pages examined on average, only 6 incidents were identified where media did not load. Two incidents were identified on the first level and only 4 on the second level. Importantly, only media that did not load were counted. Media that loaded, but required an extensive amount of time were not counted as *Non-Loading Media*.

Interestingly, no incidents of *"Under Construction" Pages* were found. Some pages were presented as having information, but when assessed, provided the declaration "No Records Found." Consequently, because of their incompleteness and manner in which they were presented, these pages were recorded as obsolete content and not pages under construction.

A few other interesting discoveries were also made. First, no incidents were

identified for *Donating Functions (Direct).* Although some terrorist organizations offered

online stores where multiple items may be purchased such as t-shirts, photographs,

miscellaneous downloads for personal computers, and a sophisticated role-playing

video game, none were found to present information related to direct monetary support

of the organization.

Second, it was assumed for this study that *Repeat Visitor Recognition* would be

an appropriate metric for the Web sites under review. However, no incidents were

identified for this metric. It is possible that it is simply not necessary in that it provides no

tangible benefit to the organization or that it is done in confidence, without the user's

knowledge.

Third, this study concluded that *Offers 'How To Guides'* was an impractical metric

for such a study as the one conducted here. It is likely that the organizations assessed

here might be considered as legitimately positioned in their relative communities by

supplying members for government positions or providing social services for their

constituents. Thus, the organizations hold a sense of legitimacy within the population

that helps sustain their position and ensure their survival. Consequently, they are able

to maintain a presence on the Internet, but cannot afford to present too extreme a

stance or present their activities in such a way that might threaten their current status.

Accordingly, an organization might tend to focus on the narrative that it functions within

and proliferates, and steer away from the distribution of instructional material via the

Web, at least where it can be easily found by the average information seeker.

Additional factors were also used to assess *Functionality*. These were *Different

Languages Offered, Number of Sites Offered*, and *Onsite Searching Links.* Figure 2

illustrates some of the more interesting findings related to these metrics. Concerning the quantity and types of languages offered by the Web sites, all sites provided either a link to an alternate site which was in a different language or provided sections of their Web site in different languages. Many, however, did both.

In fact, 8 different languages were used: English, Arabic, Farsi, Tamil, French, Hebrew, Spanish, and Italian. All of these languages were offered on the first level and 6 of them offered on the second level. The presumption is that the use of multiple languages to disseminate information increases the recipient base for that information.

The four Web sites investigated also offered numerous alternate sites. As Figure 2 illustrates, on the first level, 12 alternate sites were offered. On the second level, 7 alternate sites were offered. As stated in Chapter 2, multiple sites are advantageous to terrorist organizations for a variety of reasons.
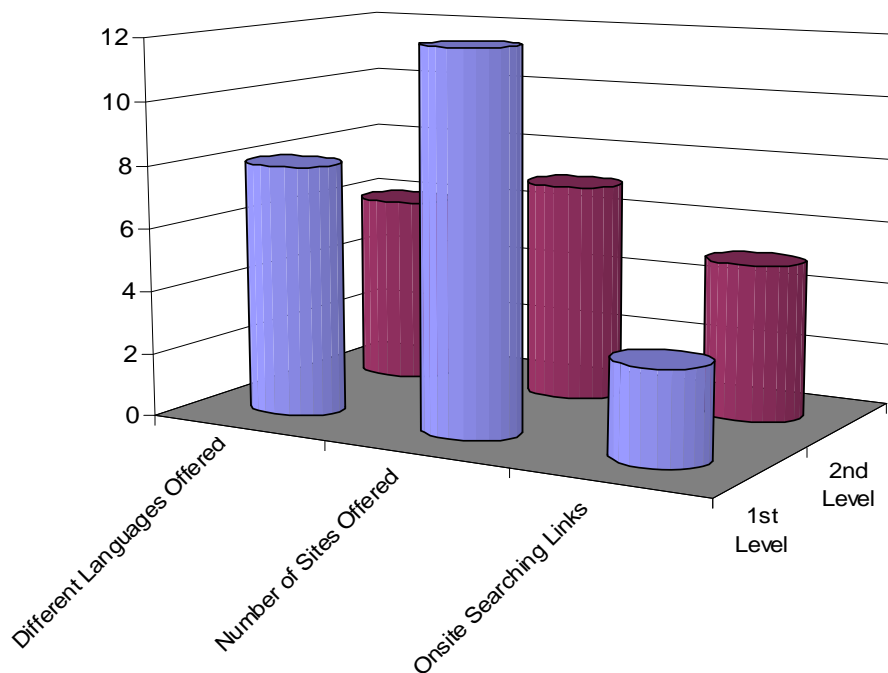
Figure 2: Additional Factors Related to Functionality

Furthermore, some of the Web sites reviewed in this study had links to alternate sites that were almost identical to the original, except for the application of a different language. Others were far from mirrored images of the original. These additional sites will be discussed below at greater length.

Information Reliability

This study assumed that *Information Reliability* increased in significance and influence, as the information user moves deeper into a Web site. In addition, the literature suggested that it takes at least 12 errors on a single page for an information user to identify one. Accordingly, this study employed several metrics to illustrate the occurrence of errors, thereby gauging perceived credibility of the user. The metrics used in this category were *Spelling Errors, Typographical Errors*, and *Grammatical Errors*. The general findings are presented in this section.

Table 9: Factors Related to Information Reliability

	1st Level	2nd Level	Total
Number of Pages	4	396	400
Number of Errors	149	900	1049
Mean of Errors/Page	37.25	2.28	2.62
Spelling Errors	6	50	56
Typographical Errors	57	15	72
Grammatical Errors	86	835	921

Table 9 reiterates the quantity of pages at each level and for both levels combined. The table also illustrates the quantity of errors for each level and the average errors per page. Finally, it provides the quantity of each type of error per level.

As Table 9 shows, an average of 149 errors were recorded on the first level and 900 errors recorded at the second level. At the first level, this equates to 37.25 errors per page. This value implies that it is quite possible that an information user may be able to identify numerous errors on the Web sites' homepages and adjust perceived credibility accordingly. However, the high quantity of errors came mainly from one Web site.

At the second level, the average amount of errors per page was 2.28. For the entire 400 pages reviewed, on average 1049 errors were recorded. Combining both levels resulted in an average of 2.62 errors per page.
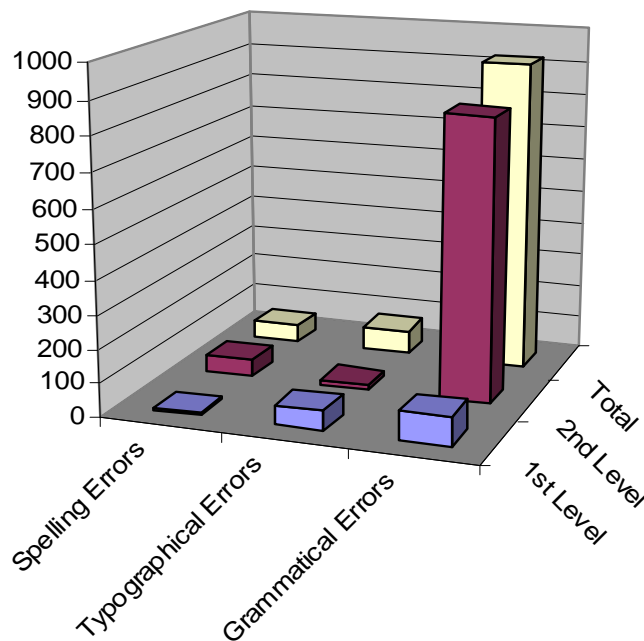
Figure 3: Breakdown of Errors Per Level

The distribution of errors per level is shown from different perspectives in Figures 3 and 4. These charts also correlate with the lower half of Table 9. Both figures illustrate a huge disparity between types of errors. Referencing Table 9, one can see

that at the first level 6 incidents of *Spelling Errors*, 57 incidents of *Typographical Errors*, and 86 incidents of *Grammatical Errors* were found. At the second level 50 spelling, 15 typographical, and 835 grammatical errors were recorded on average. Combining both levels resulted in 56 spelling, 72 typographical and 921 grammatical errors. On the surface, these data seem to imply that the second level is consistently receiving little attention concerning grammar. However, a few important issues need to be addressed.

Spelling Errors,
56, 5%

Typographical
Errors, 72, 7%

Grammatical
Errors, 921, 88%
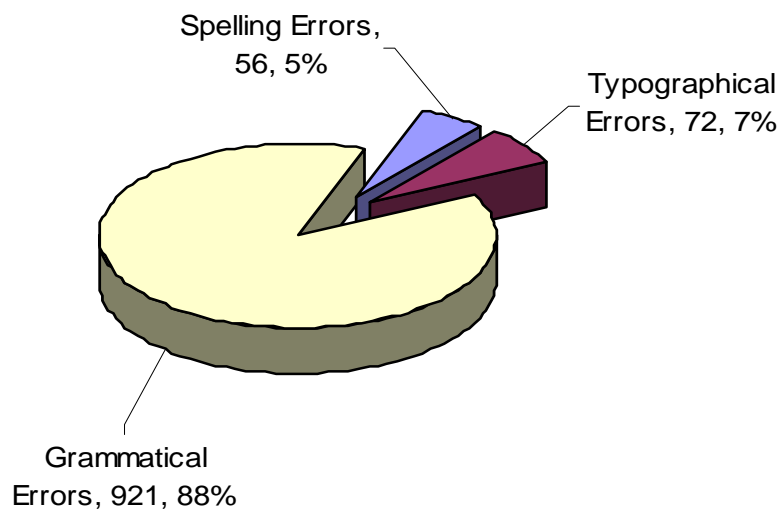
Figure 4: Number and Percent of Errors

First, one site had a significant number of errors while two others shared moderate levels. The remaining site had a low quantity of errors. Second, because of the massive amount of information translated from one language to another, grammatical errors might intuitively occur. That is, a person employed to translate information from one language to another may only have a certain level of proficiency in that language. Consequently, when the information is translated, it is likely that the

number of grammatical errors may be proportionate to the proficiency level of the translator.

Common software applications are less than helpful to correct these errors. However, spelling errors can be fixed. Indeed, much of the information on the four Web sites had few spelling errors. This is likely due to the use of a spell checker or other tool utilized by the Web site designer. The findings related to the individual groups (discussed below) appear to concur.

In conclusion, the general findings discussed here demonstrate the complexity and various other issues related to such an innovative study, support for many of the arguments presented in the literature, and several areas that require more in-depth probing. Accordingly, the findings related to each individual Web site are discussed in the next section.

Religious Nationalist Web Sites

This section illustrates to what extent differences, or possibly even similarities, existed between the religious nationalist Web sites investigated for this study. That is, this section addresses the research sub-question: *What are the perceived credibility differences between the Web sites of each religious nationalist terrorist organization?*

First, findings for the religious nationalist groups, Hamas and Hezbollah, are presented. Second, findings for the secular nationalist groups, the Tamil Tigers and the Popular Front for the Liberation of Palestine (PFLP) are discussed. Each area affecting perceived credibility is addressed starting with *Ambience.*

Hamas

The Web site sponsored by Hamas was located at www.sabiroon.org (Hamas, 2009) and provided a great deal of information. Overall, it had a professional appearance and appeared to be updated relatively often. However, a few issues were discovered pertaining to perceived credibility.

First, as Table 10 shows, Hamas' Web site had 87 pages on average for the first and second levels combined. Generally, the first level had contrast between the background and text. This made it easy to identify and retrieve information. In addition, it only averaged 1 incident associated with each metric for font use, column placement, and word spacing. It also, had good line spacing.

It is important here to elaborate on the repetition found in many Web sites. As the data show with each Web site, several metrics received a 0 or 1 value, indicating no incidents or only a single incident being identified. This is due to little change of the predominant sections of each Web page over time. As important, most Web sites also neglected to fix errors over time, so the mean value related to a specific metric varies little.

Table 10: Ambience Factors Related to Hamas' Web Site

Category	Incidents Recorded
Average Pages	87
Contrast	Good
Consistent Font	1
Crooked Columns	1
Word Spacing	1
Line Spacing	0

Data for *Functionality* in Table 11 show that no Web site presented pages under construction (an indicator of incompleteness). However, some sites did present the user pages with incomplete information. In the case of Hamas' Web site, it had numerous pages that displayed the declaration "No Records Found." In fact, Hamas had the greatest quantity of pages with obsolete content, with 41 identified incidents. This equates to 47 percent of its pages with obsolete or incomplete information. All of these pages were at the second level. Additionally, it had three obsolete links, all on the second level. This value is quite low considering that the overall quantity of links on the second level was 1715.

Table 11: Functionality Factors Related to Hamas' Web Site

		Level 1	Level 2
Links Per Level		56	1715
"Under Construction" Pages	(Incidents Recorded)	0	0
Obsolete Content	(Incidents Recorded)	0	41
Obsolete Links	(Incidents Recorded)	0	3
Non-Loading Media	(Incidents Recorded)	1	2
Onsite Searching		1	1
Donating Functions		None	None
Repeat Visitor Recognition		No	No
Offers "How To" Guides		No	No
Multiple Sites Offerings		1 (Arabic)	1 (Arabic)

Hamas' Web site only had 3 non-loading media, but it did offer onsite searching capabilities with one link on each of the levels. The search engine functioned in both English and Arabic. Concerning direct donating functions, Hamas' Web site offered none. It also offered no instructional material and did not recognize repeat visitors. It did however offer an alternate site in Arabic. Hamas also designed and presently operates

a Web site specifically for the youth. This alternate sight mostly focuses on proliferation of the narrative which the organization operates under and is intended for children at the primary level of education. However, it was not found to be linked to www.sabiroon.org.

Hamas' Web site did offer several types of multiple media such as a mailing list to subscribe to its newsletter and RSS feeds that were also linked to an Arabic version of facebook. Video was also offered, but this media was presented on one of the many pages declaring that no records existed. Finally, information was presented in different languages including Arabic and English.

Table 12: Information Reliability Factors Related to Hamas' Web Site

	Level 1	Level 2
Number of Errors	109	510
(Avg. Per Page)	>12	>12 (17)
Spelling Errors	5	27
Typographical Errors	43	2
Grammatical Errors	61	481

Information Reliability is the final category. As Table 12 demonstrates, Hamas' Web site received high incident scores on grammatical and typographical errors, indicating a potential for low perceived credibility. At the first level, 109 errors were found including 5 spelling, 43 typographical, and 61 grammatical errors. This is above the threshold of 12 errors for one page and suggests that the perceived credibility of an information user may be considerably low.

On the second level, 510 errors were found including 27 spelling, 2 typographical, and 481 grammatical errors. The average quantity of errors for all 86 pages at the second level was 17 per page. Importantly, not all pages had more than 12

90

errors. However, a high percentage did and moreover, many pages that had less than

12 errors had little information presented. Although those pages did not surpass the

threshold outlined in the literature, an information user might feasibly identify one error

with less than 12 errors present on a single page. Consequently, this study identified a

weakness in the literature concerning the threshold of errors necessary for one to be

identified. Thus, further research to clarify the relationship between the quantity of errors

and the amount of information on a single page is needed.

Hezbollah

The Web site sponsored by Hezbollah, was located at www.moqavemat.com

(Hezbollah, 2009). This Web site shared some similarities with Hamas' Web site, but

with 167 pages offered on average, it surpassed the amount of information offered by

Hamas.

Table 13: Ambience Factors Related to Hezbollah's Web Site

Category	Incidents Recorded
Average Pages	167
Contrast	Good
	5 (Article Dates)
Consistent Font	5 (Section Headings)
Crooked Columns	0
Word Spacing	0
Line Spacing	0

Similar to Hamas' Web site, Hezbollah's Web site had good contrast overall

between its background and text at the first level. However, 5 incidents were identified related to the poor contrast of dates used to differentiate articles. Five incidents were also identified where font use was poor. These were all related to section headings. However, no incidents were found related to columns, word spacing or line spacing.

Table 14 shows the data collected on *Functionality*. At the first level, 213 links were identified with none leading to pages under construction or having content that was obsolete. In fact, over time, it became clear that this Web site was updated every 24 hours with major revisions sometimes being instituted. This was evident in that the Web site repeatedly offered news stories or articles from that same day.

Table 14: Functionality Factors Related to Hezbollah's Web Site

		Level 1	Level 2
Links Per Level		213	3483
"Under Construction" Pages	(Incidents Recorded)	0	0
Obsolete Content	(Incidents Recorded)	0	0
Obsolete Links	(Incidents Recorded)	2	2
Non-Loading Media	(Incidents Recorded)	1	1
Onsite Searching		Yes	Yes
Donating Functions		None	None
Repeat Visitor Recognition		No	No
Offers "How To" Guides		No	No
Multiple Sites Offerings		5	5*

Two links were identified as obsolete, meaning that they failed to load. This was interesting because of the seemingly meticulous attention this Web site appeared to receive. However, it is likely that these two links failed to upload due to issues unrelated to the Web site. Nevertheless, this amount seemed acceptable when the total quantity of links offered was considered, particularly at the second level.

Hezbollah's Web site also offered an advanced search engine that might lead the information user to numerous locations both within the Web site and without. Additionally, the first level did not have a direct method to donate monies, did not offer instructional material, and did not recognize repeat visitors. However, on the latter, it did use a counter to quantify the amount of hits it received. Therefore, it is likely that IP addresses and other supplemental data related to the visitor were collected for various internal purposes.

Hezbollah's Web site also offered links to 5 alternate sites that it sponsors and provided a vast amount of information in several different languages including Hebrew, Arabic, English, Farsi, and French. The site also used several various media, including RSS feeds, "contact us" links, video, and audio. Hezbollah's Web site was the only site to respond to email inquiries for more information about the organization from its "contact us" link. At first it appeared as if the tool was malfunctioning, repeatedly stating that the information submitted was incomplete. However, within 24 hours, an email was received from the organization offering assistance.

Interestingly, Hezbollah designed a video game which it sells through its Web sites. In the game, the player takes on the role of a Hezbollah soldier and participates in battles with Israeli soldiers and citizens. High demand for the video game led to a second version which became available in recent months. The latest version positions a player in battles that occurred during the war with Israel in 2007.

For Hezbollah's Web site, *Information Reliability* had somewhat mixed results. On level one, a total of 28 errors were found including 14 typographical and 14 grammatical errors. No spelling errors were found. The average quantity of errors for

the homepage was above the threshold of 12. However, it is not likely to have a

significant impact on perceived credibility due to greater importance given to ambience

at this level. Furthermore, assuming the user will only identify one error for every 12

errors, only 2 errors should be found by the average visitor.

Table 15 also illustrates the findings for Hezbollah's Web site at level two. On this

level, 148 errors were found. The average quantity of errors per page was 87. No page

was identified with more than 12 errors. Concerning the breakdown of the individual

errors, no spelling errors were found and the common disparity between typographical

and grammatical errors was seen with 5 and 143 respectively.

Table 15: Information Reliability Factors Related to Hezbollah's Web Site

	Level 1	Level 2
Number of Errors	28	148
(Avg. Per Page)	>12	<12 (.87)
Spelling Errors	0	0
Typographical Errors	14	5
Grammatical Errors	14	143

Religious Nationalist Web Sites and Perceived Credibility

The main objectives of this study were twofold. First, identify and then illustrate

the extent to which there are perceived credibility differences between the Web sites of

each religious nationalist terrorist organization and each secular nationalist terrorist

organization. Second, identify and then illustrate perceived credibility differences

between the Web sites of the religious nationalist groups and the secular nationalist

groups. This section addresses the first research question posited by this study: *What*

are the perceived credibility differences between the Web sites of each religious nationalist terrorist organization? To this end, it discusses the differences and similarities between the Hamas Web site, www.sabiroon.org, and the Hezbollah Web site, www.moqavemat.com.

First, Tables 10 and 13 show that both Web sites were assessed with "good" contrast between the background and text. However, Hezbollah's Web site had several headings and dates that might have been improved by increasing contrast. Nevertheless, Hezbollah's Web site had no incidents concerning columns, word spacing, or line spacing. Conversely, Hamas' Web site had a few incidents recorded for these metrics, but they were minimal. As a result, both were quite similar in *Ambience* overall.

In terms of *Functionality*, several significant differences were recorded. First, Tables 11 and 14 illustrate that although both Web sites presented a vast amount of information on their respective homepages, Hezbollah's Web site offered nearly twice as many pages (167) as Hamas' Web site did (87). While this allowed Hezbollah's Web site the capacity to offer more information, perhaps more importantly, it provided the information user more options. In other words, Hezbollah's Web site offered 20.86 links per page and Hamas' Web site offered 19.7 links per page. At first glance, a significant difference between these two values is not evident. However, the considerable disparity in total links offered illustrates the presumed attempt by the designer to give an information seeker a substantial amount of choices in their search for information.

Furthermore, Hezbollah's Web site had no obsolete content identified and offered information in several languages via internal pages and alternate sites. Conversely,

Hamas' Web site had 41 *Obsolete Content* incidents recorded and offered information only in English and Arabic. Both sites were similar to one another regarding the remaining metrics. Accordingly, Hezbollah's Web site, www.moqavemat.com, exceeded Hamas' Web site, www.sabiroon.org, in *Functionality*.

Finally, reexamining Tables 12 and 15, further dissimilarities are evident. Importantly, Hamas' Web site had approximately 3.5 times as many errors as did Hezbollah's Web site, with 510 and 148 respectively. As the two tables illustrate, sabirron.org scored more poorly on all three metrics. Consequently, although some similarities in *Ambience* and *Functionality* were found, numerous noteworthy differences were identified. Overall, Hezbollah's Web site is more likely to receive higher levels of perceived credibility from the average information user.

Secular Nationalist Web Sites

This section illustrates to what extent differences, or possibly even similarities, exist between the secular nationalist Web sites investigated for this study. That is, this section addresses the research sub-question: *What are the perceived credibility differences between the Web sites of each secular nationalist terrorist organization?*

Tamil Tigers (LTTE)

The Web site sponsored by the Tamil Tigers was located at <u>www.eelamweb.com</u> (Tamil Tigers, 2009). This site offered the least amount of pages, with only 36 on average, and the least amount of information. Overall, it had a good appearance, but appeared less professional in its design. Moreover, no indication existed that it received

frequent updates and it presented some outdated and incomplete information. However, it did have some positive attributes.

First, as Table 16 shows, the Tamil Tigers' Web site generally had good contrast between the background and text which made it easy to identify and retrieve information on the first level. It did have 2 incidents recorded on average where contrast might be improved. These two areas, the top and lower banners of the homepage, were also repeated on numerous other pages. Although information was not too difficult to identify and assess, these areas did require greater attention relative to other Web sites. The top banner also had inconsistent font use. The Tamil Tigers' Web site did receive good marks related to column structure, word spacing, and line spacing.

Table 16: Ambience Factors Related to Tamil Tigers' Web Site

Category	Incidents Recorded
Average Pages	36
Contrast	Good 2
Consistent Font	1 (Top Banner)
Crooked Columns	0
Word Spacing	0
Line Spacing	0

In Table 17, the metrics illustrating *Functionality* are presented. At the first level, the Tamil Tigers' Web site had 44 links including 5 obsolete or non-functioning links. These were the links that led to "Broken Promises," "TRO," "Write To Us," "Press Release," and "Contact." However, at the first level, it presented no obsolete content

97

and all of the media loaded properly. In addition, the first level had no onsite searching

capabilities, direct donating functions, repeat visitor recognition, or instructional material.

This level offered an online store where items such as screensavers, postcards, songs,

books, and maps may be purchased. This investigation could not ascertain the ultimate

destination of the generated revenue from the online store.

Interestingly, this organization offered 5 different associated Web sites with

information presented in English and Tamil. These Web sites were a mixture of officially

and unofficially sponsored Web sites. It also offered multiple media such as archived

radio broadcasts, audio messages, mailing lists, numerous photographs, and

downloadable wallpapers of martyrs. Additionally, attempts were made to contact the

site via email, but no reply was received.

On level two, 868 links were identified, with 6 obsolete. Each of these links led to

a page declaring "File Not Found." No pages were recorded as "Under Construction,"

but this level did offer onsite searching capabilities.

Table 17: Functionality Factors Related to Tamil Tigers' Web Site

		Level 1	Level 2
Links Per Level		44	868
"Under Construction" Pages	(Incidents Recorded)	0	0
Obsolete Content	(Incidents Recorded)	0	7
Obsolete Links	(Incidents Recorded)	5	6
Non-Loading Media	(Incidents Recorded)	0	0
Onsite Searching		No	Yes
Donating Functions		None	None
Repeat Visitor Recognition		No	No
Offers "How To" Guides		No	No
Multiple Sites Offerings		5	0

Although much of the Tamil Tigers' Web site was informative, with several links

to additional sites offering up-to-date information on their struggle, several pages within

the Tamil Tigers' Web site did however, present obsolete content. For example, an

"Urgent Press Release" declaration was on a page that was actually from 2004, the

"Women's Day Messages" were from the early to mid-1990s, the "Military Campaigns"

information was from 1986 and 1998, "Interviews" were from the 1980s and 1990s,

"Unceasing Waves" presented information from the 1990s and early 2000s, the

statistics provided on those who have died for the cause were from 1982 to 2005, and

"Women Fighters' History" spoke of current information that was actually significantly

aged.

The values for *Information Reliability* are shown in Table 18. On level one, a total

of 8 errors were found, including 7 grammatical errors. Interestingly, no spelling or

typographical errors were found. Thus, the average quantity of errors for the homepage

was below the threshold of 12.

Table 18: Information Reliability Factors Related to Tamil Tigers' Web Site

	Level 1	Level 2
Number of Errors	8	224
(Avg. Per Page)	<12	<12 (6.4)
Spelling Errors	0	23
Typographical Errors	0	3
Grammatical Errors	7	198

Table 18 also illustrates the *Information Reliability* findings for Hezbollah's Web

site at level two. On this level, 224 errors were found. The average quantity of errors per

page was 6.4. However, multiple pages were identified where more than 12 errors were

found. As with Hamas' Web site, several pages were indentified with little information presented and with several, but less than 12, errors. Consequently, errors on these pages are likely to be discovered by the average user and, as a consequence, have a negative impact on perceived credibility. Concerning the breakdown of the individual errors, 23 spelling errors were found, 3 typographical and 198 grammatical errors.

Popular Front for the Liberation of Palestine (PFLP)

The Web site sponsored by the PFLP was located at www.pflp.ps/english/ (PFLP, 2009). This site offered a large amount of information within its 110 total pages. *Ambience* factors related to PFLP's Web site are illustrated in Table 19. This Web site's overall appearance was good and appeared professional in its general design. *Consistent Font* did record 5 incidents. This was due to 4 links' headings and 1 banner that had inconsistent font size. Additionally, one incident of *Crooked Columns* was found, but no incidents related to word or line spacing were identified.

Table 19: Ambience Factors Related to PFLP's Web Site

Category	Incidents Recorded
Average Pages	110
Contrast	Good 0
Consistent Font	5
Crooked Columns	1
Word Spacing	0
Line Spacing	0

Table 20 exhibits the values associated with *Functionality.* On the first level, 110 links were identified with none being obsolete. Moreover, no incidents were recorded for *"Under Construction" Pages, Non-Loading Media,* or *Obsolete Content.* Also, no online searching capabilities or direct donating functions were found at this level. However, numerous links were found that offered the information user the means to donate to various charities.

Table 20: Functionality Factors Related to PFLP's Web Site

		Level 1	Level 2
Links Per Level		110	7127
"Under Construction" Pages	(Incidents Recorded)	0	0
Obsolete Content	(Incidents Recorded)	0	0
Obsolete Links	(Incidents Recorded)	0	17
Non-Loading Media	(Incidents Recorded)	0	1
Onsite Searching		No	Yes
Donating Functions		None	None
Repeat Visitor Recognition		No	No
Offers "How To" Guides		No	No
Multiple Sites Offerings		1	1

PFLP's site did offer a link to an alternate site in Arabic which was similar. In addition, several other links were identified that led to sites where information was presented in a variety of languages including French, Spanish, Italian, and Hebrew. This site was found to limit its use of multiple media. It did however, offer an RSS feed at this level. Finally, at the first level, PFLP's Web site did not offer instructional material and did not seem to recognize repeat visitors.

The second level had similar results to the first. Interestingly, it received relatively good marks at this level even with 7127 links. Indeed, the metrics *"Under Construction"*

Pages and *Obsolete Content* recorded no incidents. However, 17 obsolete links and one non-loading media were found. Nevertheless, it is likely that these may have little effect on perceived credibility. In addition, at this level the site did offer onsite searching capabilities, but no direct donating functions, repeat visitor recognition, or instructional material.

Although at first glance it appeared that this site offered a tremendous amount of information due to its 7127 links, a high percentage of these links were repetitive. That is, 110 links were found on the first level in the form of various types of menus. A vast majority of these menus, and thus links, were repeated on nearly all of the pages at the second level. Furthermore, most of these links redirected the user to an external site, therefore they did not redirect the user to another page internally that offered information controlled by the Web site designer. Those links that did were often recurring, taking the user to the same set of pages within the original Web site. Accordingly, on the surface it appeared as if this Web site was extremely expansive, providing a massive amount of information. Indeed, a significant amount of information was offered, but when solely assessing the amount of links, the overall amount of information that might be reviewed may be misleading to the average information user.

Table 21 illustrates *Information Reliability*. On level one, PFLP's Web site had a total of 4 grammatical errors. No spelling or typographical errors were found. At the second level, this Web site also exhibited low values with only 18 total errors, 5 typographical and 13 grammatical.

The findings illustrated in Table 21 are interesting. The data show that this Web site was the only one that did not have a significant amount of grammatical errors. It is

likely that this is a result of the point addressed above. That is, much of the homepage, particularly the menus and links, was duplicated on subsequent pages. Importantly, the information that was duplicated was more or less error free. As a result, few errors existed on the pages of the second level. This is dissimilar to the previous Web sites discussed where the process of duplicating information and placing it on supplemental pages also transferred the errors within that information.

Table 21: Information Reliability Factors Related to PFLP's Web Site

	Level 1	Level 2
Number of Errors	4	18
(Avg. Per Page)	<12	<12
Spelling Errors	0	0
Typographical Errors	0	5
Grammatical Errors	4	13

Secular Nationalist Web Sites and Perceived Credibility

This section addresses the second research question posited by this study: *What are the perceived credibility differences between the Web sites of each secular nationalist terrorist organization?* Similar to the comparison between the two religious nationalist Web sites, this section looks at the differences and similarities in perceived credibility factors between the Tamil Tiger's Web site, www.eelamweb.com, and the PFLP Web site, www.pflp.ps/english/.com.

First, as Tables 16 and 19 show, both Web sites were assessed with "good" contrast between the background and text. Importantly, the Tamil Tigers' Web site had an average of 36 pages with two *Contrast* incidents recorded compared to 110 pages

and no *Contrast* incidents on PFLP's Web site. Beyond PFLP's Web site exhibiting a few more incidents related to font use, the *Ambience* of these two sites was comparable and therefore perceived credibility may be similar.

Secondly, reexamining *Functionality* in Tables 17 and 20, PFLP's Web site offered a substantially greater amount of links to the user, but the overall quantity of information offered may be misleading. In fact, a disparity did exist between the two Web sites, but it was not as great as the quantity of links conveyed. Nevertheless, PFLP's Web site is likely to rate much higher in *Functionality* because it provided more information and because Tamil Tigers' Web site appearance was more amateurish with a greater amount of obsolete information.

Finally, looking at Tables 18 and 21 illustrates a significant difference between these two Web sites. That is, the quantity of errors found on Tamil Tigers' Web site was far greater than on PFLP's Web site. Consequently, the PFLP's Web site may be more likely to receive higher ratings in *Information Reliability* from an average user. Finally, because the Tamil Tiger's Web site generally received far worse scores than PFLP's Web site, it is likely that PFLP's Web site might have higher perceived credibility than the Tamil Tigers' Web site.

Religious and Secular Nationalist Web Sites

This section assesses the four Web sites in their respective category, religious nationalist and secular nationalist, to illustrate similarities or dissimilarities. Accordingly, this section addresses the third research question posited by this study: *What are the perceived credibility differences between the Web sites of the religious nationalist*

groups and the secular nationalist groups? All three areas are discussed beginning with *Ambience*.

First, Table 22 shows the distribution of the average amount of Web pages (when counting only the first two levels of the Web site) per Web site for each group. For the two religious nationalist organizations, Hamas had the fewest with 86 average pages. Hezbollah had nearly double that amount with 167 pages on average. Their combined average was 127 pages.

Table 22: Ambience Scores for Religious and Secular Nationalist Web Sites

Category	Incidents Recorded			
	Hamas	Hezbollah	Tamil Tigers	PFLP
Average Pages	87	167	36	110
Contrast	Good	Good	Good	Good
	0	5	2	0
Consistent Font	1	5	1	5
Crooked Columns	1	0	0	1
Word Spacing	1	0	0	0
Line Spacing	0	0	0	0

When compared to the secular nationalist organizations, Hezbollah remained the organization with the highest quantity of pages. In the Secular group, the Tamil Tigers had an average of 36 pages, while the PFLP had 110. The combined average of pages for this group was 73.

Undoubtedly, Hezbollah surpassed all other groups in quantity of pages on the first two levels. This supports arguments in the literature that terrorist organizations are

increasingly using the Internet to disseminate a large amount of information in a variety

of categories. Moreover, the religious nationalist group offered a greater amount of

pages when contrasting group averages. However, does a higher amount of Web pages

translate into greater quantities of information? Furthermore, might a greater quantity of

pages correlate with increases in perceived credibility? On one hand, the more pages a

Web site offered, the more information offered. Thus, the higher the perceived credibility

may be. On the other hand, the greater amount of pages within a Web site, the greater

the potential for errors to exist or for functionality to be inhibited. Therefore, by creating

more pages, the designer runs the risk of negatively affecting perceived credibility. This

was evident in the individual assessments. Undoubtedly, further research is needed to

address these issues.

Contrast was recorded as good for all Web sites, with Hezbollah's site receiving

the worst incident rating. When comparing the two groups, the secular nationalist group

fares slightly better. This is also true when assessing the remaining metrics for

Ambience. However, significant differences in ambience between these Web sites were

not accounted for by the metrics utilized by this study. Therefore, this category needs

additional metrics to more accurately assess the overall ambience of a Web site.

Table 23 illustrates the values for *Functionality*. Many similarities between the

two groups were found, as well as some interesting differences. First, neither group was

found to have *"Under Construction" Pages*. This finding implies that designers are

attentive to the effects that incomplete pages have. Such an implication seems even

more plausible when considering the numerous pages included in each Web site.

Table 23: Functionality Scores for Religious and Secular Nationalist Web Sites

	Hamas		Hezbollah		Tamil Tigers		PFLP	
	Level 1	Level 2	Level 1	Level 2	Level 1	Level 2	Level 1	Level 2
Links Per Level	56	1715	213	3483	44	868	110	7127
"Under Construction" Pages	0	0	0	0	0	0	0	0
Obsolete Content	0	41	0	0	0	7	0	0
Obsolete Links	0	3	2	2	5	6	0	17
Non-Loading Media	1	2	1	1	0	0	0	1
Onsite Searching	Yes	Yes	Yes	Yes	No	Yes	No	Yes
Donating Functions	None	None	None	None	None	None	None	None
Repeat Visitor Recognition	No	No	No	No	No	No	No	No
Offers "How To" Guides	No	No	No	No	No	No	No	No
Number of Languages Offered	2	2	5	5	2	2	5	6
Multiple Sites Offerings	1	1	5	5	5	0	1	1

Second, both groups' Web sites offered some form of onsite searching capabilities. This is an important function as it provides the information user the ability to seek out additional information within the Web site. Therefore, the presence of this function may have a positive impact on perceived credibility.

Interestingly, neither group's Web sites offered any mechanism for users to directly donate funds, recognized repeat visitors, or offered instructional material online. These findings are representative of the context in which these types of groups operate. That is, because of the level of covertness they maintain, having a direct line of monetary support established for authorities to trace is not strategically sound. In addition, recognizing repeat visitors, or at least projecting the image that such an activity occurs, may not be beneficial. Also, because each of these groups is relatively established in its own society, offering instructional material might be construed as too

107

radical by constituents. Accordingly, the absence of these attributes may not negatively affect perceived credibility.

Each group similarly used multiple languages to present information. This demonstrates attempts to increase the base of persons receiving information related to the group's activities.

Concerning the differences between the two groups' Web sites, the religious nationalist group did worse on *Obsolete Content* as a result of Hamas' high marks. It was also found that the religious nationalist group was more likely to have non-loading media. However, the secular nationalist group scored significantly worse on *Obsolete Links,* with four times as many non-functioning links.

Table 24 illustrates the findings for *Information Reliability*. In this category, the religious nationalist group, with 795 total errors, did comparatively worse than the secular nationalist group with 254 errors recorded. That is, Hamas and Hezbollah's Web sites had more spelling, typographical, and grammatical errors than the Tamil Tigers and PFLP's Web sites. Consequently, perceived credibility may be higher for the secular nationalist Web sites.

Table 24: Information Reliability Scores for Religious and Secular Nationalist Web Sites

	Hamas		Hezbollah		Tamil Tigers		PFLP	
	Level 1	Level 2	Level 1	Level 2	Level 1	Level 2	Level 1	Level 2
Total Number of Errors	109	510	28	148	8	224	4	18
Spelling Errors	5	27	0	0	0	23	0	0
Typographical Errors	43	2	14	5	0	3	0	5
Grammatical Errors	61	481	14	143	7	198	4	13

Most of the grammatical errors found on Hamas' site seemed to result from poor English language skills of the person(s) conducting the translation of information. Similar incidents were found on the Tamil Tiger's Web site. However, a significant amount of incidents were recorded for Hamas' Web site. Predicting the impact of the quantity of errors found on Web sites such as Hamas' and the Tamil Tiger's is difficult because of the consistency in which they were made. According to the literature, consistent errors such as those identified with *Grammatical Errors*, are likely to be seen by the information user as somewhat expected and thus acceptable. As a result, perceived credibility may not suffer significantly. Nevertheless, if *Grammatical Errors* were not considered, the secular nationalist group may still receive higher perceived credibility.

Summary

In conclusion, while on one hand the comparative analysis suggests that secular nationalist groups' Web sites are more likely to receive higher perceived credibility resulting from better *Ambience* and *Information Reliability*; on the other hand the analysis shows little difference in *Functionality*. Although significant differences between the two groups were found related to obsolete content and links, pages under construction, onsite searching capabilities, donating funds, recognition of repeat visitors, provision of instructional material, and uses of multiple languages are all similar. For a more accurate representation of the perceived credibility differences between religious nationalist and secular nationalist Web sites to be correctly addressed, additional metrics might be created because many important contrasts are often obscured.

The findings of this study do demonstrate that terrorist organizations are extremely advanced in the design and use of Web sites for information dissemination. Importantly, the findings additionally illustrate stark differences in perceived credibility between the Web sites of the same type of terrorist organization.

CHAPTER 5

CONCLUSIONS

Introduction

This study addressed two issues. First, it was illustrated that terrorist groups continuously seek tools to securely, effectively, and efficiently communicate a message. Second, it was discussed that many who study terrorism are faced with methodological challenges to increase understanding of terrorist strategies, actions, or intentions.

Accordingly, three fundamental objectives were established for this research. The first was to move toward improved understanding of Web site effectiveness by assessing perceived credibility of various terrorist organizations' Web sites. Such an approach can increase knowledge of what varying purposes terrorists use Web sites, what types of information terrorists disseminate, and how effective a Web site may be. The second was to develop an applicable model that was feasible for researchers to employ. The research question asked was, *to what extent are there perceived credibility differences between terrorist organizations' Web sites?* The final objective was to illustrate differences in perceived credibility between terrorist organizations' Web sites using descriptive statistics.

The literature on terrorism makes several arguments: a) that terrorism is a means of communication; b) terrorists depend on media to get their message out; c) the World Wide Web endows terrorists with a tool that has revolutionized communications; and d) credibility is a major factor considered in Web site design or information seeking.

The literature review suggested numerous factors that inhibit or contribute to perceived credibility of Web sites. The findings of this assessment illustrate that in some

areas differences exist while in others there are similarities.

Results

This study compared the Web sites of two types of terrorist organizations, religious nationalist and secular nationalist. Additionally, it compared the Web sites of the terrorist organizations in each group. The investigation conducted here focused on three areas to assess perceived credibility: ambience, functionality, and information reliability.

Many scholars suggest that credibility is important to Web site designers and information seekers. The overall findings of this analysis support that claim. Indeed, Table 22 illustrated that all four Web sites investigated here had good ambience and only a few incidents recorded that might potentially affect perceived credibility. Table 8 provided evidence that the terrorist organizations' Web sites offered a tremendous amount of information and had relatively few issues with functionality. Conversely, Table 9 showed that a significant amount of errors were found, but these were primarily grammatical and likely due to the translation of information from one language to another. Accordingly, because they were consistent, they were expected, and it is unlikely that perceived credibility would suffer.

The findings also illustrated differences (albeit slight) between terrorist organizations Web sites that might affect perceived credibility. Tables 22 and 24, focused on ambience and information reliability. These tables showed that secular nationalist organizations may potentially receive relatively better perceived credibility from the average information user. However, Table 23 illustrated little difference in

functionality between religious nationalist and secular nationalist groups' Web sites. However, it is important to note that the findings demonstrated significant differences in perceived credibility factors between the two terrorist organizations' Web sites of each group.

Contribution

As a result of this study, evidence exists that terrorists conceive credibility as an important factor when designing and using Web sites. This suggests that terrorists have identified a tool that they can use to securely, effectively, and efficiently disseminate information. Moreover, the findings imply that terrorist organizations are resolute about maintaining those Web sites due to the advanced use of technology as well as the quantity and diversity of information they provide on the sites.

The model adapted for this study also offers a feasible mechanism to assess perceived credibility of terrorist organizations' Web sites without requiring physical contact with group members or supporters. Nevertheless, a few problematic issues arose.

Limitations

Although this study examined ten distinct records for each Web site, it was found that the information provided by each Web site changed relatively little over time. This presented three problematic issues and illustrated related weaknesses in the model.

First, this study only assessed information as it was presented for that particular day. That is, errors or incidents were recorded for each metric in each category for each

day. However, the metrics did not account for the corrections that were completed over time by the organization. For example, hypothetically a site might have ten spelling errors consistently throughout all ten records for a given level. However, those errors might be different errors. That is, a few errors might be corrected over time, while others remain uncorrected, and still more come about. Nevertheless, the model would only illustrate that ten errors occurred. It would not illustrate that more than ten errors came about over the time period, but that some were corrected while others were not. Consequently, the model might imply that little to no attention was given by the organization to improve the presentation of information which is not accurate.

Second, evidence of revisions made to specific pages on some Web sites existed, such as adding images or headlines of more recent events or activities. However, the vast majority of the information provided by the four Web sites received little to no revisions. The information that was replaced was more often than not, relocated in a section or component of the Web site specifically designated for archived information. Importantly, revisions were not completed on every Web site, every day. Nevertheless, the changes that were made in relation to the entire amount of information available made for a significant amount of redundancy in information. Consequently, the amount of times each Web site was to be recorded for this study was likely greater than necessary.

Third, it was discovered that a large amount of information was duplicated throughout the Web site. For example, the homepages had a significant amount of information that was related to a variety of issues. In many instances, some information was copied and pasted elsewhere in the Web site, generally where that information was

expanded on. However, if the information that was copied from the homepage had errors in it, then those same errors were present on the page where the information was pasted. Consequently, the quantity of errors was affected and the model was unable to illustrate that these were duplicated errors.

Fourth, a significant amount of information presented in different languages was found. Consequently, this information was not assessed. Although this is not believed to have had a significant impact on the overall assessments, it did present this study with an obstacle, not able to be overcome. Finally, the metrics for *Ambience* did not fully articulate the differences in appearance between the Web sites because these metrics were too broadly defined.

As shown, several limitations in the model were identified. Overall, it was unable to illustrate important variances in the data that occurred over time. Although this was not its intention, future studies might consider adjustments in the methodology in order to account for these concerns.

Implications and Future Research

This research study was ground-breaking, establishing a foundation for future research to be conducted. Consequently, many issues and areas were identified where research might be focused.

Theoretical

This study moves beyond recent research by demonstrating *how* terrorist organizations establish legitimacy. The findings suggest that they potentially contribute

115

to their legitimacy by effectively using Web sites. Evidence was found that suggests

these terrorist organizations present themselves in a way that establishes them as

legitimate social, political, or religious entities. That is, that these groups act as they are,

and present themselves to be, a contributing body to local society. Indeed, this is not a

novel discovery. In fact, many members of these groups do participate in governmental

activities and sponsor social welfare programs. However, it contrasts the general,

stereotypical assumption about a terrorist group's Web site. Nonetheless, can such an

approach to information dissemination on a Web site potentially be perceived as

credible, thus, establishing the group as a legitimate and relatively moderate group that

protects the interests of the people to which it serves? It is stated here that propaganda

grants authority to its makers. I suggest that it also brings legitimacy to its makers.

Accordingly, the type of propaganda is directly related to the type and level of legitimacy

held by an organization.

The evidence here additionally supports the claim that Web sites can be effective

tools impacting the longevity of a terrorist organization. They provide the means for

movements to continue to communicate with fighters, followers, sympathizers and

supporters worldwide. Interestingly, information found on each Web site for this

assessment indicated that the groups were addressing the most salient concerns of the

people to which they serve or who sympathize with them in their struggle. Future

research might address theoretical questions as to why this may be and how Web sites

are utilized to further these interests. For example, why do terrorist organizations focus

primarily on socially salient issues on their Web sites? To what extent do their efforts

build support among constituents? To what extent do supporters apply credibility to

certain issues promoted on groups' Web sites? And, is there a direct correlation between Web site effectiveness and group longevity?

I suggest that the findings indicate that these groups are in a form of competition, not too unlike corporations seeking greater market share. However, the ultimate goal is not profit, it is survival. The differences in perceived credibility likely reflect the overall aggressiveness and attentiveness of the group to lead over others in that endeavor. That is, these groups contend for the greatest amount of support possible. To acquire support equates to longevity. Therefore, they must attract as much communal support as possible relative to other groups operating in the same struggle. This may also help explain why the groups provide such a large amount of information in a wide array of communally salient categories. By presenting the group as the advocate for the community's interests and/or the protector of its way of life, it will gain legitimacy and credibility, ultimately leading to its own indefinite sustainment.

If groups evolve toward becoming a participating component of society, then hypothetically they might begin to move away from more violent behaviors. In time, such groups may eventually renounce terrorist activity entirely. Studies such as the one conducted here might identify these particular groups and monitor them throughout that process. Policies can thus be appropriately adjusted to manipulate the process.

Additionally, evidence was not discovered that indicated strategic or tactical communication to members, although such information may be present but not overtly identifiable. For example, no "How To Guides" were found, but instead information focusing on the narrative (under which these groups operate), clinics, schools, martyrdom, oppressive actions by the adversary, and other emotionally based issues

were found. This is in contrast to many other terrorism organizations' Web sites throughout the world and is an interesting finding. Further investigations are needed in order to increase understanding of why this is the case. Such research will clarify correlations with Web site effectiveness and actual success of the organization, and thus have significant policy implications.

It was also discovered that many Web sites created by group supporters exist. This may be an indicator of organizational success, an attempt by the group to reach a greater amount of people, or something completely different. Accordingly, this area demands further research and should address certain theoretical questions. For example, to what extent does an organization's success correlate with the creation of Web sites by supporters? Or, for what purposes are additional Web sites created by organizations and/or their supporters? As is evident, many questions for future research remain. However, this study does have implications for future policy related to terrorist organizations.

Practical

Advancements in technology, diverse uses of multimedia, professional appearance, and a focus on salient issues have given terrorists an edge in the world-wide struggle to eradicate terrorism. Efforts must be established that effectively counter the messages of hate disseminated around the globe on Web sites. With the increasing use of the Internet by terrorist organizations to disseminate information, greater attention must be given to the effectiveness of terrorists' Web sites. This study moves toward that end.

First, it provides evidence that indicates terrorist organizations' Web sites are potentially effective at achieving their objectives. This should be of high concern for counterterrorist agencies. Moreover, the findings show that differences between the Web sites of groups operating in the same struggle exist. This is likely due to access to resources and/or the level of communal support a particular group receives. As the literature suggested, as groups improve their situation, their access to resources increases. Greater resources can provide the terrorist organization with greater technological means to reach its goals. Consequently, studies such as the one conducted here will provide policy-makers with a greater understanding of what groups are strengthening their position in a specific struggle relative to other groups. Such information is invaluable for designing and implementing strategies meant to combat certain group's activities.

Second, this study illustrates the day-to-day strategy that these groups use to win the hearts and minds of their constituents and its potential effectiveness. It does so by utilizing a method that assesses their Web sites. The findings suggest that for any counterterrorism policy to be successful, it must focus on impeding this dynamic and multifaceted strategy.

Counterterrorism efforts must focus on the dialogue that is occurring between the terrorist organization, as an information provider, and the information seeker. Furthermore, it must do so through efforts similar to those used by terrorists' Web sites. In other words, a greater emphasis must be applied to policy that will establish and sustain a dialogue with the targeted population on the same issues and topics addressed by terrorists. Moreover, any Web-based dialogue must be supported with

actions. Any other policy will undermine counterterrorism efforts and strengthen the position of the terrorist organization relative to its adversary.

Methodological

Assessments of perceived credibility of Web sites over time should emphasize the further development of applicable, viable models that can be used by researchers in a variety of contexts. Such research should account for changes/corrections in information over time, differences in the information offered, and the impact of obsolete information relative to the amount of pages/information on a Web site. They should also provide greater clarity on which errors have greater effects on credibility.

This study identified important contrasts between religious nationalist and secular nationalist Web sites. However, other important contrasts were obscured. Future studies can benefit by incorporating innovative metrics in their models that provide a more accurate representation of the perceived credibility differences between these types of groups' Web sites.

Models should also consider the stages at which the information users establishes credibility, what factors play a role in that process, and to what extent those factors increase or decrease in effect as the user travels through the levels of the Web site.

This research applied a model to several terrorist groups to illustrate potential effectiveness by measuring perceived credibility. Many other organizations exist that attempt to sell an ideology such as political parties, interest groups, churches, or other religious associations. Subsequent research can be conducted by applying this model

to these types of organizations. It is likely that analytical methods might be refined in such contexts as the risk to the researcher would be decreased. Greater understanding of the importance of credibility as well as how users decide what is credible and what is not may also be achieved.

This study also discovered several interesting things about terrorist organizations' Web sites. For example, they use online stores for revenue generation. Future research may improve understanding of Web site effectiveness by assessing the success of online stores and the types of products they sell. A more in-depth study might also be undertaken to investigate this further and disclose the final destination for funds received in such online stores.

Fourth, the Web sites investigated here provided different amounts of information. Such disparities lead to a variety of research questions that need to be addressed in future analyses. That is, does a greater amount of information on the homepage affect credibility? Does a higher quantity of Web pages translate into greater quantities of information? Furthermore, might a greater quantity of pages correlate with increases in perceived credibility? Do errors have the same effect on credibility regardless of the amount of information on a single page?

Uniformly, much more information was presented on the homepage relative to the other pages in the site. It is suggested here that this is evidence indicating that terrorist groups understand the importance of gaining the information user's attention and keeping it. However, further research is needed to confirm this finding.

Finally, although this study gives significant importance to other variables, context was suggested to be the primary factor affecting perceived credibility.

Essentially, the contexts that information is created, distributed, and received in, impact all other contributing factors. This seems apparent not only in assessing perceived credibility of Web sites, but also in the design and operation of Web sites. This was evident in the vast dissimilarities found between Web sites of terrorist organization in the same struggle. This was an interesting find and for scholars who research context, this provides an enormous amount of potential for future research. Moreover, this discovery presents a significant opportunity for interdisciplinary research.

Future research on terrorist organizations' Web sites should consider the amount of data that will be assessed and how that process will be conducted. Furthermore, consideration should be given to modifications to the model and the potential effects to coding data. That is, if modifications to metrics in the model are made to better assess changes in information over time, then it is likely that variations in coding the data will increase. Therefore, the guidelines for coding the data will need to be much more stringent. Moreover, future methodological approaches should attempt to assess all information presented on the Web sites regardless of the language.

Summary

In conclusion, this research presents novel insight on evaluating Web sites as well as a new approach to studying terrorist organizations. The findings showed that terrorist organizations' Web sites will potentially receive positive levels of credibility from the average information user. As a consequence, these Web sites are empowered with the capacity to effectively reach the goals set out for them by their members. In other words, the findings show that through the use of Web sites, these groups will effectively

increase their support base improving recruiting, monetary contributions, physical protection, covertness, intimidation, or even establish themselves as legitimate components of society.

However, like other groundbreaking studies, many unanswered questions emerged. Indeed, an opportunity exists for future scholars to conduct interdisciplinary research in this field to increase understanding of how information seekers perceive credibility as well as the effectiveness of terrorist organizations' Web sites. To that end, future scholars will be able to use this study as a foundation to build research on terrorist strategies, tactics, intentions, and status. Furthermore, policy-makers now have a tool to accurately assess the potential effectiveness of terrorist organizations' Web sites and negate the threat that they pose. As important, this tool will enable counterterrorism agencies to identify the day-to-day strategies terrorists use and the specific methods or trends in tactics implemented to accomplish their goals. Accordingly, policy can be more accurately structured to thwart any and all terrorist activities.

APPENDIX

CODE BOOK FOR PERCEIVED CREDIBILITY ASSESSMENT MODEL

Ambience	*(Cosmetic factors impacting a user's interaction. Evaluate at the first level.)*	
Factor	*Objective*	*Rules*
Contrast	Determine if the contrast on a page between background and text is good or poor.	Contrast is either good or poor. The contrast of a page is poor if the contrast between background and text makes it difficult to identify and read information quickly. *1) Delineate the quantity of incidents per level. An incident is defined as a section of information that presents poor contrast.*
Consistent Font	Determine if the font style and font size on a page are consistent.	Inconsistencies exist if the font style and/or size make it difficult to determine headings from supportive text. *1) Delineate the quantity of incidents per level. An incident is defined as a section of information that presents poor font use.*
Crooked Columns	Determine if column alignment on a page is consistent.	Inconsistencies exist if the column alignment of an individual section makes it difficult to identify and read information quickly. *1) Delineate the quantity of incidents per level. An incident is defined as a section of information that presents crooked columns.*
Word Spacing	Determine if word spacing on a page is consistent.	White spacing between words must be consitent throughout each individual section of a page (e.g. single or double spacing). *1) Delineate the quantity of incidents found on each level.*
Line Spacing	Determine if line spacing on a page is consistent.	Spacing between lines must be consistent throughout each independent section (e.g. single or double spaced.). *1) Delineate the quantity of incidents found on each level.*

Functionality	*(Mechanical factors impacting a user's interaction. Evaluate at the first and second levels.)*	
Factor	*Objective*	*Rules*
"Under Construction"	Determine if links redirect the user to a page that is declared "Under Construction."	Consider only pages that display an "Under Construction" declaration. These are not to be dually classified as linked pages that do not upload or display a "File Not Found" declaration. *1) Delineate the quantity of links examined on each level.* *2) Delineate the quantity of incidents found on each level.*
Obsolete Content	Determine if information is > 30 days old.	Obsolete content is information on a page that is presented as recent, but is > 30 days old and/or incomplete (Do not include purposely archived or reposited information.). *1) Delineate quantity of incidents per level.* *2) Qualify the obsolete information by describing how old the information appears to be and for what purpose it is being used on the level.*
Obsolete Links	Determine if links to supporting pages display "File not Found" or other similar declaration.	Obsolete links are those that connect to a separate, system default page that displays that page cannot be found *1) Delineate the quantity of links per level.* *2) Delineate the quantity of incidents found on each level.*
Non-Loading Media	Determine if any media presented do not load.	Non-loading media include pictures, RSS feeds, video, or other non-text sources of information that do not load. *1) Delineate the quantity and type of incidents per level.*

Factor	*Objective*	*Rules*
Uses of Multiple Media (Video, RSS Feeds, Blogs, Mail Lists)	Determine uses of media such as video, RSS feeds, blogs, or mail lists.	Other media are defined as video, RSS feeds, blogs, or mail lists and are used to support the Web site's objective of disseminating information. *1) Delineate the quantity and type of incidents per level.*
Onsite Searching	Determine if Web site offers onsite searching capabilities.	Onsite searching capabilities are defined as the means to search the organization's Web site for specific information via a mechanism provided by the site's designer. *1) Delineate capabilities or lack thereof.*
Multiple Languages	Determine if the site offers information in multiple languages.	Offers Web site or pages/sections in more than one language *1) Delineate the total quantity of languages offered, and* *2) Delineate the type of languages offered.*
Repeat Visitor Recognition	Determine if the site recognizes repeat visitors.	*1) Visit Web site multiple times and delineate whether site recognizes repeat visitors or not*
Multiple Site Offerings	Determine if the organization offers multiple sites for information dissemination.	Multiple Site Offerings is defined as a Web site that offers links to other pages sponsored by the terrorist organization under review. These sites can be of the same language or not. *1) Delineate the quantity of additional sites the organization offers.* *2) Delineate the languages they are presented in.*
Offers "How To" Guides	Determine if the site offers instructional materials related to its activities.	"How to Guides" are instructional materials that provide guidance and/or instruction on activities related to the organization's activities. *1) Delineate the quantity of different types of materials offered.* *2) Delineate the type of materials offered.*

Information Reliability	*(Language factors impacting a user's interaction. Evaluate at the first and second levels.)*	
Factor	*Objective*	*Rules*
Number of Errors	Determine if the page has less than 12 errors or 12 or more errors.	Errors are defined as language errors such as spelling, typographical, or grammatical. *1) Delineate the quantity of incidents per level.* *2) Delineate 1 to 12, or more than 12 errors per each level.*
Spelling Errors	Determine if the page has spelling errors.	Spelling errors are those identified in the English version of the information presented. *1) Delineate the quantity of incidents per level.*
Typographical Errors	Determine if the page has typographical errors.	Typographical errors are those identified in the English version of the information presented. *1) Delineate the quantity of incidents per level.*
Grammatical Errors	Determine if the page has grammatical errors.	Grammatical errors are those that have been identified in the English version of the information presented. *1) Delineate the quantity of incidents per level.*

REFERENCE LIST

Allen, B. L. (1996). Information Tasks: Interacting with Information Systems. *Information Tasks: Toward a User-Centered Approach to Information Systems.* London: Academic Press.

Andrews, L.W. and Gutkin, T.B. (1991). The Effects of Human Versus Computer Authorship on Consumers' Perceptions of Psychological Reports. *Computers in Human Behavior*, 7, 311-317.

Baker L. and Wagner, J.L. (1987). Evaluating Information for Truthfulness: The Effects of Logical Subordination. *Memory Cognition*, 15(3), 247-255.

Barry, C. L. (1993). *The Identification of User Relevance Criteria and Document Characteristics: Beyond the Topical Approach to Information Retrieval.* Unpublished Doctoral Dissertation. Syracuse University, Syracuse, New York.

Barry, C. L. (1994). User-Defined Relevance Criteria: An Exploratory Study. *Journal of the American Society for Information Science,* 45(3), 149-159.

Barry, C. L. and Schamber, L. (1998). User's Criteria for Relevance Evaluation: A Cross-Situational Comparison. *Information Processing and Management,* 34(2/3), 219-236.

Bauhs, J.A. and Cooke, N.J. (1994). Is Knowing More Really Better? Effects of System Development Information in Human-Expert System Interactions. *CHI 94 Companion*, 99-100. New York: ACM.

Benard, Cheryl. (2005). A Future for the Young: Options for Helping Middle Eastern Youth Escape the Trap of Radicalization. RAND's Initiative on Middle Eastern Youth Conference. WR-354. Retrieved 29 March 2009, from http://www.rand.org/pubs/working_papers/2006/RAND_WR354.pdf.

Benbasat, I. and Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, 23(1), 3-16.

Buller, D.B. and Burgoon, J.K. (1996). Interpersonal Deception Theory. *Communication Theory*, 6(3), 203-242.

Burgoon, J.K., Bonito, J.A., Bengtsson, B., Cederberg, C., Lundeberg, M., and Allspach, L. (2000). Interactivity in Human-Computer Interaction: A Study of Credibility, Understanding, and Influence. *Computers in Human Behavior*, 16, 553-574.

Burnstein, E. and Vinokur, A. (1973). Testing Two Classes of Theories about Group-Induced Shifts in Individual Choice. *Journal of Experimental Social Psychology,* 9, 123-137.

Byrne, D. (1971). *The Attraction Paradigm*. New York: Academic.

Chen, H., Qin, J., Reid, E., Chung, W., Zhou, Y., Xi, W., Lai, G., Bonillas, A.A., and Sageman, M. (2004). The Dark Web Portal: Collecting and Analyzing the Presence of Domestic and International Terrorist Groups on the Web. In: *Proceedings of International IEEE Conference on Intelligent Transportation Systems*.

Cialdini, R.B. (1993). *Influence: Science and Practice*. (3rd ed.). New York: Harper Collins.

Cioffi-Revilla, C. (1983). A Probability Model of Credibility: Analyzing Strategic Nuclear Deterrence Systems. *The Journal of Conflict Resolution*, 27(1), 73-108.

Cohen, S. (1986). Knowledge and Context. *The Journal of Philosophy*, 83(10), Eighty-Third Annual Meeting American Philosophical Association, Eastern Division. 574-583.

Coll, S. and Glasser, S.B. (2005). Terrorists Turn to the Web as Base of Operations. *Washington Post*, August 7, 2005.

Corritore, C.L., Kracher, B., & Wiedenbeck, S. (2003). On-Line Trust: Concepts, Evolving Themes, a Model. I*nternational Journal of Human-Computer Studies*, 58(6), 737-758.

Crenshaw, M. (1981). The Causes of Terrorism. *Comparative Politics,* 13(4).

Crenshaw, M. (2005). Addressing the Causes of Terrorism: Political Explanations. *The Club de Madrid Series on Democracy and Terrorism. Volume 1.* The International Summit on Democracy, Terrorism, and Security. Club de Madrid: March, 2005.

Crenshaw, M. (2007). The Organization of Terrorism. In James O. Ellis III (Ed.), *Terrorism: What's Coming - The Mutating Threat*. Memorial Institute for the Prevention of Terrorism (MIPT). Oklahoma City, OK.

Dale, S.F. (1988). Religious Suicide in Islamic Asia: Anticolonial Terrorism in India, Indonesia, and the Philippines. *The Journal of Conflict Resolution,* 32(1).

Denning, D.E. (2000) Cyberwarriors: Activists and Terrorists Turn to Cyberspace. *Harvard International Review*, 23(2), 7-75.

Denning, D.E. (2002). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Retrieved July 17, 2008 from http://www.nautilus.org/info-policy/workshop/papers/denning/html.

Dennis, A. R. (1996). Information Exchange and Use in Group Decision Making: You can Lead a Group to Information, but You Can't Make It Think. *MIS Quarterly*, 20(4), 433-457.

Eubank, W. and Weinberg, L. (2001). Terrorism and Democracy: Perpetrators and Victims." *Terrorism and Political Violence,* 13(1), 155-164.

Everard, A. and Galletta, D. F. (2005). How Presentation Flaws Affect Perceived Site Quality, Trust, and Intention to Purchase from an Online Store. *Journal of Management Information Systems*, 22(3), 55-95.

Fanon, F. (1965). *A Dying Colonialism*. New York, New York: Grove Press.

Fogg, B.J., and Tseng, H. (1999). The Elements of Computer Credibility. *Proceedings of AM CHI 99 Conference on Human Factors in Computing Systems,* 1, 80-87. New York: ACM Press.

Fogg, B.J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., Rangnekar, A., Shon, J., Swani, P., and Treinen, M. (2001). What Makes Web Sites Credible? A Report on a Large Quantitative Study. *SIGCHI '01*, 3(1), 61-68.

Fogg, B.J., Lee, E., and Marshall, J. (2002a). Interactive Technology and Persuasion. In J.P. Dillard and M. Pfau (Eds.), *The Handbook of Persuasion: Theory and Practice*. Thousand Oaks, CA: Sage.

Fogg, B.J., Kameda, T., Boyd, J., Marshall, J., Sethi, R., Sockol, M., & Trowbridge, T. (2002b). *Stanford-Makovsky Web Credibility Study 2002: Investigating What Makes Websites Credible Today*. A Research Report by the Stanford Persuasive Technology Lab & Makovsky & Company. Stanford University. Available at www.webcredibility.org.

Friedman, T.L. (2005). *The World is Flat*. New York: New York.

Gatignon, H. and Robertson, T.S. (1991). Innovative Decision Processes. T.S. Robertson and H.H. Kassarjian (Eds.), *Handbook of Consumer Behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Glassie, H. (1979). *Folk Housing in Middle Virginia*. Knoxville, Tenn.

Goffman, E. (1974). *Frame Analysis*. New York, New York.

Goldstein, K. (1964). *A Guide for Field Workers in Folklore*. Hatboro, Pennsylvania.

Goodman, S.E., Kirk, J.C., and Kirk, M.H. (2007). Cyberspace as a Medium for Terrorists. Technological Forecasting and Social Change, 74, 193-210.

Grabner-Krauter, S. and Kaluscha, E.A. (2003). Empirical Research in On-line Trust: A Review and Critical Assessment. *International Journal of Human-Computer Studies*, 58(6), 783-812.

Gunaratna, R. (2007). Strategic Counterterrorism: The Way Forward. In James O. Ellis III (Ed.), *Terrorism: What's Coming - The Mutating Threat*. Memorial Institute for the Prevention of Terrorism (MIPT). Oklahoma City, OK.

Gurr, T.R. (2005). Addressing the Causes of Terrorism: Economic Factors. *The Club de Madrid Series on Democracy and Terrorism. Volume 1.* The International Summit on Democracy, Terrorism, and Security. Club de Madrid: March, 2005.

Hall, E. T. (1977). *Beyond Culture*. Garden City, New York.

Hamas Web Site. (2009). Retrieved from www.sabiroon.org. Last visited 28 March 2009.

Hanowski, R.J., Kantowitz, S.C., & Kantowitz, B.H. (1994). Driver Acceptance of Unreliable Route Guidance Information. *Proceedings of the Human Factors Society 38th Annual Meeting*, 1062-1066.

Herz, J. (1971). "Relevancies and Irrelevancies in the Study of International Relations," *Polity*, 4, 29 and 31.

Hezbollah Web Site (2009) Retrieved from www.moqavemat.com. Last visited 28 March 2009.

Hoffman, D.L., Novak, T.P., & Peralta, M. (1999). Building Consumer Trust Online. *Communications of the ACM*, 42(4), 80-85.

Hoffman, B. (2001). Change and Continuity in Terrorism. *Studies in Conflict and Terrorism*, 24, 417-428.

Hoffman, B. (2005). *Does Our Counter-Terrorism Strategy Match the Threat?* Testimony to the Committee on International Relations Subcommittee on International Terrorism and Nonproliferation, United States House of Representatives. September 29, 2005.

Hoffman, B. (2006) Inside Terrorism. New York, New York: Columbia University Press.

Honaker, L.M., Hector, V.S., & Harrel, T.H. (1986). Perceived Validity of Computer Versus Clinician-Generated MMPI Reports. *Computers in Human Behavior*, 2, 77-83.

Institute for Security Technology Studies (ISTS). (2004). *Examining the Cyber Capabilities of Islamic Terrorist Groups*. Report, ISTS. http://www.ists.dartmouth.edu/.

Jenkins, B. M. (1975). International Terrorism: A New Mode of Conflict. In David Carlton and Carlo Schaerf (Eds.), *International Terrorism and World Security*. London: Croom Helm.

Jenkins, B.M. (2007). Introduction. In James O. Ellis III (Ed.), *Terrorism: What's Coming - The Mutating Threat*. Memorial Institute for the Prevention of Terrorism (MIPT). Oklahoma City, OK.

Kantowitz, B.H., Hanowski, R.J., & Kantowitz, S.C. (1997). Driver Acceptance of Unreliable Traffic Information in Familiar and Unfamiliar Settings. *Human Factors*, 39(2), 164-176.

Kelley, J. (2002). Information Security News: Militants Wire Web With Links to Jihad. *InfoSec News*, 11. Retrieved June 12, 2008, from http://seclists.org/isn/2002/Jul/0050.html.

Kerber, K.W. (1983). Attitudes Towards Specific Uses of the Computer: Quantitative, Decision-Making and Record-Keeping Applications. *Behavior and Information Technology*, 2, 197-209.

Kim, J. and Moon, J.Y. (1997). Designing Towards Emotional Usability in Customer Interfaces: Trustworthiness of Cyber-Banking System Interfaces. *Interacting with Computers*, 10, 1-29.

Lee, J. (1991). The Dynamics of Trust in a Supervisory Control Simulation. *Proceedings of the Human Factors Society 35th Annual Meeting,* 1228-1232.

Lee, J. and Moray, N. (1992). Trust, Control Strategies and Allocation of Function in Human-Machine Systems. *Ergonomics*, 35(10), 1243-1270.

Lerch, F.J. and Prietula, M.J. (1989). How Do We Trust Machine Advice? Designing and Using Human-Computer Interfaces and Knowledge Based Systems. *Proceedings of the Third Annual Conference on Human Computer Interaction*, 411-419. Amsterdam: Elsevier.

Lia, B. (2005). Globalization and the Future of Terrorism. New York: Routledge.

Lombard, M., Snyder-Duch, J., & Bracken, C. C. (2005, June 13). Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Research Projects. In *Intercoder Reliability in Content Analysis*. Retrieved February 20, 2009 from http://www.temple.edu/sct/mmc/reliability/.

Lord, C.G., Ross, L., and Lepper, M.R. (1979). Biased Assimilation and Attitude Polarization: The Effects of Prior Theories on Subsequently Considered Evidence. *Journal of Personality and Social Psychology*, 37, 2098-2109.

Mackie, D. M., Worth, L.T., & Asuncion, A. (1990). Processing of Persuasive In-group Messages. *Journal of Personality and Social Psychology*, 58, 812-822.

Matarazzo, J.D. (1986). Response to Fowler and Bitcher on Matarazzo. *American Psychologist*, 41, 96.

McKnight, D.H., Kacmar, C., & Choudhury, V. (2003). Whoops – Did I Use the Wrong Construct to Predict E-commerce Trust? Modeling the Risk-Related Effects of Trust Vesus Distrust Concepts. In R.H. Sprague Jr. (ed.), *Proceedings of the 36th Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Computer Society Press, (available at csdl2.computer.org/comp/proceedings/hicss/2003/1874/07/187470182b.pdf).

Metzger, M. J. (2007). Making Sense of Credibility on the Web: Models for Evaluating Online Information and Recommendations for Future Research. *Journal of the American Society for Information Science and Technology*, 58(13), 2078-2091.

Meyer, C. (1991). *Underground Voices: Insurgent Propaganda in El Salvador, Nicaragua, and Peru*. Santa Monica, CA.: RAND Corporation.

Miller, C.A. and Larson, R. (1992). An Explanatory and "Argumentative" Interface for a Model-Based Diagnostic System. *Proceedings of the ACM Symposium on User Interface Software and Technology*, 1993, 43-52.

Morley, D.D. and Walker, K.B. (1987). The Role of Importance, Novelty, and Plausibility in Producing Belief Change. *Communication Monographs*, 54, 436-442.

Muir, B.M. (1988). Trust Between Humans and Machines, and the Design of Decision Aids. *Cognitive Engineering in Complex Dynamic Worlds*, 71-83.

Muir, B.M. and Moray, N. (1996). Trust in Automation: Part II. Experimental Studies of Trust and Human Intervention in a Process Control Simulation. *Ergonomics*, 39(3), 429-460.

Osgood, C.E. and Tannenbaum, P.H. (1955). The Principle of Congruity in the Prediction of Attitude Change. *Psychology Review*, 62(1), 42-55.

Pancer, S.M., George, M., & Gebotys, R.J. (1992). Understanding and Predicting Attitudes Toward Computers. *Computers in Human Behavior*, 8, 211-222.

Pape, R.A. (2005). *Dying to Win: The Strategic Logic of Suicide Terrorism*. New York: Random House.

Peirce, C.S. (1877). How to Make Our Ideas Clear. *Popular Science Monthly*, 12, 286-302.

Petty, R.E. and Cacioppo, J.T. (1981). *Attitudes and Persuasion: Classic and Contemporary Approaches*. Dubuque, IA: Brown.

Petty, R.E. and Cacioppo, J.T. (1986). *Communication and Persuasion*. Springer-Verlag, New York.

Popular Front for the Liberation of Palestine Web Site. (2009). Retrieved from www.pflp.ps/english/. (2009). Last visited 28 March 2009.

Qin, J., Zhou, Y., Reid, E., Lai, G., and Chen, H. (2007). Analyzing Terror Campaigns on the Internet: Technical Sophistication, Content Richness, and Web Interactivity. International Journal of Human-Computer Studies, 65, 71-84.

Rapoport, D.C. (1984). Fear and Trembling: Terrorism in Three Religious Traditions. *The American Political Science Review,* 78(3), 658-677.

Ross, J.I. and Gurr, T.R. (1989). Why Terrorism Subsides: A Comparative Study of Canada and the United States. *Comparative Politics*, 21(4), 405-426.

Russell, C.A., Banker, L. J., and Miller, B.H. (1979). Out-inventing the Terrorist. In *Terrorism: Theory and Practice.* (Eds.) Y. Alexander et al., Boulder, Colorado: Westview Press.

Sandler, T. and Enders, W. (2003). *An Economic Perspective on Transnational Terrorism*. A Working Paper No. 03-04-02. University of Alabama, Working Paper Series.

Schmid, A. P. and de Graaf, J. (1982). *Violence as Communication: Insurgent Terrorism and the Western Media.* Beverly Hills, Ca.: Sage Publishing.

Schmid, A.P. (1983). *Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature,* (New Brunswick: Transaction Books.

Schmid, A.P. and Jongman, A.J. (1988). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*. Amsterdam: North Holland, Transaction Books.

Self, C.S. (1996). Credibility. In M. Salwen and D. Stacks (Eds), *An Integrated Approach to Communication Theory ad Research*. Mahway, NJ: Erlbaum.

Sheridan, T.B., Vamos, T., & Aida S. (1983). Adapting Automation to Man, Culture, and Society. *Automatica*, 19(6), 605-612.

Sivasailam, N., Kim, D.J., & Rao, H.R. (2002). What Companies are(n't) Doing About Website Assurance. *IEEE IT Professional*, 4(3), 33-40.

Slater, M.D. and Rouner, D. (1996). How Message Evaluation and Source Attributes May Influence Credibility Assessment and Belief Change. Journalism and Mass Communication Quarterly, 73, 974-991.

Stiff, J. (1994). *Persuasive Communication*. New York: Guilford.

Sullivan, M. P. (1973). The Question of "Relevance" in Foreign Policy Studies. *The Western Political Quarterly*, 26(2), 314-324.

Tamil Tigers Web Site. (2009). Retrieved from www.eelamweb.com. Last visited 28 March 2009.

Taylor, R.S. (1962). The Process of Asking Questions. *American Documentation*, 13(4), 391-396.

Taylor, R.S. (1968). Question-Negotiation and Information Seeking in Libraries. *College and Research Libraries*, 29(3), 178-194.

Taylor, R. S. (1985). Information Values in Decision Contexts. *Information Management Review*, 1(1), 47-55.

Taylor, R.S. (1988). *Value-Added Processes in Information System*. Norwood, NJ: Ablex.

Thomas, T.L. (2003). Al Qaeda and the Internet: The Danger of 'Cyber-Planning. *Parameters*, 112-123.

Tsfati, Y. and Weimann, G. (2002). www.terrorism.com: Terror on the Internet. Studies in Conflict and Terrorism, 25, 317-332.

Tseng, S. and Fogg, B.J. (1999). Credibility and Computing Technology. *Communications of the ACM*, 42(5), 39-44.

United Nations. (2007). *Definitions of Terrorism*. United Nations, Office on Drugs and Crime. Retrieved June 30, 2007, from http://www.unodc.org/unodc/terrorism_definitions.html.

U.S. Department of Justice. (2004). *FBI Policies and Guidelines 2000/2001*. Federal Bureau of Investigation. Washington: Government Printing Office. Retrieved June 11, 2007, from http://www.fbi.gov/publications/terror/terror2000_2001.htm.

U.S. Department of State. (2004). *Patterns of Global Terrorism 2003.* Washington: Government Printing Office. Retrieved June 11, 2007, from http://www.state.gov/s/ct/rls/crt/2003/.

Waern, Y., Hagglund, S. et al. (1992). Communication Knowledge for Knowledge Communication. *International Journal of Man-Machine Studies*, 37, 215-239.

Waern, Y. and Ramberg, R. (1996). People's Perception of Human and Computer Advice. Computer Human Behavior, 12(1), 17-27.

Wathen, C.N. and Burkell, J. (2002). Believe It or Not: Factors Influencing Credibility on the Web. Journal of the American Society for Information Science and Technology, 53(2), 134-144.

Weinberg, L. (2007). Observations on the future of Terrorism. In James O. Ellis III (Ed.), *Terrorism: What's Coming - The Mutating Threat*. Memorial Institute for the Prevention of Terrorism (MIPT). Oklahoma City, OK.

Weimann, G. (2004). www.terror.net: How Modern Terrorism Uses the Internet. *Special Report, US Institute of Peace*. Retrieved June 11, 2008, from http://www.usip.org/pubs/specialreports/sr116.pdf.

Weinmann, G. (2006). *Terror on the Internet*. Washington, D.C.: U.S. Institute of Peace Press.

Whine, M. (1999). Islamist Organizations on the Internet. *Terrorism and Political Violence*, 11(1).

White, J. (1991). *Terrorism: An Introduction*. Pacific Grove, CA: Brooks/Cole.

Wilson, E. and Sherrell, D. (1993). Source Effects in Communication and Persuasion Research: A Meta-Analysis of Effect Size. Journal of the Academy of Marketing Science, 21, 101-112.

Young, K. (1985). The Notion of Context. *Western Folklore*, 44(2), 115-122.

Zajonc, R.B. (1980). Feeling and Thinking: Preferences Need No Inferences. *American Psychologist*, 35, 151-175.

Zanini, M. and Edwards, S. (2001). Networking of Terror in the Information Age. In J. Arquilla and D.F. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand.

Zimbardo, P. and Leippe, M. (1991). *The Psychology of Attitude Change and Social Influence*. New York: McGraw-Hill.

Zhou, Y., Reid, E., Qin, J., Chen, H., & Lai, G. (2005). US Domestic Extremist Groups on the Web: Link and Content Analysis. IEEE Intelligent Systems (Special Issue on Homeland Security), 20(5), 44-51.