

# Evaluating the Impact of Contextual Background Fusion on Unclassified Homeland Security Intelligence

Charles S. Eaneff, Jr.

## INTRODUCTION

The 2007 National Strategy for Information Sharing recognizes that state, local, and tribal governments “carry out their counterterrorism responsibilities within the broader context of their core mission(s)...”<sup>1</sup> In order for this national strategy to be successful, intelligence provided to these state, local, and tribal recipients must also be presented within the context of these core missions. Multiple initiatives have ensured that these non-traditional recipients (NTR) in law enforcement, fire, emergency medical services (EMS), emergency management, public health, and the private sector are now receiving unclassified intelligence products from multiple sources including the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), Fusion Centers, Joint Terrorism Task Forces (JTTF), and Terrorism Early Warning Groups (TEWG). However, simply pushing intelligence products to non traditional recipients (NTR) is not enough. As discussed in a Markle Foundation Working Group Report, *Networking of Federal Government Agencies with State and Local Government and Private Sector Entities*, “...adequate context for homeland security providers to effectively utilize information is specific, tailored for each local entity, rapidly disseminated, and does not overburden recipients with vague or irrelevant information.”<sup>2</sup> The *Final 9/11 Commission Report* noted the importance of context in decision making, reporting that the president was provided intelligence “news without... much context” prior to September 11, 2001, contributing to a failure of decision makers to recognize that Bin Laden posed a “novel danger.”<sup>3</sup>

This paper does not attempt to determine whether providing classified or unclassified intelligence to NTR is an effective strategy. *The National Criminal Intelligence Sharing Plan* cites the need to “identify technical means to aid and expedite the production of unclassified ‘tear line’ reports.”<sup>4</sup> Department of Justice “Fusion Center Guidelines” (2006) document guidelines on the sharing of unclassified intelligence. The National Strategy for Homeland Security (2007) outlines the need to share intelligence with all levels of government. Clearly, the choice to share unclassified intelligence products has already been made. This article explains the impact of implementing contextual background fusion (CBF) with intelligence already provided to NTR in terms of the perceived value and quality of that intelligence.

Policy demands that more intelligence be shared with NTR; for that intelligence to be effectively utilized, decision makers must perceive both the value and quality of that intelligence.<sup>5</sup> Providing unclassified intelligence “on demand, in context” (a motto of the Congressional Research Service) is critical for millions of employees in NTR disciplines who incorporate that context into day-to-day decision making in public contacts, policy development, strategy, and tactics. In the absence of CBF by intelligence producers, open Internet searches by intelligence recipients can prove entirely inaccurate, degrading both the value and quality of the intelligence. For instance, a Google search that might be completed by a homeland security professional searching for contextual background on aircraft use in Islamic terrorist attacks, “Islamic terrorists kamikazes

weapon aircraft” leads to a “Non Aligned Press Network” story where it is reported that the planes on 9/11 were flown utilizing remote controls by individuals in American government. The U.S. State Department attempts to identify such misinformation on USINFO.STATE.GOV.<sup>6</sup> If the intelligence producer fails to provide CBF with their product, NTR may find very authentic looking information on the Internet that, when combined with timely, accurate, and actionable intelligence, produces poor decisions. Failure to control the value and quality of the contextual background that will be utilized by NTR to understand intelligence is a failure to ensure the value and quality of that intelligence.

The objective of this study is to improve the value and the quality of homeland security information sharing by examining the impact of adopting CBF in intelligence sharing. As part of the national information sharing strategy, DHS and FBI provide unclassified intelligence to NTR and routinely request feedback on perceived value and quality. If CBF is shown to improve DHS/FBI defined value and quality factors, the technology utilized must be evaluated for technology acceptance by NTR. Studies using the Technology Acceptance Model (TAM) have provided empirical support for a positive relationship between perceived value/ease of use and technology adoption.

Allied non-state actors in the private sector control approximately 85 percent of the nation’s critical infrastructure in the over 87,000 different U.S. jurisdictions.<sup>7</sup> For every federal law enforcement officer, there are approximately five public sector health professionals, seven state/local law enforcement officers, ten firefighters and twenty-one private security professionals, along with countless other public works, emergency management and emergency medical professionals.<sup>8</sup> As of June 2000, there were approximately 708,022 state and local law enforcement officers in the United States.<sup>9</sup> As of June 2002, there were only 93,000 Federal law enforcement officers, or less than 12% of sworn law enforcement.<sup>10</sup> The FBI, lead investigative agency for domestic terrorism, had only 12,416 agents as of October 2005, or approximately 1.5% of total law enforcement. In order to maximize our defense against asymmetric threats, we must effectively utilize unclassified intelligence to educate these diverse professionals on threats, engage them in the intelligence process, and enlist them to provide information to federal partners so that appropriate preventative measures can be considered. If found to be effective, CBF for NTR would represent a concrete, visible step in the transformation from a need-to-know to a need-to-share culture.

## **SIGNIFICANCE OF CONTEXTUAL BACKGROUND**

In the study of philosophy, some believe the understanding of text is dependent on the context in which the reader exists. As the text is read, it is interpreted based on the social context and bias of the interpreter. Additionally, text has its own “horizon of meaning” which is influenced by the contextual background of the writer, the time of writing, and the originating context. Philosophical hermeneutics examines the relationship between a reader and text, both of which must be understood within the context of their experience and creation respectively.<sup>11</sup>

In the creation and distribution of unclassified intelligence, hermeneutic fusion is problematic; the original process of creation is often based on classified intelligence, which may not be fused to an unclassified document. As the author/producer of unclassified intelligence is prohibited from the fusion of classified hermeneutic material, open source contextual background chosen by authors/producers must be used to

replace the original, classified material that influenced the hermeneutic of the writer at the time of creation. In this article, contextual background is defined as unclassified material that best represents the hermeneutic of the producer at the time of creation.

### **Contextual Background and Intelligence Usefulness**

As expressed by John Hillen in the *National Review*, “U.S. Intelligence Failures stem from too much information, not enough understanding.”<sup>12</sup> This is a subtle, but critical point; even a high quality intelligence product that is not fully understood by NTR may lack usefulness, failing to provide the knowledge required to improve decision making.

The sentiment of Hillen is echoed in CIA reports, outlining that the provision of contextual background is a critical component in the usefulness of intelligence products.

In periods of crisis, when demands are high and response time is short, most written intelligence production is in the form of policy-driven memos and briefs and pieces written for daily publications. The result of this narrowly focused and piecemeal intelligence flow is that it does not foster continuity of analysis nor does it provide a context within which to place seemingly unrelated information... **The Intelligence Community has made substantial, although sporadic, efforts over the past decade and a half to explore better and more technologically advanced methods of communicating with consumers. The results, however, have been modest at best. The requirement to have background and contextual information available at the policymaker's fingertips in a timely fashion remains unfulfilled.**<sup>13</sup> (Emphasis added)

Decision makers often demand “tailored” intelligence briefs beyond what is prepared for general distribution in order to meet their decision making needs.<sup>14</sup> This issue is exacerbated by the recent addition of NTR. These recipients do not have personal intelligence analysts to produce “tailored” briefs that contain necessary contextual background. NTR are often unaccustomed to the intelligence cycle and use of intelligence products as their discipline related training and experience did not previously require the use of such intelligence. As described by Lisa Palmieri, President of the International Association of Law Enforcement Intelligence Analysts,

I also recall thinking that ***if these executives got what they asked for; they would be buried in uncorroborated, unevaluated, “white noise”... This has, unfortunately, come to pass***, with law enforcement agencies erring on the side of caution; they are sharing more piece-meal information than could ever be made useful in case any small detail might possibly be deemed important in retrospect.<sup>15</sup> (Emphasis added)

Volumes of information without contextual background can overwhelm NTR and is not useful.

### **Contextual Background and Decision Making**

There is agreement that contextual background is a critical component in intelligence decision making.<sup>16</sup> Extensive research exists on decision-making theory, with similarly extensive discussion of the impact of intelligence products on decision making. Context is defined as the “sum of all the knowledge possessed by the operators on the whole task.”<sup>17</sup>

In a Pomerol and Brézillon model, a decision maker would, when presented with an intelligence product, access his or her contextual knowledge, and then proceduralize that knowledge based on the intelligence product in hand; in this process, the decision maker may also access available external contextual information, incorporating that knowledge and proceduralizing it prior to decision making. Pomerol and Brézillon note, “... it is clear that a Palestinian whose prior knowledge is reduced to his Imam’s preaches [sic] cannot have the same interpretation of Middle East events as a Harvard alumnus.”<sup>18</sup>

## A Traditional Model for Decision Making

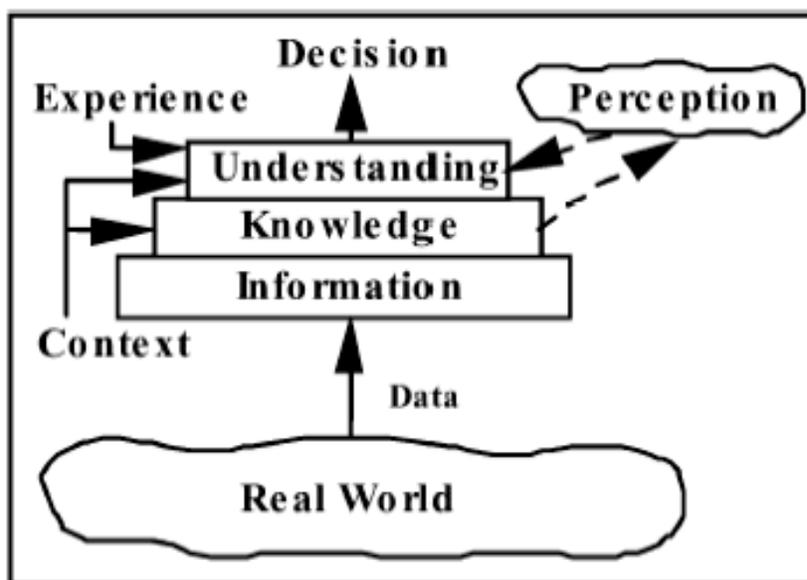


Figure 1: Context (From the North Atlantic Treaty Organization, 2002)

Understandably, military applications of context in decision making center on pragmatic application. Training material utilized by the North Atlantic Treaty Organization (NATO) reflects that practical application of context in decision making: “...knowledge is produced when information is correlated with a model of the world and the current context.”<sup>19</sup>

In describing the power of context in terrorism decision making, Professor Fathali Moghaddam contends that “terrorism is explained by the power of context”<sup>20</sup> Regardless of whether context and decision making are evaluated through the lens of the academic or the war fighter, literature documents that context involved in the decision-making process has a significant impact on the nature, quality, and effectiveness of the decision.

### Non Traditional Recipients and Contextual Background

Robert Steele highlights the value of context in the intelligence process for all recipients:

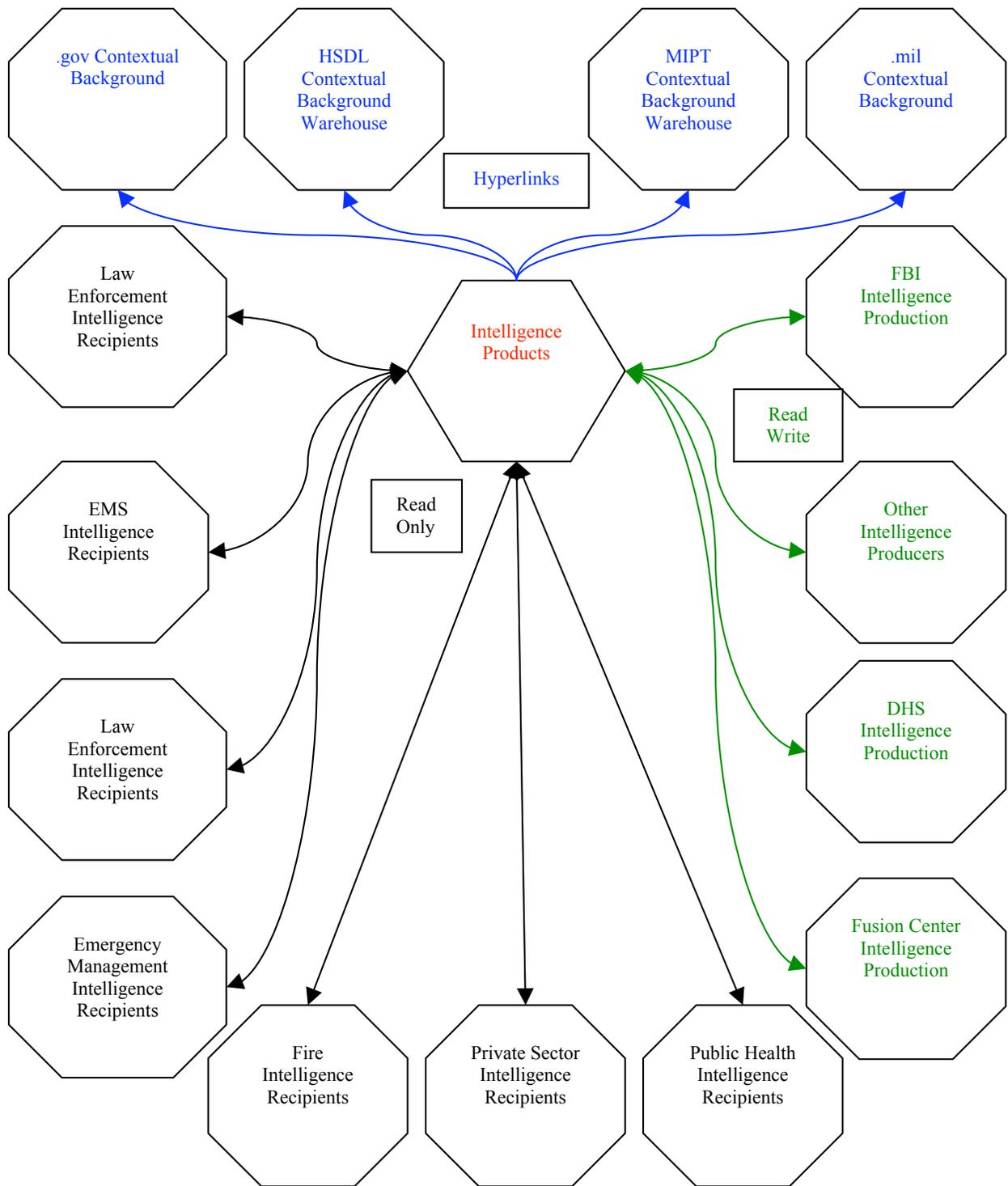
New Value is in Content + **Context** + Speed. ***The traditional craft of intelligence has tended to fragment content from its context***, and be largely oblivious to timing. This is true both in the collection cycle and in the production cycle. The new craft of intelligence ***recognizes that the value of any given information***, apart from its relevance to the decision at hand, ***stems from a combination of the content in context, and the content in time.***<sup>21</sup> (Emphasis Added)

Steele understands that the value of intelligence is not based solely on the sources utilized in the intelligence product, and that “historical knowledge,” (referenced by Pomerol and Brézillon as “contextual knowledge”) is a critical factor in the value of intelligence products. This research identifies the impact of avoiding “fracturing content from its context,” by fusing content (existing intelligence products) + context (vetted, valid, and accurate) + speed (hyperlink fusion) for non traditional recipients. Speed through hyperlink fusion leverages the attention span of the reader, providing contextual background at the exact moment the issue is facing the reader. (Hyperlinks are words, phrases or pictures that can be “clicked” when a cursor passes over, redirecting the reader to another web page or section of the page. Hyperlinks are also referred to as “clickable links” or “links.”)

### **Technology and Contextual Background**

The literature shows that decision making is impaired when insufficient information is available; it also documents that too much information (or information overload) impairs decision-making. Technology has the potential to impair decision making through the provision of too much information (the “white noise” discussed by Lisa Palmieri) or to assist by increasing a decision maker’s ability to acquire, transform, and explore knowledge as envisioned by the IC. Technological assistance in providing the right amount and type of knowledge to decision makers has the potential to improve decisions, increase decision timeliness, and decrease staff support requirements. Given the lack of intelligence specialists in NTR disciplines outside of law enforcement, and the fact that 79 percent of police departments have twenty-five or fewer sworn officers, technology support is critical if we are to effectively engage NTR in homeland security.<sup>22</sup>

Intelligence products with CBF can function as a critical hub or node in networking multiple databases of open source contextual background and NTR; the producer (expert) manages the interface between the warehouses and NTR through the selection of appropriate hyperlinks. The diagram below outlines the impact of such hyperlinks on a small part of the homeland security information network.



**Homeland security information source network**

Understanding the critical importance of improving the usefulness of intelligence products for decision makers, the IC has utilized varied methods to provide user-defined access to contextual background for intelligence products, including personal briefings by intelligence professionals, ongoing feedback as part of the intelligence cycle, along with technological solutions such as a finished classified intelligence dissemination system (Intelink). The experience with Intelink highlights the importance of technology acceptance by decision makers; Intelink is a secure network of intelligence databases that supports user defined receipt of customized intelligence products.<sup>23</sup> It is intended to “provide robust and timely access to all available intelligence information, regardless of location, medium, or format, for all interested users...who are authorized access.”<sup>24</sup> Intelink was designed not to just “push” intelligence information; it allows recipients to “pull” information as well.<sup>25</sup>

Intelink has not been as successful as envisioned. Many intelligence recipients have expressed a preference for hard copies of reports, personal briefings, and traditional communication methods over Intelink.<sup>26</sup> As reflected in Technology Acceptance Model research, ease of use and perceived usefulness are significant factors in the successful implementation of any solution. Despite the extensive capabilities of Intelink, users “claim they go first to the Agency web sites, find no information at all, usually become quickly frustrated, and log off with the impression the intelligence agencies do not store information on Intelink.”<sup>27</sup> Intelligence system design must support the needs and preferences of decision makers or run the risk of rejection, regardless of how exceptional the technology or the potential of the system.

### **Technology Acceptance**

The theory of reasoned actions (TRA) serves as a theoretical base for examining technology acceptance.<sup>28</sup> TRA posits that an individual’s beliefs influence his or her attitudes that, when combined with societal norms, drive behavioral intentions, leading to actual behavior. Based on TRA, the technology acceptance model (TAM) is an established method of predicting user acceptance. In this model, perceived “ease of use” and perceived “usefulness” explain why individuals accept or do not accept technology.<sup>29</sup> A review of previous studies shows that TAM, with strong empirical support, has become a dominant model for predicting technology adoption.<sup>30</sup> TAM is one method to predict user acceptance before large scale investment or commitment to a technology in mission critical systems.

Of the two constructs, it appears that usefulness is critical; “no amount of ease of use can compensate for a system that does not perform a useful function.”<sup>31</sup> The use of technology in knowledge management systems has been studied using TAM to determine factors that impact loyal use; both perceived usefulness and ease of use were found to be factors positively related to loyal use.<sup>32</sup>

### **HYPOTHESIS**

- H<sub>1</sub>: CBF increases customer satisfaction “value” for NTR as defined by DHS/FBI.
- H<sub>2</sub>: CBF increases customer satisfaction “quality” for NTR as defined by DHS/FBI.
- H<sub>3</sub>: NTR find hyperlink technology applications in unclassified intelligence as “easy to use” as defined by technology acceptance model research.

- H<sub>4</sub>: NTR perceive hyperlink technology applications in unclassified intelligence as “useful” as defined by technology acceptance model research.
- H<sub>5</sub>: Given a choice, NTR believe a CBF intelligence document is of greater value to themselves and their organization than a non CBF product.

### **Hypothesis Testing**

A null hypothesis (H<sub>0</sub>) is a hypothesis that can be statistically examined. It is presumed to be true until statistical analysis demonstrates it to be false, or nullified, in which case the alternative hypothesis (H<sub>1</sub>) may be accepted. A null hypothesis can be designed to test that there is no difference between variables; it is then evaluated and the results examined to determine what the probability is that observed differences between variables are by chance. In determining whether to reject the null hypothesis in favor of the alternative hypothesis, we must determine an appropriate level of significance that must be met to reject the null hypothesis. The smaller this p-value is, the more significant the result; 5% or .05 is generally accepted as significant, while 1% or .01 is more statistically powerful, as it is a much more difficult threshold to meet. In this article the following two null hypotheses are evaluated to determine whether to accept the alternative hypothesis:

#### *Value*

H<sub>0</sub>: There is no difference in intelligence product perceived value as represented by DHS/FBI customer satisfaction surveys, on average, with the application of CBF.

H<sub>1</sub>: An intelligence product with hyperlinks to open source contextual background is perceived as more valuable based on DHS/FBI customer satisfaction surveys than a non-CBF product, on average.

#### *Quality*

H<sub>0</sub>: There is no difference in intelligence product perceived quality as represented by DHS/FBI customer satisfaction surveys, on average, with the application of CBF.

H<sub>1</sub>: An intelligence product with hyperlinks to open source contextual background is perceived as higher quality based on DHS/FBI customer satisfaction surveys than a non-CBF product, on average.

### **METHODOLOGY**

A control product was presented and a base measurement of DHS/FBI quality and value factors was established. The experimental CBF product was presented and a second measurement of DHS/FBI quality and value factors was recorded, establishing the positive or negative impact of CBF on the customer satisfaction factors established by DHS/FBI. Questions from previously validated technology acceptance model factors of ease of use and usefulness were then presented in order to determine if intelligence recipients would accept hyperlinks to achieve CBF. A final forced choice question to determine preference for control or experimental products was presented to confirm DHS/FBI factor results.

## Instrument Construction

Two identical sample intelligence products were produced for the survey: one text file as similar as practical to a typical intelligence product distributed to non traditional recipients and a second identical product fused with hyperlinks to contextual background (CBF). The material in the sample report was unclassified, having been adapted from the Southern Poverty Law Center Intelligence Project Eco-Radicalism, open source, online report, allowing this research to remain unclassified.<sup>33</sup> The intelligence sample product was distributed to four intelligence subject matter experts from local, county, state, and federal jurisdictions and based on their feedback the sample was shortened.

The survey was prepared for “Zoomerang” online distribution. A standard intelligence product was presented; seven questions were asked that mirror DHS/FBI value and quality surveys, then a CBF intelligence product was presented along with the same seven questions. These questions provide direct feedback to DHS/FBI on the impact of CBF on the exact measures that they seek from their “customers.” These questions utilized the same five-point Likert scale as DHS/FBI products, with Strongly Disagree on one end and Strongly Agree on the other end, along with an N/A option. One question from the DHS/FBI Customer Satisfaction Survey regarding timeliness was not utilized – “The product was delivered within established guidelines” – as the sample product was not being delivered based on guidelines. All other customer satisfaction survey questions and Likert scale are exactly as found in DHS/FBI documents.

Twelve additional questions directly related to ease of use and usefulness consistent with the Technology Acceptance Model (TAM) were then presented. A factor analysis was conducted to verify that the questions within ease of use and usefulness factors moved together and were in fact measuring distinct factors. The twelve additional questions were adapted from Technology Acceptance Model research first validated by Davis in 1989. In this model, the two factors of “Usefulness” and “Ease of Use” have been demonstrated to predict the use of technology.<sup>34</sup> The questions in these factors utilized an ordinal Likert 6-point scale with Strongly Disagree at one extreme and Strongly Agree at the other end. A final question in the survey asked respondents to directly identify whether a CBF or standard product would be of greater value to their organization.

The pilot study was sent to fifteen subject matter experts in public health, fire, emergency management, and law enforcement who suggested a “header” and “legalistic sounding disclaimer” to make the survey look more realistic, as well as changing one jurisdiction choice from “city” to “local.” After making these adjustments, the survey was distributed to the target audience, who were requested to complete the survey and forward the survey to other homeland security professionals. As this research utilizes customer satisfaction survey questions from DHS and the FBI, a bifurcated sampling method was utilized. In one frame invitations to participate in the survey were emailed to current and former students of the DHS-sponsored Center for Homeland Defense and Security (CHDS). These students, all of whom were selected by DHS to attend the school, include diverse homeland security disciplines including police, fire, public health, military, EMS, and emergency management. This sampling frame is intended to represent intelligence recipients of interest to DHS. As every current and former student was invited to participate, these students represent the entire universe of CHDS students and no further sampling was needed to survey this population.

A second sampling frame consisted of former students of the FBI National Academy (FBINA). Similar to the CHDS program, each student attending the FBINA is sponsored and selected by one of the fifty-six FBI Field Offices. Each student attending the FBINA is a member of law enforcement, representing local, county, state, and international jurisdictions. By 2005, over 38,000 students from 220 sessions had attended FBINA, so further sampling was required. Several domestic students from FBINA session 214 were selected to represent intelligence recipients of interest to the FBI. A total of 172 email invitations to participate in the survey were sent to current and former homeland security professionals sponsored by the FBI or DHS to attend these courses. Snowball-style secondary distribution by these initial recipients was encouraged.

### ***DHS/FBI Customer Satisfaction Survey Questions***

#### Quality:

1. The product was timely and relevant to your mission, programs, priorities, or initiatives.
2. The product was clear and logical in the presentation of information with supported judgments and conclusions.
3. The product is reliable; i.e., sources well documented and reputable.

#### Value:

1. The product would contribute to satisfying intelligence gaps or predicating cases or intelligence operations, especially previously unknown areas.
2. The product would result in a change in investigative or intelligence priorities and/or a shift from unaddressed to addressed work, or vice versa.
3. The product would result in more informed decisions concerning investigative or intelligence initiatives and/or resource allocation.
4. The product would identify new information associated with pending matters or offered insights into information that could change the working premise in a program or initiative.

### ***Technology Acceptance Model***

#### Perceived usefulness:

1. Using the intelligence product with hyperlinks in my job would enable me to accomplish tasks more quickly.
2. Using intelligence products with hyperlinks would improve my job performance.
3. Using intelligence products with hyperlinks would increase my productivity.
4. Using intelligence products with hyperlinks would enhance my effectiveness on the job.
5. Using intelligence products with hyperlinks would make it easier to do my job.
6. I would find intelligence products with hyperlinks useful in my job.

#### Perceived ease of use:

1. Learning to utilize intelligence products with hyperlinks would be easy for me.
2. I would find it easy to use intelligence hyperlinks to obtain decision-making information.
3. My interaction with the intelligence product with hyperlinks was clear and understandable.

4. I found the intelligence hyperlinks to be flexible to interact with.
5. It would be easy for me to become skillful at using intelligence products with hyperlinks.
6. I found the intelligence product with hyperlinks easy to use.

### **Preference**

1. Which type of intelligence product would be of greater value to you and your organization?

The data obtained from the online survey was downloaded into a Statistical Package for the Social Sciences (SPSS) program for descriptive, bivariate, multivariate, correlation, regression, and reliability analysis.

## **SURVEY FINDINGS**

### **Demographics**

The sample contained 285 responses. Six discipline choices were offered in the survey; law enforcement was the largest single represented discipline with 35.1 percent of responses. Six jurisdictions were represented; the largest single jurisdiction was local respondents at 41.1 percent. The largest single discipline/jurisdiction respondent combination was local law enforcement, with fifty individual responses or 17.5 percent of total respondents, followed by local fire at 14.4 percent.

### **Perceived Value and Quality**

The Wilcoxon test conducted examines the hypothesis that there is no difference in perceived quality and value between standard and CBF products. This was not the case; the observed increased perception in both value and quality was statistically significant and would occur fewer than once every thousand times if there really was no difference in perceived quality or value. While not included in the original hypothesis, the Wilcoxon test on each of the seven questions comprising the DHS/FBI quality and value measures would occur fewer than once every thousand times if there really were no difference between the standard and CBF products. The CBF product was rated higher by an overwhelming margin, from three to sixteen times higher on individual variables.

Reject  $H_0$ : There is no difference in intelligence product perceived value as represented by DHS/FBI customer satisfaction surveys, on average, with the application of CBF to open sources in favor of  $H_1$ . An intelligence product with CBF to open sources is perceived as more valuable based on DHS/FBI customer satisfaction surveys than a non-CBF product, on average.

Reject  $H_0$ : There is no difference in intelligence product perceived quality as represented by DHS/FBI customer satisfaction surveys, on average, with the application of CBF to open sources in favor of  $H_1$ . An intelligence product with CBF to open sources is perceived as higher quality based on DHS/FBI customer satisfaction surveys than a non-CBF product, on average.

### **Conclusions: Technology Acceptance**

With a mode of five of six on every question, respondents showed overwhelming acceptance of hyperlink technology.

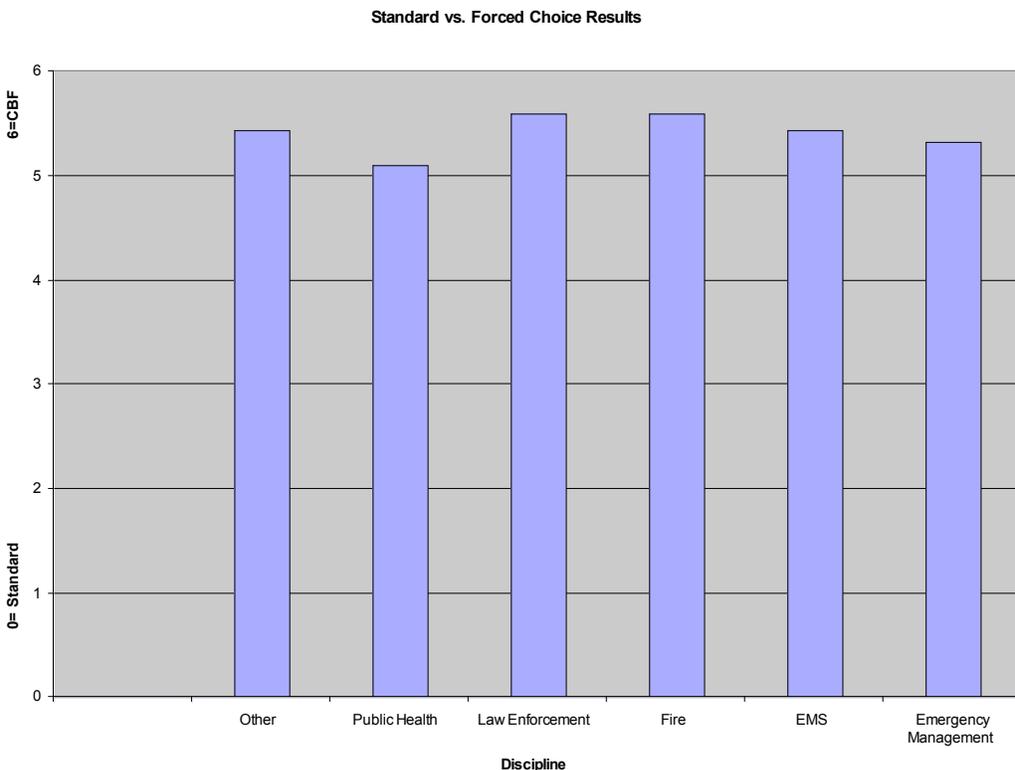
### Standard vs. CBF Forced Choice Results

The final Likert question, “Which type of intelligence product would be of greater value to you and your organization?” represented a direct choice for subjects between CBF and standard unclassified intelligence products. Of respondents, 65.8 percent indicated the strongest possible preference for the hyperlinked option offered, producing both a median and mode of six with a mean of 5.45. This indicates that, given a choice, homeland security professionals overwhelmingly preferred the CBF product.

Although variation between disciplines is to be expected, all disciplines and jurisdictions uniformly preferred the CBF product with means ranging from 5.1 to 5.67 on the six-point Likert scale with law enforcement, fire, local, and private sector respondents showing the strongest preference for the CBF product.

Jurisdiction	Greater Value
Other	5.38
Federal	5.49
State	5.41
County	5.13
Local	5.57
Private Sector	5.67
Total	5.45

Discipline	Greater Value
Other	5.43
Public Health	5.10
Law Enforcement	5.60
Fire	5.59
EMS	5.43
Emergency Management	5.33
Total	5.45



## Analysis

CBF has been demonstrated to be one tool that can assist in meeting the demands and recommendations of the Markle Foundation, NTR, the 9/11 Commission, California Police Chiefs, DHS, Major City Police Chiefs, the CIA, the National Strategy for Homeland Security, the National Infrastructure Advisory Council, and the RAND Corporation. CBF of unclassified intelligence for NTR contributes toward:

- “...news...in context.” (9/11 Commission)<sup>35</sup>
- “...adequate context for homeland security providers to effectively utilize information...specific, tailored for each local entity, rapidly disseminated, and does not overburden recipients with vague or irrelevant information.” (Markle Foundation)<sup>36</sup>
- Improves law enforcement perception of intelligence quality and value. (California Police Chiefs)<sup>37</sup>
- Is a “better method of sharing intelligence with state and local law enforcement agencies?” (DHS)<sup>38</sup>
- Contributes toward providing “adequate...background...for 700,000 officers on the street.” (Major City Police Chiefs)<sup>39</sup>
- “...Harness(es) the power of information technology...” (Markle Foundation)<sup>40</sup>
- Provides “background and contextual information available at...policymaker’s fingertips in a timely fashion...” (CIA)<sup>41</sup>

- Moves toward “full integration of (the) private sector into the intelligence cycle.” (National Infrastructure Advisory Council)<sup>42</sup>
- Encourages “effective partnership with state and local government and the private sector...” (National Strategy for Homeland Security)<sup>43</sup>
- Is “tailored to meet requests from government departments, police, and private industry.” (RAND)<sup>44</sup>

Research has found that even well-educated decision makers who understand the power of statistical testing often rely on analogies or metaphors to change deeply held beliefs; analogical reasoning combined with statistical analysis is more effective in changing those beliefs than statistics alone.<sup>45</sup>

One contextual metaphor/urban legend about the FBI describes how J. Edgar Hoover demanded short memos with wide margins (in order to make notations), then received a memo with narrow margins. He promptly returned the memo with the notation, “Watch the borders.” Subordinates promptly sent hundreds of agents to guard our national borders with Canada and Mexico!

Whether it is as expensive as sending hundreds of agents to the borders, or as critical as meeting the unclassified intelligence needs of millions of homeland security professionals, context matters. This research demonstrates that through CBF it is practical for the Intelligence Community to provide NTR the context required to make good decisions. Context that is consistent with the hermeneutic of the originating agency, is immediately available to decision makers, is “fused” to keywords, is available to over 87,000 jurisdictions, improves both quality and value of intelligence products, and utilizes technology that is widely accepted.

## **LIMITATIONS OF RESEARCH**

The original list of survey recipients, although geographically diverse, was based on two advanced educational programs, which may introduce bias in the results; these professionals had attended the FBI National Academy or the Naval Postgraduate School Center for Homeland Defense and Security. As DHS and the FBI jointly distribute unclassified intelligence products, and the questions utilized in the survey were in part based on their joint customer satisfaction survey, it is believed that sending the survey to students of a DHS-sponsored and FBI-sponsored program would represent a reasonable target audience for DHS/FBI intelligence products. Original distribution may not adequately represent the technological diversity of homeland security professionals, given the online format of NPS CHDS and leadership positions of FBINA graduates. Pilot study subject matter expert (SME) feedback, participant free-form comments, and demographic results reflect stronger ecological validity than external validity; while the survey was originally widely distributed, the anonymous nature of feedback and low frequency of individual jurisdiction/discipline responses demands caution interpreting individual discipline and jurisdiction results.

The “snowball” distribution style, where those who were originally requested to participate were encouraged to redistribute to their homeland security contacts, reduces validity, while increasing sample size. This distribution style can introduce bias as it reduces the likelihood that the respondents represent an appropriate population sample. Secondary distribution by these recipients, not controlled by the researcher, was

intended to similarly represent the target audience of the DHS and the FBI; the extent to which this sample does not represent the target audience of these agencies represents potential bias in the survey results.<sup>46</sup>

As the survey responses were anonymous, recipients who visited the site or only partially completed the survey, then came back to complete the survey, registered as a visit, a partial, and a complete response. Therefore only completed survey data were utilized for research, and the resulting visit/partial/complete response rates are not utilized. 285 Total surveys completed were 285, 182 partial responses were not utilized, and the website was visited a total of 648 times. From this data, the response rate may have been anywhere from 44 to 100 percent. Not knowing the true response rate is a limitation in this research.

The sample was derived from DHS- and FBI-sponsored educational programs that do not generally include private sector participants. As a result, the two million private-sector security professionals are under-represented in this research.

## **RECOMMENDATIONS**

Research has outlined the critical impact of context on decision making, the importance of intelligence in homeland security, the need to involve millions of diverse homeland security professionals in asymmetric conflict, and the importance of technology in intelligence operations. Statistical analysis of the data indicates that hyper linking unclassified intelligence products to open source contextual background (CBF) increases the perceived value and quality of that intelligence. Given a choice, homeland security professionals overwhelmingly preferred a CBF product, 268 to sixteen. Observed increases in perceived value and quality and clear preference for CBF in intelligence products make it clear that CBF positively impacts information sharing as demanded by national directives, initiatives, and homeland security professionals. Strong ease of use and usefulness findings across disciplines and jurisdictions predict that NTR will use this technology if employed in unclassified intelligence production and distribution. In order to improve information sharing to and between NTR as demanded, the following recommendations should be considered.

First, the Office of the Program Director for the Information Sharing Environment and unclassified intelligence producers with the capability should immediately fuse vetted, accurate, open source contextual background to their intelligence products through the use of hyperlink technology. The newly created Federal Coordinating Group (FCG) at the National Counterterrorism Center provides a timely opportunity to introduce CBF into unclassified intelligence distributed nationwide.

Homeland security professionals have expressed acceptance of hyperlink technology in unclassified intelligence distribution. Intelligence producers such as NYPD have successfully integrated other technologies such as PowerPoint into unclassified intelligence production and advanced contextual background technology such as "Intelink," "K2," "Profiler," and "Autonomy" are successfully used in classified intelligence systems in order to reduce the time it takes for analysts to identify links and discover previously unidentified links. In order to eliminate or minimize the time it takes for analysts to identify appropriate hyperlinks for use in CBF, search criteria that limits responses to .mil, .gov, and websites previously identified as accurate and credible can be shared between analysts. Whether through technology or shared resources, the time required to identify appropriate hyperlinks must be minimized so that it is equal to

or less than the time saved by the production of a one page CBF product versus a longer standard product. This DHS-sponsored research has demonstrated the acceptance of technology across a broad range of homeland security disciplines and the effectiveness of TAM in evaluating technology prior to widespread homeland security application.

Second, DHS should immediately sponsor research to determine what other technologies, including contextual background systems such as K2, Profiler, Autonomy, and community-of-interest search systems, would be acceptable and improve perceived value and quality in unclassified intelligence products. Technology that is found useful and easy to use should be considered for widespread application to improve information sharing.

This research has demonstrated that statistically significant improvements in DHS/FBI-defined perceived value and quality factors, along with strong TAM ease of use and usefulness factor ratings, are possible with the addition of open source contextual background to unclassified intelligence. NTR found the simple addition of contextual background to unclassified intelligence improved that intelligence, contributing to improved information sharing as demanded by national directives, initiatives, and homeland security professionals.

Third, the Department of Homeland Security should sponsor research into what other information, data, or intelligence components would improve perceived quality and value of unclassified intelligence products for NTR. The preferred length of unclassified intelligence, the optimal amount of contextual background, the inclusion of sources for further information, citations, and the fusion of related online training to unclassified intelligence products are examples of changes to unclassified intelligence that should be evaluated utilizing TAM.

The regional fusion center concept has demonstrated an ability to coordinate multiple disciplines in counter terrorism efforts.

Finally, the Department of Homeland Security should continue to support the fusion center concept, encouraging the use of these centers to “tailor” intelligence to the unique needs of their multidisciplinary partners and geographic areas of responsibility, consistent with study recommendations. Additionally, DHS should sponsor research into additional methods of geographic “tailoring” of unclassified intelligence.

*Charles (Chuck) Eaneff is a retired deputy chief with the Sunnyvale Department of Public Safety, a fully integrated public safety agency providing police, fire and EMS services in the heart of the Silicon Valley, California. Mr. Eaneff has served as both the chief of Fire Services and the chief of Police Services, reporting to the Director of Public Safety. Over the course of his career, he has worked in every area of public safety with extensive opportunities to work jointly with multiple disciplines and federal agencies on local, national, and international criminal and national security investigations. Mr. Eaneff possesses undergraduate degrees in Psychology and Criminal Justice/Industrial Security, is a graduate of the FBI National Academy and received a Master of Arts in Security Studies from the Naval Postgraduate School in March 2007. Mr. Eaneff can be reached at [ceaneff@comcast.net](mailto:ceaneff@comcast.net).*

- 1 *National Strategy for Information Sharing* (Washington, D.C.: General Accounting Office, 2007), 17.
- 2 Zoë Baird, *Creating a Trusted Network for Homeland Security* (New York: The Markle Foundation, 2003), 119.
- 3 Thomas Kean, et al., *The 9/11 Commission Report* (Washington, D.C.: General Accounting Office, 2004), 119.
- 4 U.S. Department of Justice, *The National Criminal Intelligence Sharing Plan* (Washington, D.C.: General Accounting Office, 2003), vi.
- 5 Maryam Alavi, "An Assessment of the Concept of Decision Support Systems as Viewed by Senior-Level Executives," *MIS Quarterly* 6, no. 4 (December 1982): 1-9.
- 6 United States State Department, *Did a Plane Hit the Pentagon?* (Washington, D.C.: Department of State, 2005), 1.
- 7 George W. Bush, *The National Security Strategy of the United States of America* (Washington, D.C.: Government Printing Office, 2002), vii.
- 8 *State and Local Law Enforcement Statistics* (Washington, D.C.: Bureau of Justice Statistics, 2006), 1; Association of State and Territorial Health Professionals, *State Public Health Worker Employee Shortage Report, A Civil Service Recruitment and Retention Crisis* (Washington, D. C.: ASTHO.org, 2005), 3; *Federal Law Enforcement Statistics* (Washington, D.C.: Bureau of Justice Statistics, 2006), 1.
- 9 Ibid.
- 10 Ibid.
- 11 Frank Ravitch, "Struggling with Text and Context: A Hermeneutic Approach to Interpreting and Realizing Law School Missions," *St. Johns Law Review* (2000): 5.
- 12 John Hillen, "Know Nothings: U.S. Intelligence Failures Stem from Too Much Information, Not Enough Understanding," *National Review* 8, no. 3 (1998), 1
- 13 Kerr et al., *Intelligence and Analysis on Iraq: Issues for the Intelligence Community* (Washington, D.C.: The Kerr Group, 2005), 1.
- 14 Peter Pirolli, *Assisting People to Become Independent Learners in the Analysis of Intelligence* (Palo Alto, CA: Office of Naval Research, 2006), 38.
- 15 Lisa Palmieri, *Information vs. Intelligence: What Police Executives Need to know* (Massachusetts: IALEIA, 2005), 1.
- 16 H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Managers' 'Pandering,'" in *Strategic Intelligence: Windows into a Secret World*, Loch Johnson and James Wirt zeds. (Los Angeles, CA: Roxbury Publishing Company, 2004), 198.
- 17 Jean-Charles Pomerol and Patrick Brézillon, *Proceduralization of the Contextual Knowledge for Decision Making*, Abstract (Luxembourg; Proceedings of the HCP-2003, the 14<sup>th</sup> Mini-Euro Conference on Human Centered Processes, 2002), 139-147.
- 18 Ibid.
- 19 North Atlantic Treaty Organization (NATO), *Tactical Decision Aids and Situational Awareness* (Amsterdam: NATO, 2002), 14.
- 20 Fathali Moghaddam, *From the Terrorists' Point of View What They Experience and Why They Come to Destroy* (London: Prager Security International, 2006), 11.
- 21 Robert Steele, *The New Craft of Intelligence Personal, Public and Political* (Oakton, VA: OSS International Press, 2002), 154.

- 22 Geoffrey Alpert, *Police Pursuit and the Use of Force. A Final Report to the National Institute of Justice* (Washington, D.C.: National Criminal Justice Reference Service, 1997), 7.
- 23 Lorne Teitelbaum, *The Impact of the Information Revolution on Policymakers' Use of Intelligence Analysis* (Santa Monica, CA: RAND, 2005), 98.
- 24 Frederick Martin, *Top Secret Intranet: How U.S. Intelligence Built Intelink – the Worlds Largest Most Secure Network* (Upper Saddle River, NJ: Prentice Hall, 1999): foreword.
- 25 Patrick Kelly, *Intelligence Support to Homeland Security: Supporting the Supporting Effort* (Carlisle Barracks, PA: U.S. Army War College, 2002), 29.
- 26 Teitelbaum, *Impact of the Information Revolution*, 101.
- 27 Ibid., 106.
- 28 M. Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research* (Reading, MA: Addison-Wesley, 1975), 21-52.
- 29 F.D. Davis, R.P. Bagozzi, and P.R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* 35, no. 8 (1989): 982-1003.
- 30 Chiening Lin, et al., *Examining User Acceptance of COPLINK Technologies by Law Enforcement Officers: A Survey Study* (Tempe, AZ: University of Arizona, 2002), 2.
- 31 Davis et al., "User Acceptance of Computer Technology," 333.
- 32 Paul Clay, Alan Dennis, and Dong-Gil Ko, *Factors Affecting the Loyal Use of Knowledge Management Systems* (Bloomington, IN: Indiana University, 2005), 1-10.
- 33 Southern Poverty Law Center, *Eco-Radicalism, Feds Across Country to Smash 'Eco-Terrorists'* (Montgomery, AL: Southern Poverty Law Center, 2005), 1.
- 34 Davis et al., "User Acceptance of Computer Technology," 982-1003
- 35 Kean et al, The 9/11 Commission Report. 119.
- 36 Baird, *Creating a Trusted Network for Homeland Security*. 56.
- 37 Patrick Miller, *How Can We Improve Information Sharing Among Local Law Enforcement Agencies*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 2005.
- 38 *Department of Homeland Security Appropriations Act, 2007*, H.R. 5441, 109, 2, July 17, 2006, S7632, [https://www.chds.us/courses/file.php/112/moddata/forum/742/13414/DHS\\_Approp\\_Bill.txt](https://www.chds.us/courses/file.php/112/moddata/forum/742/13414/DHS_Approp_Bill.txt) (accessed August 22, 2006).
- 39 Edward Tully, *Terrorism the Impact on State and Local Law Enforcement* (Alexandria, VA: International Association of Chiefs of Police, 2002), 5, <http://www.neiassociates.org/mccintelligencereport.pdf> (accessed September 2, 2006).
- 40 Zoë Baird, *Protecting America's Freedom in the Information Age* (New York, New York: The Markle Foundation, 2002), 15, <http://knxup2.ad.nps.navy.mil/homesecc/docs/nonprof/nps05-070903-01.pdf> (accessed February 2, 2006).
- 41 Kerr et al., *Intelligence and Analysis on Iraq: Issues for the Intelligence Community*, 1.
- 42 Chambers, John, and Erie Nye. Letter to George Bush from the National Infrastructure Advisory Council, Edited by George W. Bush. Washington, D.C.: The National Infrastructure Advisory Council, 2004. [http://www.dhs.gov/interweb/assetlibrary/NIAC\\_EEIS\\_Letter\\_0804.pdf](http://www.dhs.gov/interweb/assetlibrary/NIAC_EEIS_Letter_0804.pdf) (accessed 1/24/2006).
- 43 George W. Bush, *National Strategy for Homeland Security* (Washington, D.C.: Office of Homeland Security, 2002), 5-6.

44 Peter Chalk, Seth Jones and William Rosenau, *Understanding the Enemy: Lessons for Effective Threat Assessments* (Santa Monica, CA: RAND, 2004), 9.

45 Thomas Nagy, Theresa Jefferson, and Jamal Altorkistani, *Selling Proven Methods for Improving the Usability of the Web: Experimental Evidence of the Benefits of Metaphors for Supporting Heuristic Evaluation* (Washington, D.C., George Washington University 2006), 1

46 *Survey Sampling Methods* (Bloomington, Minnesota, Stat Pac, 2006), 1