Activity-Based Target Acquisition Methods for Use in Urban Environments

Kimberly Myles

Dissertation submitted to the faculty of the Virginia
Polytechnic Institute and State University in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy
In
Industrial and Systems Engineering

Dr. Tonya L. Smith-Jackson, Chair
Dr. Kari L. Babski-Reeves
Dr. V. Grayson CuQlock-Knopp
Dr. Joel T. Kalb
Dr. Woodrow W. Winchester

July 7, 2009
Blacksburg, Virginia

KEY WORDS: nonverbal behavior; covert mischievous intentions; threat detection; urban environment; MOUT; judgment and decision making

Activity-Based Target Acquisition Methods for Use in Urban Environments

Kimberly Myles

ABSTRACT

Many military conflicts are fought in urban environments that subject the U.S. soldier to a number of challenges not otherwise found in traditional battle. In the urban environment, the soldier is subject to threatening attacks not only from the organized army but also from civilians who harbor hostility. U.S. enemies use the civilian crowd as an unconventional tactic to blend in and look like civilians, and in response to this growing trend, soldiers must detect and identify civilians as a threat or non-threat. To identify a civilian as a threat, soldiers must familiarize themselves with behavioral cues that implicate threatening individuals. This study elicited expert strategies regarding how to use nonverbal cues to detect a threat and evaluated the best medium for distinguishing a threat from a non-threat to develop a training guide of heuristics for training novices (i.e., soldiers) in the threat detection domain. Forty experts from the threat detection domain were interviewed to obtain strategies regarding how to use nonverbal cues to detect a threat (Phase 1). The use of nonverbal cues in context and learning from intuitive individuals in the domain stood out as strategies that would promote the efficient use of nonverbal cues in detecting a threat. A new group of 14 experts judged scenarios presented in two media (visual, written) (Phase 2). Expert detection accuracy rates of 61% for the visual medium and 56% for the written medium were not significantly different, F (1, 13) = .44, p = .52. For Phase 3 of the study, a training development guide of heuristics was developed and eight different experts in the threat detection domain subjectively rated the heuristics for their importance and relevance in training novices. Nine heuristics were included in the training guide, and overall, experts gave all heuristics consistently high ratings for importance and relevance. The results of this study can be used to improve accuracy rates in the threat detection domain and other populations: 1) the soldier, 2) the average U.S. citizen, and 3) employees of the Transportation Security Administration.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

First, before any other, I would like to give thanks to my heavenly Father, to whom I owe this accomplishment. Truly, without Him, obtaining this degree would not have been possible. Through the dark paths of this process, God was always there to remind me that impossible is not of His agenda. The process of obtaining this degree has been long and challenging and sometimes almost a struggle, but through the journey I have learned so much about God, myself, and life. I have gained much more patience. I have learned to wait on God when He says "Not Yet My Child". I have found new purposes in life and really do understand that I must live my life on purpose. Thank you God, for I have lived through in order to be prepared for where you are taking me.

Thank you Mom and Dad for being the best parents a girl could have. I love you and thank you for encouraging my dreams and making it known that if I put my mind to it, I can achieve it. Mom, you are the best and believe me when I tell you I would "choose" you again if I had a choice. Dad, no matter what it was, I am so used to looking up and seeing you there. So the only thing I regret about this moment is that you are not here to see it, but I am sure you are looking down upon me, saying, "I'm proud". I love you Christina for being my "unique" sister. Thank you for your words of support and knowing when to lighten it up at just the right time…ok, maybe not, but never change because you are the best.

Thank you to the members of my committee for your scholarly guidance and enduring support. Thank you to my chair, Dr. Smith-Jackson, for lending an ear to more than the frameworks and theories and for your ability to advise without suppressing creativity. It is rare, but you are truly great at seeing solutions from different angles. Thank you, Dr. Babski-Reeves and Dr. Winchester, for offering your unique points of view, which were really helpful for the completion of this effort. To Dr. CuQlock-Knopp and Dr. Kalb, thank you for agreeing to be a part of this project. Your knowledge and perspectives in the area were helpful in bringing it full circle.

Thank you to the U.S. Army Research Laboratory for supporting this project. Also, I want to thank my immediate supervisors for helping me to complete this project in the later stages. The support was greatly appreciated.

Nancy: Thank you for lending your editing expertise to this project and thank you for your patience through the many versions of this document.

To the KPPS Dissertation Support Group: When we formed the group, I do not think any one of us knew the impact it would have on us. We were four phenomenal African-American women on a similar path: working to obtain the Ph.D. in ABD status. We provided each other encouragement, advice, and wisdom during the high and low points of the process. During many support group meetings, we shared similar revelations about the profound impact that the dissertation process can have on both the professional and personal life. We all realized, however, that through it all, the strength of God was our balancing factor and that He was the orchestrator of our individual experiences in the process, and so we embraced the process and knew that it was our destiny to be where we were in order to be prepared for the places we were going. Dr. Pam Love, Dr. Pam Smith, and Dr. Sharon Duncan Jones-Eversley, I love you all and thanks for sharing in a piece of the journey.

Grayson, thanks for the many years you have devoted to being a great mentor. I have seen the effort and passion you put into mentoring young people and not many people would give that level of effort on a daily basis. You truly care about the educational opportunities for young people and for that you have truly inspired me to live my life doing the same. You have a genuine spirit that could only come from God just like the "Favor" I have seen bestowed upon your life.

Latrice: Although you did not know what the journey entailed, you knew it was something within reach. Joshua, Laila, and Lindsay: thank you for offering time away for a break. Linda: thanks for the many words of encouragement over my lifetime. Carolyn: thank you for the encouraging perspectives regarding the will of God. Ms. Georgia: thanks for the many conversations about life lessons and the future. Charneta: thanks for never getting tired of

listening (at least you didn't let me know) to my frustration during that one-hour drive to work and home. Kayenda: you are truly an optimist, never change. Charneta, Kayenda, LaTanya, Ryan, and Tom: thanks for the good food and fellowship in Blacksburg. To my Emmanuel family: I appreciate your concerns and help during this process.

Thank you to all my family and friends who offered encouraging words and support during this process. You will never know how much those words meant.

1. INTRODUCTION

Because of its expanding role, the United States (U.S.) military is no longer being used for the sole purpose of conducting war. The military's role now includes nontraditional missions in hopes of maintaining world order (Department of the Army, 2006). The U.S. military defines non-traditional missions as "military operations other than war" (MOOTW), which includes humanitarian assistance, peace-keeping operations, recovery operations, combating terrorism, counter-drug operations, and support of civil authorities (Department of the Navy, 1998, p. 7-1). Most MOOTW missions are conducted within an urban environment, and missions (including urban warfare) that are conducted in urban environments are referred to as "military operations on urbanized terrain" (MOUT) (Brown, 1997; Dupont, 1998; Glenn, 1999; Grau & Kipp, 1999). Therefore, all military missions conducted in an urban or city environment fall under the category of MOUT.

Urban environments, characterized by large civilian populations, present a significant challenge to the U.S. soldier (Department of the Army, 2002, 2006) where infantry soldiers may be surrounded by civilians while engaged in mission tasks and duties. Most civilians can be considered noncombatants and harbor no hostile intentions. However, there are a growing number of civilians who are willing to commit hostile acts toward American soldiers. In response to this growing trend, soldiers must now detect and identify civilians as a threat[1] or non-threat to protect themselves and other innocent civilians. This becomes difficult because civilians are not affiliated with an organized military entity and do not wear uniforms bearing visible military insignia. In the absence of this, soldiers must shift their focus from the

[1] Threat is defined as an observer's judgment of potential danger using indicators of harmfulness (Russell, Russell, & Benke, 1996). Specific indicators of harm that are pertinent to this research include covert actions, behaviors, and activities that would implicate someone as a threat.

traditional characteristic of a civilian (i.e., non-insignia = noncombatant and non-threat) to the behavioral characteristics that civilians display. Therefore, to identify a non-insignia civilian as a threat, soldiers must familiarize themselves with behaviors that implicate threatening individuals and must learn the strategies regarding the use of nonverbal behaviors to detect a threat.

Chapter 1 further discusses the soldier's problem of identifying threatening civilians in urban environments and how the current military tool for identifying civilian threat is ineffective. The frameworks that guide the solutions to the research problem and the purpose and objectives of the research are identified. Chapter 2 includes background regarding the research problem abroad (i.e., MOUT) and here at home (i.e., within U.S. borders). The chapter also includes literature relevant to solving the research problem, such as the research frameworks and the factors that may influence one's ability to identify a threat. Chapters 3, 4, and 5 focus on methodology for designing tools to solve the soldier's problem of civilian classification. Chapter 3 specifically discusses the collection of strategies that facilitate decisions about threats. Chapter 4 reports threat detection accuracy rates for experts in the threat detection domain. Chapter 5 discusses the development of a training development guide containing heuristics that training personnel in the domain of threat detection can employ to develop training for the novice in the domain. Domain expert ratings for importance and relevance for the heuristics in the training development guide are also reported. Chapter 6 discusses key findings regarding the underlying strategies and factors that influence one's ability to detect threats and the promising role of training in helping to improve threat detection rates for the novice. Chapter 6 also includes areas in which the developed tools would be beneficial and the potential for future research in threat detection.

1.1 Statement of Problem

The U.S. military's current approach for identifying a potential enemy is based on memory and association (Brister, 1997; MSG L. Garrett, personal communication, November 2003). During basic training, soldiers are provided with a "deck of playing cards" that display specific equipment features and military insignia of friendly and enemy militaries, and the soldier is expected to memorize the information contained on the playing cards (Brister, 1997; MSG L. Garrett, personal communication, November 2003). During times of conflict, soldiers are expected to retrieve the above information from memory and associate equipment features with a threat or non-threat. When asked, MSG L. Garrett (personal communication, November 2003) acknowledges that the current method only includes the recognition of threatening military materiel (e.g., tanks, aircraft) and contains no information for the identification of a human threat.

The most challenging aspect for soldiers when they are conducting missions in urban environments is the involvement of civilians (Dupont, 1998; Gerwehr & Glenn, 2000; Grau & Kipp, 1999; Groves, 1998; Peters, 2000). Because of the current hostility directed toward the United States from around the world, the U.S. soldier is subject to threatening attacks from civilians who harbor political hostility or have ties to the enemy (Peters, 2000). Thus, during urban warfare, soldiers must not only be concerned with the opposing army, but they must also focus on civilians with threatening intentions. Specifically, soldiers are exposed to attacks by insurgent civilians that involve suicide bombers and improvised explosive devices (IEDs) (Cockburn, 2005; Karadsheh & Damon, 2007; Partlow, 2008). There were 62 daily insurgent attacks in Iraq between February and June of 2005 and the number of daily attacks increased in

2006 and 2007 to 90 and 160, respectively, for the same reporting time period (O'Hanlon & Campbell, 2007). Of the insurgent attacks in Iraq, it is estimated that IED attacks are responsible for 75% to 80% of all U.S. soldier casualties (O'Hanlon & Campbell, 2007). In contrast to an opposing army, civilians are difficult to identify because they lack distinguishable displayed insignia, which has caused the soldier's current method (i.e., looking for visual military insignia) of civilian classification to become impractical. Therefore, the soldier's problem is stated: how does a soldier who has been trained to acquire (detect, recognize, identify) an enemy based on knowledge of visual military insignia, detect and identify a non-insignia civilian as threatening or non-threatening?

For soldiers to effectively use the current method to identify a threat, two variables must be defined: military materiel type and military insignia type. Civilian classification is not a variable considered in the current method of threat identification; therefore, the current method is not feasible. Since the greatest threat to "U.S. troops in Iraq remains makeshift bombs (e.g., IEDs),…, that are used to target soldiers on foot and in their vehicles" (Partlow, 2008), a better suited threat identification method to identify insurgent civilians is needed for use in the urban environment. A behavior-based identification method fits this criterion because it allows the soldier, particularly an infantry soldier who is a novice in threat detection, to classify civilians as a threat or non-threat based on behaviors.

1.2 Research Frameworks

This research is governed by two main theoretical frameworks: 1) target acquisition, and 2) nonverbal communication. Target acquisition, the process used to locate and discriminate a target, contains three phases: detection, recognition, and identification (O'Connor et al., 1996):

1) Detection: perceives an object within the visual field;
2) Recognition: categorizes the target into a functional and meaningful category;
3) Identification: describes exact details of the target.

Here we see the detection phase beginning with the acknowledgment that something is seen and progressing to the identification phase where a very detailed description of the object is given. For soldiers, the detailed description will include whether a civilian is threatening or non-threatening. In the military sector, the theory of target acquisition is mostly applied to aid in the detection and identification of military materiel systems or equipment (Vaughan, 2006) and not in the identification of humans (O'Connor et al., 1996).

The theory of nonverbal communication has been studied for many years and suggests that inferences can be made about an individual, based on behavior (Wiener, Devoe, Rubinow, & Geller, 1972). Physical characteristics, facial features, body build, gestures, behaviors, and posture are among some of the nonverbal cues recognized as being meaningful (Secord, Backman, & Slavitt, 1976). Research has shown that nonverbal information can assist in revealing one's attitudes, emotions, intentions, and motives (Baldwin & Baird, 2001; Gerwehr & Glenn, 2000; Secord et al., 1976). Baldwin and Baird (2001) clearly state the underlying importance of studying nonverbal communication.

> When we observe others in motion, we usually care little about the surface behaviors they exhibit. What matters are their underlying intentions. Judgments about intentions and intentionality dictate how we understand and remember others' actions, how we respond, and what we predict about their future action. (p. 171)

When target acquisition and nonverbal communication are integrated, a new concept labeled Activity-Based Target Acquisition (ABTA) is created. ABTA is defined as the act of detecting threatening individuals based on activities, actions, and behaviors (Figure 1). ABTA is

relevant to any situation in which an individual may be a possible threat and assumes that subtle behavioral cues can be used to identify the threat before the threat is apparent via an attack.

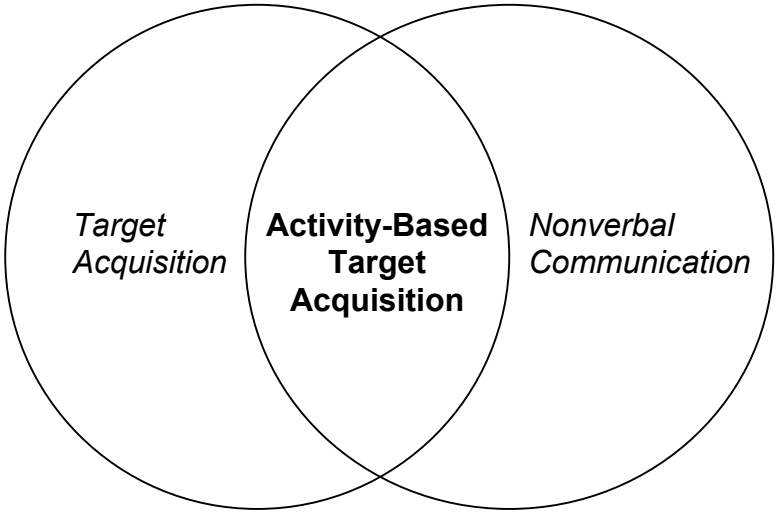


Figure 1. The relationship among Target Acquisition, Nonverbal Communication, and Activity-Based Target Acquisition.

1.3 Purpose of Research

The purpose of this research is to provide the soldier with an improved civilian classification method when s/he is conducting missions in an urban environment. This research uses the theoretical principles of nonverbal communication to advocate the use of behavior-based indicators of threat and to highlight threat detection strategies of the expert in the threat detection domain to improve the soldier's capability to identify a civilian threat. The behavior-based method developed in this research is called ABTA and is defined as acquiring or categorizing a human target (i.e., threat, non-threat) based on displayed behaviors. The use of and strategies

associated with the use of ABTA will impact the soldier in five ways. The soldier will be able to (1) detect and identify threatening behavior cues, (2) identify civilians as a threat or non-threat, (3) minimize the possibility of innocent civilians being injured or killed, (4) minimize the risk of death of oneself, and (5) increase the opportunity for successful completion of assigned MOUT missions.

1.4 Research Objectives

There are four objectives of this research. The first is to elicit expert strategies regarding how to use nonverbal cues to detect a threat. The second objective is to evaluate the best medium for distinguishing a threat from a non-threat and for highlighting threatening people and nonverbal cues that indicate an imminent threat. A third objective is to evaluate threat detection accuracy rates of experts in the threat detection domain. The fourth objective is to design a training development guide for training developers responsible for training the novice in the threat detection domain.

1.4.1 *Research Questions*

The first research question will examine if experts utilize specific strategies that are likely to assist in identifying someone as a threat among a civilian population.

This research effort will also answer the following:

2. How is threat detection accuracy affected by media presentation?
3. To what extent will experts be successful in identifying potential threat?
4. What do expert ratings of perceived importance and relevance reveal regarding the expert's opinion about how to train the novice in the threat detection domain?

1.4.2 *Research Hypotheses*

It is hypothesized that

1. The visual medium will be most effective for distinguishing a threat from a non-threat and for highlighting threatening people and nonverbal cues that indicate an imminent threat;

2. Experts in the threat detection domain will achieve threat detection accuracy rates significantly above 50%; and

3. A training development guide of heuristics for the development of threat detection programs for novices in the threat detection domain will be considered important and relevant by domain experts.

2. LITERATURE REVIEW

2.1 MOUT --- Urban Warfare: Soldiers' Need for ABTA

2.1.1 *How Did We Get Here?*

When people envision two countries at war, they may imagine the two countries going into rural, isolated, open-spaced land areas with military materiel to fight one another. People may not envision two countries at war in a populated city filled with innocent civilians. However, we are increasingly seeing war occurring in cities, which can be directly traced to increased urbanization (Department of the Army, 2002; Glenn, 1999; Grau & Kipp, 1999). Urbanization, or the phenomenon of creating, developing, and expanding cities, is propelling the world toward a mostly urban environment (United Nations, 2001). It has been predicted that by the year 2025, 85% of the world's population will reside in cities (Department of the Navy,

1998). Therefore, with little rural and sparse land available, future wars will be fought in urban or city areas (Department of the Navy, 1998; Glenn, 1999; Mabry et al., 2000).

According to the World Resources Institute (1996-97), urbanization is a trend that will include countries throughout the world. Urbanization rates may decrease in developed countries, but it will continue to grow in less developed countries (Department of the Army, 2006; United Nations, 1999, 2001). Latin American, Caribbean, African, and Asian regions are currently experiencing urban growth at a phenomenal rate (United Nations, 1994). For example, by 2015, 11 of the 15 largest cities will be in Asian countries (United Nations, 1994). Also, Africa and Asia are currently about 37% urban; however, by the year 2030, both regions are expected to report 54% of their land resources as being urbanized (United Nations, 1999, 2001). Mega-cities (a city of 10 million or more inhabitants), one outcome of urbanization (Department of the Army, 2002, 2006; World Resources Institute, 1998-99), have grown from one in 1950 to 17 in 2001, and by 2015, that number is predicted to rise to 21 (United Nations, 2001). These statistics on urbanization clearly show that available rural, isolated, and open-spaced land areas around the world will continue to decline. Because of the depletion of open-spaced and rural land, military conflicts have been and will continue to be fought in city environments, which subject the soldier to a number of challenges not otherwise found on the traditional isolated and open-spaced battlefield.

2.1.2 *Urban Warfare Challenges*

Historically, countries fought conventional wars. However, because of the rapid development of urban areas, warfare will no longer resemble an historic conventional structure but will be seen and described as having an unconventional structure. Conventional warfare can

be thought of as fighting the "old" or "customary" way, in which armies fought on isolated land away from civilians (Matloff, 1989). Unconventional warfare can be described as fighting other than the "customary" way, but for the purpose of this research, unconventional warfare will refer to any conflicts that take place in a city or urban environment.

There are three defining characteristics of conventional warfare. First, conventional warfare usually takes place on a restricted, isolated, and open-spaced battlefield (Matloff, 1989). Second, fighting between armies usually occurs with the use of large and powerful artillery (Department of the Army, 2008). Artillery can consist of machine guns, antitank missiles, surface-to-surface missiles, cannons, and tanks. Third, there are no civilians present on or near the battlefield (Department of the Army, 2008). The absence of civilians on the battlefield makes the soldier's job of identifying a threat much easier. Upon detecting someone on the conventional battlefield, the soldier must decide if that someone is affiliated with an enemy force or friendly force. In conventional conflict, the identifiable military emblem is on military uniforms and materiel, thereby assisting the soldier in making an accurate decision about impending threat.

In contrast, there are three defining characteristics of unconventional warfare. First, combat does not take place in a restricted and isolated area, but in a city (Hahn II & Jezior, 1999) with concrete buildings and confining compartments (Groves, 1998). Second, heavy and powerful artillery is not used because of the potential for massive structural damage and civilian casualties (Hahn II & Jezior, 1999). For example, civilian casualties resulting from the 1989 U.S. invasion of Panama City are estimated to be between 300 and 4,000 (Physicians for Human Rights, 1991). Thus, to decrease civilian casualties, soldiers engage in sudden, continuous, and person-to-person combat with the enemy at close ranges (100 meters or less) (Department of the

Army, 2002; Gerwehr & Glenn, 2000; Groves, 1998). Person-to-person combat requires the use of light weaponry such as rifles, machine guns, and hand grenades (Department of the Army, 2006). Third, civilians are present on or near the battlefield and the soldier must discern whether they are a threat or non-threat. The presence of civilians in the midst of urban warfare is a big concern because enemies can falsely present themselves as civilians in order to get closer to the intended target for greater destruction (Department of the Army, 2002, 2006, 2008; Gerwehr & Glenn, 2000).

The urban environment is filled with entities that provide adequate cover and concealment for an enemy (e.g., roofs, upper stories of buildings, sewer systems, subways) (Department of the Army, 2006), which creates obstructions and limits the soldier's visibility of the enemy (Department of the Army, 2002). In addition, the soldier may find that the enemy will use the civilian crowd to blend in and look like a civilian while being perceived as non-threatening to the soldier, in order to get as close as possible to destroy and kill the intended target (Gerwehr & Glenn, 2000). Urban guerrillas, terrorists, and underdog armies are examples of urban threats that use civilian concealment tactics (Grau & Kipp, 1999). An example of such an environment existed in Mogadishu, Somalia, in 1993 where U.S. soldiers fought militiamen (an army composed of citizens) in a gun battle among the city civilian population (Mabry et al., 2000). Because the militiamen were civilians and not a part of the professional armed forces, distinguishing them from non-threatening civilians presented a challenge, and sometimes it was impossible for the soldiers to identify the enemy. As a result, 19 American soldiers were killed and 90 were wounded by Somalian civilians (Desch, 2001; Edwards, 2000). Having difficulty with identifying the enemy will not only add tension to the soldier's decision-making capabilities, but it will also affect the soldier's performance. The ultimate consequence of

repeatedly making an incorrect decision regarding the threat status of a civilian would be the death of innocent civilians. Without an available method to distinguish between friendly and threatening civilians, soldiers will continue to make poor decisions about civilian threat status which will directly lead the soldier to execute inappropriate response actions.

2.2 Trying Times on the Home Front: Citizens' Need for ABTA

This research is significant in that the concepts and ideas can be used to address solutions for the soldier and solutions regarding U.S. citizen and infrastructure safety. On February 6, 2002, Dale Watson, the Executive Assistant Director of the Federal Bureau of Investigation (FBI) over Counterterrorism and Counterintelligence, spoke to the Senate Select Committee on Intelligence concerning terrorism (Congressional Statement, 2002). Watson explained that attacks on the United States and U.S. soldiers abroad are escalating and those responsible have a goal of producing mass casualties (Congressional Statement, 2002). This is evident from the September 11, 2001, attack on U.S. soil, the USS Cole bombing in October 2000, the U.S. embassy bombings in Africa in August 1998 that killed 301 and injured 5,077 (U.S. Department of State, 1998), and the October 23, 1983, bombings of U.S. and French barracks in Beirut. The best possible solution for these situations would be to stop the events before they occurred. Quality intelligence information would be (and has been) the first method used in thwarting such planned attacks (Department of the Navy, 1998). However, if intelligence information is not available or sufficient, what other method is there to fill the gap? ABTA methods can provide a behavior-based threat identification method in addition to identification through intelligence-gathering methods. Personnel who work within high threat situations overseas would use the

methods of ABTA to increase their ability to identify behaviors that implicate people who pose a threat and have intentions of conducting massively destructive attacks.

On September 11, 2001, and October 2, 2002, bits and pieces of the American way of life were eroded. In 2001 and 2002, foreign and domestic terrorists eroded national and local security as Americans have come to know it. Both dates provide evidence that U.S. citizens are living in a climate in which they are under attack. After September 11, 2001, law enforcement agencies encouraged the public to be alert and on the lookout for suspicious individuals (White, 2002). However, many citizens were not aware of what they should have been looking for in order to recognize a suspicious individual (White, 2002). The Maryland, Washington, D.C., and Virginia area sniper attacks that started on October 2, 2002, and ended on October 23, 2002, were yet another reminder to American citizens that they could be susceptible to attack while engaging in everyday activities such as pumping gasoline. One citizen even described the attacks as something similar to a war zone (Oglesby, 2002). In light of such attacks, Johnson (2002) suggests that long gone are the days when citizens rely on the police and their government to rescue them. He suggests that citizens should become more than spectators and act individually in some capacity to help protect societal safety. Also during the time frame of the sniper attacks, the police pleaded with citizens to provide information that could help bring the persons responsible for the attacks to justice, and O'Neil (2002), the director of research for the National Crime Prevention Council, generated a list for citizens that detailed the types of information that would be helpful to police in solving the crime. However, O'Neil (2002) may have failed to realize that unless citizens were given training to contextually recognize the list of information, untrained citizens would likely miss similar information that would be salient to law enforcement officers. Other examples of domestic terrorism in the United States include the

Oklahoma City bombing (April 19, 1995), Virginia Tech shootings (April 16, 2007), and U.S. Holocaust Memorial Museum shooting (June 10, 2009).

During the 46th Annual Meeting of the Human Factors and Ergonomics Society (HFES), a special colloquium session was held, entitled "The Role of Human Factors in Homeland Security". The session was held to foster new research ideas in the area of national security and to highlight how the field of human factors could contribute solutions to help prevent future terrorist attacks (Hancock, 2002). The theories and methods of ABTA would reasonably fit as one human factors solution to the problems facing the Department of Homeland Security, specifically, preventing threatening individuals from conducting massive attacks inside the U.S. border. Overall, the methods of ABTA can help to empower citizens to be active participants in helping to protect American society from those who wish to cause it harm. By being aware and looking for potentially threatening individuals, citizens may be able to diffuse dangerous situations, thereby helping national and local law enforcement agencies to preserve order.

2.3 Research Frameworks

2.3.1 *Target Acquisition*

Target acquisition has a long history within the military sector (Koopman, 1980). However, the concept of target acquisition can also be applied to a number of non-military sectors such as the medical and police communities (Koopman, 1980). The commonality lies in the search for a target. In the medical community, the search may be for a disease and in the police community, the search may be for an alleged criminal (Koopman, 1980). In addition, similar to but outside the scope of this project is the potential for police officers, security guards,

and airport security officials to apply ABTA to determine civilian threat related to crime and criminal intent. The current military definition of target acquisition pertains to the detection and identification of materiel systems (Vaughan, 2006) for the purpose of identifying the enemy. Because conventional wars were once fought on restricted and isolated battlefields (Matloff, 1989) and fighting between armies occurred at a distance with the use of heavy and powerful artillery (Matloff, 1989), the recognition of materiel was enough for positive enemy identification. Target acquisition as just described will be referred to as traditional target acquisition.

The U.S. military has expended great efforts in furthering the approach of traditional target acquisition to improve the soldier's ability to detect an enemy. Traditional target acquisition research efforts seem to fall within a "vehicle classification" target ideology (i.e., tanks, personnel carriers, etc.), which is inherently different from "human" target ideology (O'Connor et al., 1996). A good portion of research in the traditional target acquisition area has been dedicated to finding factors that influence target acquisition, building prediction models to improve performance in target detection, and improving sensors to enhance target detection abilities. For example, background clutter is thought to be a factor that affects target detection. Doll, Schmieder, and McWhorter (1992) explain that "clutter" makes a target difficult to locate and detect. Cathcart, Doll, and Schmieder (1988, 1989) conducted a study to determine the effects of urban clutter on target detection. Urban and rural clutter images were shown, and participants were to locate the military target (M-1 tank) within the image. The authors hypothesized that target detection would be worse in urban clutter, as opposed to rural clutter, because of the presence of more man-made objects in an urban scene. However, the results showed that target detection was better in urban clutter. The efforts of Meitzler, Jackson,

Bednarz, and Collins (1992) combined the building of prediction models with the improvement of sensors with the use of a vehicle (M60 or armored personal carrier) as the target. Therefore, traditional military target acquisition research efforts focus on improving the probability of acquiring military targets (i.e., tanks, personnel carriers, etc.) with the use of a variety of factors. However, none of the research efforts focus on the use of nonverbal cues to detect threatening human activity.

When ABTA is considered, the concept of target acquisition differs. Although the military defines target acquisition as the detection and identification of military materiel systems (Vaughan, 2006), ABTA is concerned with the identification of people. Unlike traditional target acquisition, identification of a target or threat is achieved through the interpretation of behaviors displayed by an individual.

2.3.2 *Nonverbal Communication*

2.3.2.1 *Theory and Significance*

Nonverbal behaviors are defined as body movements, postural changes, gestures, and facial expressions (Ekman, 1997; Ekman & Friesen, 1969a, 1969b). The theory of nonverbal communication posits that communication is possible via behavior alone. Communication is defined as "a giving or exchanging of information, signals, or messages as by talk, gestures, or writing" (Neufeldt & Guralnik, 1988, p. 282). Communication via nonverbal behaviors has a mirrored reciprocating effect that involves the person who initiates the behavior (initiator) and the person perceiving the behavior (perceiver). Rozelle and Baxter (1975) depicted this mirrored effect: "…one person's behavior toward another may be conceived as flowing directly from his inferences about the other person's intentions and goals in a situation…" (p. 53). Here it is

assumed that the initiator has displayed behaviors that were communicated to the perceiver as meaningful (Figure 2). The perceiver then perceives and interprets the behaviors and initiates a set of responsive behaviors. This scenario shows that meaningful and specific information is being exchanged between two people. Therefore, it is theorized that nonverbal behaviors are significant (Ekman & Friesen, 1969a; Wiener, Devoe, Rubinow, & Geller, 1972). What is interesting is that this mode of communication may be just as effective as the verbal mode of communication; so much so, that the terms "nonverbal communication" and "nonverbal behavior" are often used interchangeably (Krauss, Chen, & Chawla, 1996, p. 390). In addition to providing meaningful and specific information, nonverbal behavior can provide information about an individual's internal or emotional state, intentions, and motives (Ekman, 1997; Krauss et al., 1996; Secord et al., 1976).

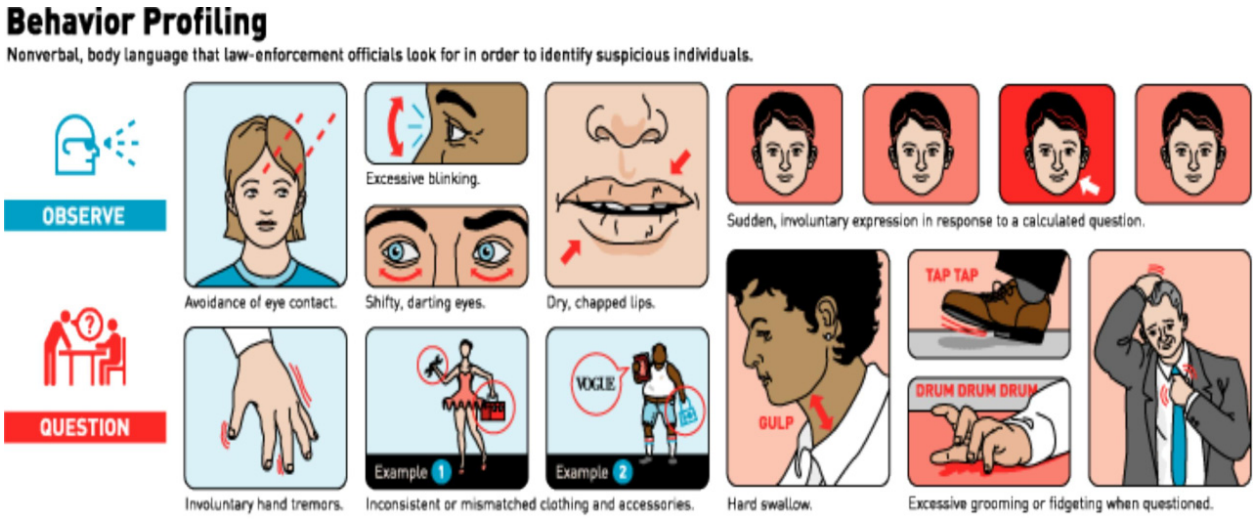


Figure 2. Examples of behaviors considered to contain meaning. (Davis, Pereira, & Bulkeley, October 2002. Reprinted with permission from the illustrator.)

Druckman and Bjork (1991) further describe nonverbal behavior as a window to an individual's underlying psychological state. However, the hypothesized connection between an individual's

behavior and underlying intentions is not visibly clear and must be made through some inferential process. Ekman and Friesen (1969a) explain that this is a complex task that requires one to interpret not only the nonverbal behavior but also the information conveyed by the behavior, as well as the circumstances surrounding the behavior.

Many agree that some theoretical mechanisms of nonverbal communication are still not completely understood, and using nonverbal behavior to interpret an individual's current internal state or next plan of action is very challenging (Baldwin & Baird, 2001; Druckman & Bjork, 1991; Ekman, 2001; Ekman & Friesen, 1969a; Vrij, 1994). Nonverbal interpretation is challenging because most people are exposed to a mass amount of nonverbal information but with very little or no idea about how to use such information to interpret intentions and motives (Ekman, 2001). To further complicate matters, it is believed that nonverbal information can be processed on a non-conscious level, especially in situations of severe time pressure or danger (Gigerenzer, 2007; University of Leeds, 2008). Considering the number of nonverbal behaviors and the different associations of intent that may be ascribed to one behavior, the theory of nonverbal communication may seem circular and hollow. Two principles, which are mainly inferred and discussed minimally in the literature, may help to funnel the theory out of its hollow circle toward a theory that can be used in a variety of new and existing applications. These principles, "multiple behaviors" and baselines, provide for a functional context in which the theory can be applied.

Any one behavior having occurred alone may not raise an eyebrow to suspicion or contain enough information for one to infer threat. However, if two or more behaviors (i.e., multiple behaviors) are present, the combination might indicate threat and the need to be alert (Nemko, 2003). This was shown in a study conducted by Ekman, O'Sullivan, Friesen, and

Scherer (1991). These researchers recruited 31 student nurses and had them watch a pleasant and unpleasant short film. After the pleasant film, the student nurses were told to give an honest interview regarding their feelings about the film. After the unpleasant film, the student nurses were told to give a deceptive interview that contradicted their true feelings about the film. Results showed that when the interviews were analyzed with four behavioral measures, interviews were correctly identified as honest or deceptive more of the time when two and three of the four behavioral measures were considered simultaneously. In contrast, interviews were correctly identified as honest or deceptive less of the time when each behavioral measure was considered alone. The idea stressed here is that individuals will have a greater chance of detecting true intentions and threat if "multiple behaviors" are used in assessing and interpreting possible threatening situations. When a number of nonverbal behaviors are present, a pattern of behavior will more likely be identified, unlike behaviors that occur in isolation. That pattern of behavior then becomes a communication tool, in which intentions are revealed (involuntary or voluntary), which is perceived by others as a window to one's current mind state. For example, if an individual is seen walking down a public street smiling and singing, that person may be judged by others as being happy. The individual did not have to verbally articulate happiness because the displayed behavior revealed a message of happiness. Had the individual walked down the street with a blank stare, the message of happiness would be almost impossible to interpret. Thus, the use of one nonverbal behavior to interpret intent and one's next plan of action does not wholly describe the theory of nonverbal communication.

The second principle that would help to move the theory of nonverbal communication from theory to application is the idea of baselines. Communication with a subject matter expert (SME) about nonverbal communication revealed that after a "what is normal" behavior baseline

is established, all other future occurring behaviors can be evaluated against the normal baseline, and behaviors outside the established normalcy would be considered inconsistent, suspicious, or threatening. Ekman (2001) also makes this point by noting that when one is interpreting nonverbal cues for intent, observation of a person should occur in several situations to allow for comparisons. This would allow for a more accurate interpretation of what the nonverbal cues are really conveying. He posits that observing a person or situation one moment in time to predict intentions from nonverbal cues might lead to incorrect assumptions about that person or situation. Because White and Burgoon (2001) found that individuals with concealed intentions changed their behavior over time, they, too, emphasize the importance of observing behaviors over some time period.

Although still quite incomplete theoretically, the theory of nonverbal communication does lend itself to be applied in situations where civilian intent must be inferred from nonverbal cues. Although appropriate, it must be acknowledged that the theory also has limitations. Ekman (2001) denotes these limitations as dangers and precautions. One such limitation noted by Ekman (2001) is that extensive knowledge of nonverbal cues will not prevent mistaken judgments. Another limitation noted by Ekman (2001) is that individuals may differ [in mind state] when expressing identical behaviors. These limitations show why the consideration of "multiple behaviors" and baselines is so important when one is applying this theory. Such factors may help to reduce the incidence of mistaken intent when one is making judgments about an individual via nonverbal cues. Overall, mistakes in judgment will occur when we apply the theory of nonverbal communication. However, knowledge about and practical application of the theory have been shown to improve one's ability to detect individuals who harbor covert intentions (Ekman, 1997).

2.3.2.2 *Threat Detection Using Nonverbal Cues and Intention*

Social stereotype theory reveals the concept of how one would use nonverbal cues to categorize individuals harboring covert mischievous intentions who are also perceived as a threat (Secord et al., 1976). When an individual socially stereotypes another, s/he 1) places that person in a category, and 2) attributes certain traits to that category. Shoemaker, South, and Lowe (1973) asked participants to view 12 facial photographs and identify the person in each photograph as most likely or least likely to be associated with several categories: murder, robbery, and treason. They found that the majority of participants agreed upon what the face of murder, robbery, and treason looked like. The participants also agreed upon what faces did not fit these categories. Because judgments were made without knowledge about the people in the photographs, we can assume that the judgments were based on perceived stereotypes. These results show that people may stereotype and categorize others based on specific criteria and characteristics which others have also found (Bar, Neta, & Linz, 2006; Spencer-Rodgers, Hamilton, & Sherman, 2007). Using nonverbal cues in detecting a threat is very similar to social stereotyping in that a descriptor category is created (e.g., threatening people), along with the characteristic behaviors (e.g., threatening behaviors) and examples (Medin & Schaffer, 1978) for that category, and is stored in long-term memory. Thus, when an observer encounters an unknown person (i.e., human target) and perceives his or her behavior as threatening, the observer is likely to categorize the unknown person as a threatening individual. Figure 3 depicts this process of classification. According to Medin and Schaffer (1978), the process of making a classification judgment of "threatening" is based on the examples stored in long-term memory regarding the behaviors of threatening people. The threatening behaviors that are seen by the

observer serve as a prompt that leads the observer to access stored information that is similar to the behaviors being viewed. Specific nonverbal cues that have been associated with mischievous or threatening intentions are listed in Table 1.

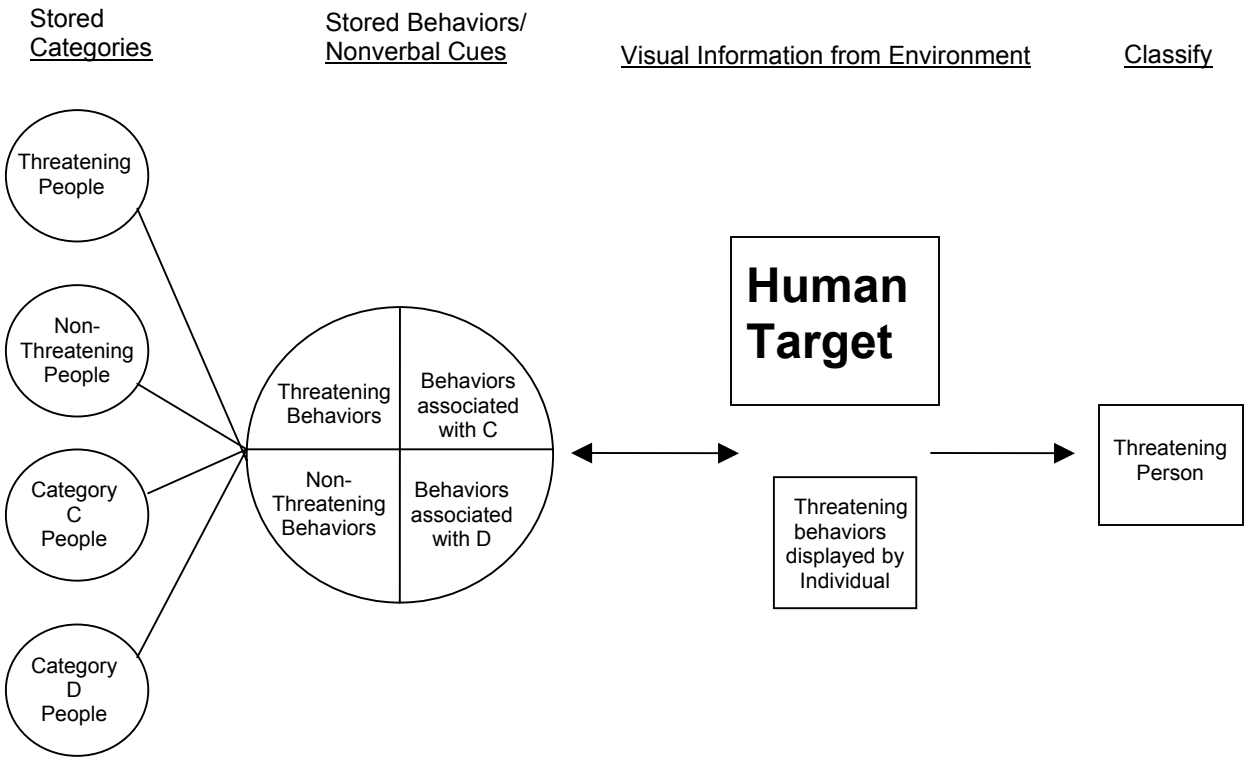


Figure 3. The human classification process using behavioral cues. (Perceived categories C and D are used as hypothetical receptacles whereby any category of people and their associated behaviors can be substituted. Categories and behaviors are stored in long-term memory.)

Table 1. Literature-identified cues associated with individuals harboring mischievous intentions.

Cues for the Identification of Individuals with Mischievous Intentions	
Turning body away; hand reaching to cover some Portion of the face; nervous movements of feet/legs	Nemko (2003)
Staring; a slouching posture; foot tapping; fidgeting	Martin (2002)
Loitering; note taking or tape recording at events; pacing	White (2002)
Blinking; postural shifts; hesitation; stuttering	Al-Simadi (2000)
Narrowing the red margins of the lips (anger)	Ekman (1997)
Decreased movements (rigidity)	Vrij, Semin, & Bull (1996)
Subtle hand/finger movements	Vrij (1994)
Facial expressions; vocal measures	Ekman & O'Sullivan (1991)
Facial features; body build; general appearance	Secord et al. (1976)
Pupil dilation; stuttering; shrugs; repetition; tense posture	Lakhani & Taylor (2003)
Gaze aversion; self-manipulations; 'ah' speech disturbances	Granhag & Stromwall (2002)

Although similarity can be found between the two theories, civilian classification using the methods of ABTA is considered more accurate than typical stereotyping. Some people believe that nonverbal cues are beneficial and important in detecting mischief (Ekman & Friesen, 1969a; Krauss et al., 1996). Arvid Kappas, a United Kingdom university psychology lecturer, agrees that analyzing behavioral cues to impart information about an individual's intention is just as reliable as analyzing a handwriting sample to impart similar information (Davis, Pereira, & Bulkeley, August 2002). Murray's (2002) statement about the September 11, 2001, terrorists illustrates the point of Davis et al. (August 2002). He states that nine of the terrorists were scrutinized more regularly than normal at target airports but were cleared to proceed. The terrorists, knowing what was about to happen, had to be under significant pressure when scrutinized, but they were still capable of displaying behavior that was considered comparatively

normal by airport security. Contradictory to the last statement and in defense of nonverbal communication, Murray's (2002) statement could also imply that airport security was led by intuitive impressions concerning the terrorists' behavior to scrutinize them at a higher than normal search rate. Intuitive impressions are automatic, fast, involuntary, guided by emotions, reached without conscious awareness, and not easy to explain or justify (Hogarth, 2001; Kahneman, 2003; Pretz & Totz, 2007). The unexplainable high search rate in the absence of suspicious behavioral evidence implies that nonverbal cues may be accurately processed on a non-conscious level. However, intuitive modes of thought often compete with analytical modes of thought which are slow, deliberate, formed consciously, and rule based (Hogarth, 2001; Kahneman, 2003; Simmons & Nelson, 2006). According to Simmons and Nelson (2006), intuitive confidence often helps the decision maker choose one mode of thought over the other. If intuitive confidence is high, the decision maker is likely to choose the decision acquired from the intuitive mode of thought and probably in the case of airport security, if intuitive confidence is low, the decision maker is likely to choose the decision acquired from the analytical mode of thought. Thus, low intuitive confidence combined with analytically, comparatively normal behavioral cues perhaps led security personnel to decide to allow the terrorists to fly.

Several physical modalities (i.e., face, hands, legs, feet, body, posture) can transmit nonverbal information (Ekman, 1988; Shoemaker & South, 1978); however, a number of early research studies conducted to document the detection of individuals with covert mischievous intentions via nonverbal information focused only on the face (Ekman & Friesen, 1976; Ekman, Friesen, & Ellsworth, 1972; Ekman, Friesen, & O'Sullivan, 1988). Interestingly, the face has been noted as the modality that can be expertly controlled and thus, most likely to send information that is completely opposite of one's true demeanor, state of mind, or emotional

status (Ekman & Friesen, 1969b). Ekman and Friesen (1969b) also believe that the face is the central modality in social interaction upon which people focus first, which makes people aware of their own facial expressions through the feedback they receive from others. For this reason, individuals wanting to hide their true intentions are able to use feedback to learn what people focus upon concerning the face and are able to inhibit and control facial nonverbal cues that give rise to suspicion (Ekman et al., 1991). If true, this may explain why some are skeptical about embracing the theory of nonverbal communication, and in their defense, more often than not, the research shows that the rate of detection for covert mischievous intention is low when one is relying on the use of nonverbal cues. However, Ekman and O'Sullivan (1991) found that nonverbal facial cues are likely to be evident in high-stake situations where people find it more difficult to control their emotions and thus their facial expressions. Unfortunately, however, most experiments in this literature have involved "white" or non-challenging lies (Al-Simadi, 2000; Ekman et al., 1991), perhaps because high-stake situations may not occur very often in average daily activities and are very difficult to recreate in a laboratory setting. Thus, Ekman and O'Sullivan (1991) speculate that without high stakes, the consequences involved would be too low to elicit those nonverbal facial cues that would raise suspicion about mischief, thus explaining the low detection rates seen in research.

A University of California, Los Angeles study found that the conveyance of information is 7% words, 38% voice (tone, pitch, and inflection), and 55% nonverbal communication (Martin, 2002). This states that people pay close attention to words first, then the face, next the voice, and last, body movements during communication. Like the face, words are also fairly easy to control (Ekman, 2001). However, harboring mischievous intentions has been found to influence voice pitch and body movements (Ekman & Friesen, 1974; Ekman et al., 1991). This

information shows that people rely on the very modalities (i.e., face, words) thought to transmit very little or no information when judging the presence or absence of mischievous intent (Ekman, 1988, 2001). More importantly, when people make judgments about an individual's intent, the use of both verbal and nonverbal information is fundamental (Vrij, Edward, Roberts, & Bull, 2000). Vrij et al. (2000) found that using a combination of verbal and nonverbal behaviors to distinguish liars from truth tellers produced a higher accuracy rate than using behaviors alone. The reliance on both information channels may help to raise suspicion about an individual's intent by showing that the verbal and nonverbal behaviors do not match (Ekman, 2001). As Ekman (2001) states, "…check the words against the face and voice [and body movements]" (p. 289). In other words, when both verbal and nonverbal information is available, the suggestion is to check the available modalities against one another for the output of contradictory information.

Although verbal information is shown to be a key component for increasing detection rates of mischievous intent, soldiers rarely dialogue with a potential enemy (MSG L. Garrett, personal communication, May 15, 2003). If soldiers were to engage in dialogue with a potential enemy, it would probably occur at a distance (e.g., 100 meters), which would decrease the usefulness of the verbal information needed to enhance the nonverbal information also received. However, when one is relying on verbal or nonverbal information in making judgments about intent, nonverbal information yields higher detection rates of true intent (Ekman & Friesen, 1974; Ekman & O'Sullivan, 1991). In Ekman and O'Sullivan's (1991) study of professional lie catchers, the only profession that achieved detection accuracy rates that were higher than 50% was the Secret Service. The Secret Service's performance was attributed to experience in observing crowds, which requires strict attention to nonverbal information. Also, when

analyzing detection rates across professions, Ekman and O'Sullivan (1991) found that those individuals with high detection accuracy rates attended to nonverbal behaviors when making judgments about intent. Those with low detection accuracy rates focused on verbal information only (Ekman, 2001; Ekman & O'Sullivan, 1991). These findings agree with earlier information that clues to true intent are more readily found in nonverbal behaviors than from words or strictly the face.

When one is considering MOUT environments and the limited interactions that occur with those being judged as threatening or non-threatening, using nonverbal information as a sole source for civilian classification should not present a problem. According to the literature, the sole use of nonverbal information to judge threat status may actually be an asset. This is indicated by the high detection rates achieved when only nonverbal information was considered in judgments about true intent.

2.3.2.3 *Threat Detection Using Nonverbal Cues and Training*

Although the debate still continues about what information is helpful in identifying a person with covert mischievous intentions, the consensus seems to be that detecting intent is a chance activity in which most individuals will correctly identify true intent 50% of the time (Ekman & O'Sullivan, 1991; Ekman et al., 1991; Levine, Park, & McCornack, 1999; Vrij, 1994). Despite low detection rates of 50% or less for judging true intent, Ekman (1996) speculates that behavioral information is present in most situations, but most people will not detect them. Even professional detectors of covert mischievous intent (i.e., customs officials, policemen, trial court judges, Federal Bureau of Investigation, Central Intelligence Agency, Drug Enforcement Administration, and trial lawyers) have shown low detection rates of 50% (Ekman, 1996; Ekman

& O'Sullivan, 1991). DePaulo and Pfeifer (1986) evaluated the perceived advantage of on-the-job experience in the detection of covert mischievous intent. When three groups were compared (college students, new law enforcement recruits, and veteran law enforcement officers) for their accuracy of detecting lies, no one group did significantly better than the others. Similar to the results obtained in Ekman and O'Sullivan's (1991) study, DePaulo and Pfeifer (1986) report that on-the-job experience provided no advantage for detecting individuals with covert mischievous intent. College students performed at the same level as officers who had seven years of experience. Therefore, some professionals would do no better in judging individuals with covert mischievous intent than a bus driver, college student, professional athlete, or soldier. A number of reasons have been offered for the 50% detection rates noted within the literature. Levine et al. (1999) offer three reasons why detection of mischievous intent may be poor: 1) there are no definitive behaviors that define harmful intent; therefore, accurate detection is not possible; 2) people focus on the wrong behavioral cues; and 3) people tend to use decision rules for judging mischievous intent instead of analyzing actual behaviors. In explaining low detection rates for professionals, Ekman (1996) offers that professionals might be more concerned with gathering evidence to convict instead of actually detecting potential harm, based on the available behavioral cues.

Currently, soldiers stand to benefit from the knowledge, methods, and application of nonverbal communication. To help people to detect a threat using behavioral cues, Vrij's (1994) findings show that giving people information about nonverbal cues may increase their accuracy for detection. In Vrij's (1994) study, those participants given nonverbal cue information achieved higher detection rates when deciding true intent than those given no information about nonverbal cues. Furthermore, he found that those given nonverbal cue information, along with

performance feedback, did better than all the other groups. In support of training people to detect individuals with covert mischievous intentions, Ekman (2001) states, "Becoming better able to spot clues to deceit requires more than simply understanding...; a skill must be developed through practice…anyone who spends the time looking and listening carefully,…, can improve." (p. 347). Vrij's (1994) results also show that those participants (i.e., police detectives) who judged mischievous intent using nonverbal cues only had poor detection rates when deciding true intent when no information regarding performance was given but significantly increased their detection rates when performance feedback was given. Druckman and Bjork (1991) also suggest that training should include learning the nonverbal cues and should provide strategies of how to weigh and combine the cues for judgments.

deTurck and Miller (1990) conducted a study to determine the effect of training on detecting individuals with covert intentions when the individuals being judged had an advantage over the observer. Detection training included the disclosure, examples, and practice with feedback of six nonverbal cues that implicate individuals with mischievous intentions. The observer's task was to watch a videotape of four people and to judge whether each person was truthful or lying. The videotaped participants were classified as high or low self-monitors. deTurck and Miller (1990) defined high self-monitors as those good at lying, while low self-monitors are poor at lying. Videotaped participants were further classified as those who rehearsed lying and those who did not rehearse lying. deTurck and Miller (1990) found that those observers who received training obtained the highest detection rates when deciding true intent, regardless if the videotaped individual was a high self-monitor or had time to rehearse. High self-monitors (i.e., good liars) and rehearsal are thought to increase the difficulty of observers to detect covert mischievous intent (deTurck & Miller, 1990). Individuals good at

hiding their true intent, combined with rehearsal, will continue to be a challenge to those trying to detect people with covert mischievous intent, especially among trained terrorists (MSG L. Garrett, personal communication, May 15, 2003). Training may help to lessen the challenge, however, and give the soldier an advantage in increasing detection rates for such individuals.

2.4 Factors That Strengthen the Relationship Between Nonverbal Cues and Threat

2.4.1 *Presentation Mode of Stimuli*

ABTA is concerned with (1) highlighting pertinent nonverbal cues and (2) the interpretation of the highlighted cues, which are deemed critical for an observer to be successful in the skill of detecting a threat. To make judgments about the intentions of civilians in the environment, soldiers must assess the environment to obtain information (i.e., nonverbal cues) believed to be helpful in decisions regarding a threat. Thus, the soldier gains a perspective of the environment, which is one of several steps before decision making and action execution (Endsley, 1988, 1995; Klein, 1998). However, if pertinent nonverbal cues are overlooked, the soldier is not likely to develop a complete understanding of the situation. Without a complete picture, situational awareness will be low, which will in turn lead to poor decision making regarding the presence or absence of threat. This is also true if the nonverbal cues are interpreted contrarily to their intended meaning. Erroneous cue interpretations may guide the soldier to an incorrect decision concerning threat and subsequently guide the soldier to take unjustifiable action.

Since the successful detection of individuals with threatening intentions is based on the observer's ability to obtain pertinent behavioral cues from the environment, it is important for laboratory stimuli to promote an environment that is ideal for the perception of the cues.

The presentation mode that is selected for presenting the behavioral cues is identified as a factor that can influence the observer's perception of the cues as well as detection accuracy. Stromwall and Granhag (2003) presented videotape, audiotape, and transcribed versions of testimony. The participants who watched the testimony rated the testimony higher in consistency, richness of detail, and logical structure than participants who read a transcript of the testimony. Participants who listened to the testimony also rated the testimony higher in consistency than participants who read a transcript of the testimony. Schweitzer, Brodt, and Croson (2002) showed that deceivers use the visual mode to monitor the target (of their deception) in order to correct their behavior to affect the outcome in their favor. This same level of deception was not afforded in the non-visual mode. In contrast to the results reported by Stromwall and Granhag (2003) and Schweitzer et al. (2002), which show an advantage for the visual mode in facilitating the perception of behavioral cues, Maier and Thurber (1968) reported a disadvantage for the visual mode. They reported significantly higher deception detection accuracy rates for participants who listened to and read an interview versus participants who watched the interview live. The behavioral cues that were exhibited in the visual mode by the interviewee were hypothesized as being a distraction that biased participants to judge the interviewee as dishonest more frequently. Finally, Lievens and Sackett (2006) examined the difference in predictive validity for video-based and written situational judgment tests (SJTs) when used for an entrance exam related to interpersonal interaction. The video-based SJT had a higher predictive validity than the written SJT. Lievens and Sackett (2006) hypothesized that the video-based SJT had a higher predictive validity because it contained the facial expressions, emotions, and voice inflections that are naturally inherent in interpersonal interactions.

2.4.2 *Judgment and Decision Making*

ABTA will require the soldier to consider a variety of behaviors that may or may not be helpful to him in judging a potential civilian threat. Concluding that a behavior is threatening involves the judging of many potential target behaviors since the objective of judgment and decision making is choice selection which often involves the gathering, organizing, combining, and weighting of information (Lehto, 1997; Sternberg, 1999). Judgment and decision making involve a host of factors that will guide the final decision regarding the presence of threat, which will then lead to the execution of an action(s). For the soldier, the ultimate action may be to shoot or not to shoot. Judgment and decision making in the MOUT environment are characterized by features also found in a naturalistic environment: (1) complex, (2) uncertain and dynamic, (3) time constrained, (4) high stakes, (5) cue learning, (6) ill-structured problems, and (7) ambiguous information (Lipshitz, Klein, Orasanu, & Salas, 2001; Orasanu & Connolly, 1993). A naturalistic environment can be envisioned as "anywhere" a human operates while using the acquired knowledge and experience necessary for decision making and action execution. The Naturalistic Decision Making (NDM) approach seeks to "understand and improve decision making in field settings, particularly by helping people more quickly develop expertise and apply it to the challenges they face….[via] useful types of tools, training, and supports" (Salas & Klein, 2001, p.3).

Lipshitz et al. (2001) consider the Recognition-Primed Decision (RPD) model (Klein, Calderwood, & Macgregor, 1989) to be a prototype of NDM (Figure 4). In the model, decisions are made on the basis of recognition of situations as typical and familiar by people recognizing goals, salient cues, the causal dynamics of the situation, feasible courses of action, and expectancies (Klein, 1998; Klein et al., 1989). RPDs can occur in three variations: (1) the

decision maker immediately recognizes a situation and instantly knows the solution, (2) the decision maker does not immediately recognize a situation and needs to gather further information to gain situation recognition before choosing an appropriate solution; the situation is compared to familiar schema and prototypes held in working memory to select the best prototype for handling the current situation, and (3) the decision maker immediately recognizes a situation, but the appropriate course of action is evaluated (Figure 5) (Klein, 1998). Judgment and decision making via the RPD approach employ current situation cues to help people visually perceive the situation, map situation cues to recognizable and prototypical mental schemas, and select an appropriate course of action based on prior experience and current situation information. In interviews of experienced firefighters, Klein, Calderwood, and Cirocco (1986) found that alternate decision choices are not compared with one another (unless ambiguity is present). Instead, expert decision makers immediately recognize what to do based on experience, even in situations of uncertainty and time pressure (Lipshitz et al., 2001; Ross, Klein, Thunholm, Schmitt, & Baxter, 2004). In contrast, novices evaluate alternate decisions using comparison strategies. Novices have not obtained an adequate level of experience to effectively make judgments and decisions using the RPD strategy (Klein, 1998).

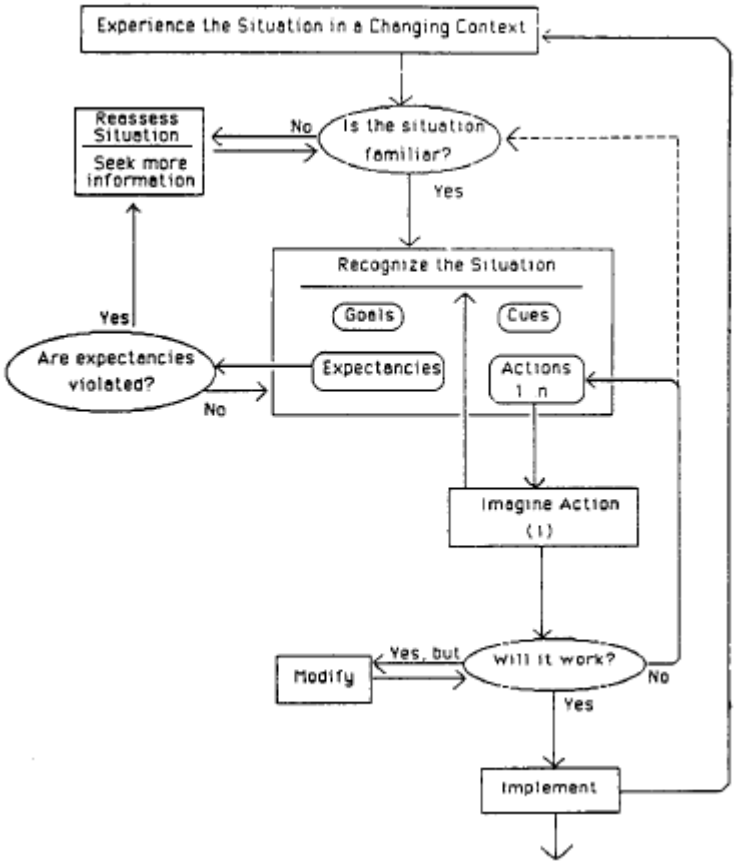


Figure 4. Recognition-Primed Decision model. (Reprinted with permission from IEEE Transactions on Systems, Man, and Cybernetics, Vol. 19, No. 3, 1989, © 1989 IEEE.)

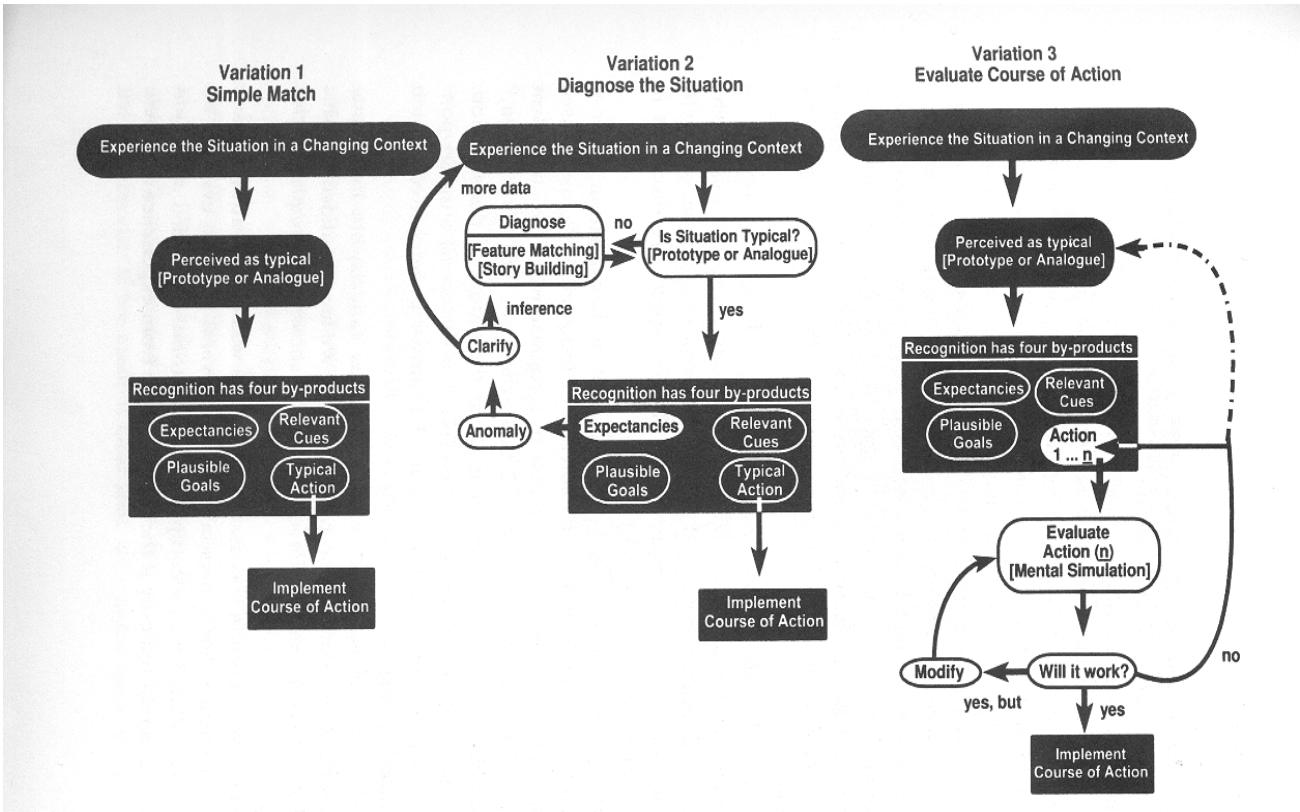


Figure 5. Variations within the RPD model shown individually. (From Gary Klein Sources of Power. Published by MIT Press. Copyright © 1998 Massachusetts Institute of Technology. Reprinted with permission from the publisher.)

Typical of a naturalistic environment, the MOUT environment is full of complex, dynamic features, one being the presence of civilians. In addition to all the other military-related tasks in MOUT, the soldier must be constantly aware of impending attacks from threatening civilians. High stakes in this environment represent death, and as a result, soldiers have little room to operate at the novice level of RPD. According to NDM theorists, decision makers need to be experts in their task domain (Klein, 1998). For the task of detecting threatening civilians, most military soldiers have not obtained the needed experience to be considered experts. Realistically, soldiers will only have the opportunity to gain experience in detecting civilian threats during conflict. Even then, every infantry soldier will not be called to duty. Thus, in the

absence of opportunity and learned experience, soldiers must still develop competent skills in detecting civilians who pose a threat to them. Ideally, judging and discriminating behavioral cues and events pertinent to detecting a civilian threat require soldiers to have existing behavioral and event prototypes or schema to map to different situations (Klein, 1998). According to Klein (1998), schemata (or prototypes) permit decision makers to tend to relevant situation cues, know what to expect, detect inconsistencies, see how situation factors fit together, adapt to changing events, and develop shortcuts and prescriptions for problem solving. All these factors combine to give the decision maker an efficient understanding of the situation. Based on the information in Table 1, the deception and nonverbal communication literature has done an excellent job at presenting the probable verbal and nonverbal cues that help to increase one's ability to detect individuals with covert mischievous intentions. However, the unimpressive detection accuracy rates prevalent throughout the literature show that knowledge about the cues to deception may not be enough. Perhaps there are strategies associated with using nonverbal cues to detect individuals with covert mischievous intentions and these strategies may be relevant in helping the soldier (i.e., novice) to quickly build cohesive behavioral and event schema for the detection of a threat.

2.4.3 *Situation Awareness, Schemata, and Scripts*

People make perceptual judgments about other people and events in their dynamically changing environment, based on a variety of factors and will eventually use those judgments to make important decisions. One factor that has been shown to be of importance when one is making judgments is situation awareness (SA) (Endsley, 1988, 1995, 2000b). Endsley (1988) defines SA in the context of three critical levels (Figure 6):

1. The perception of elements in the environment,
2. Comprehending the meaning of the environmental elements, and
3. Projecting the future status of the environmental elements.

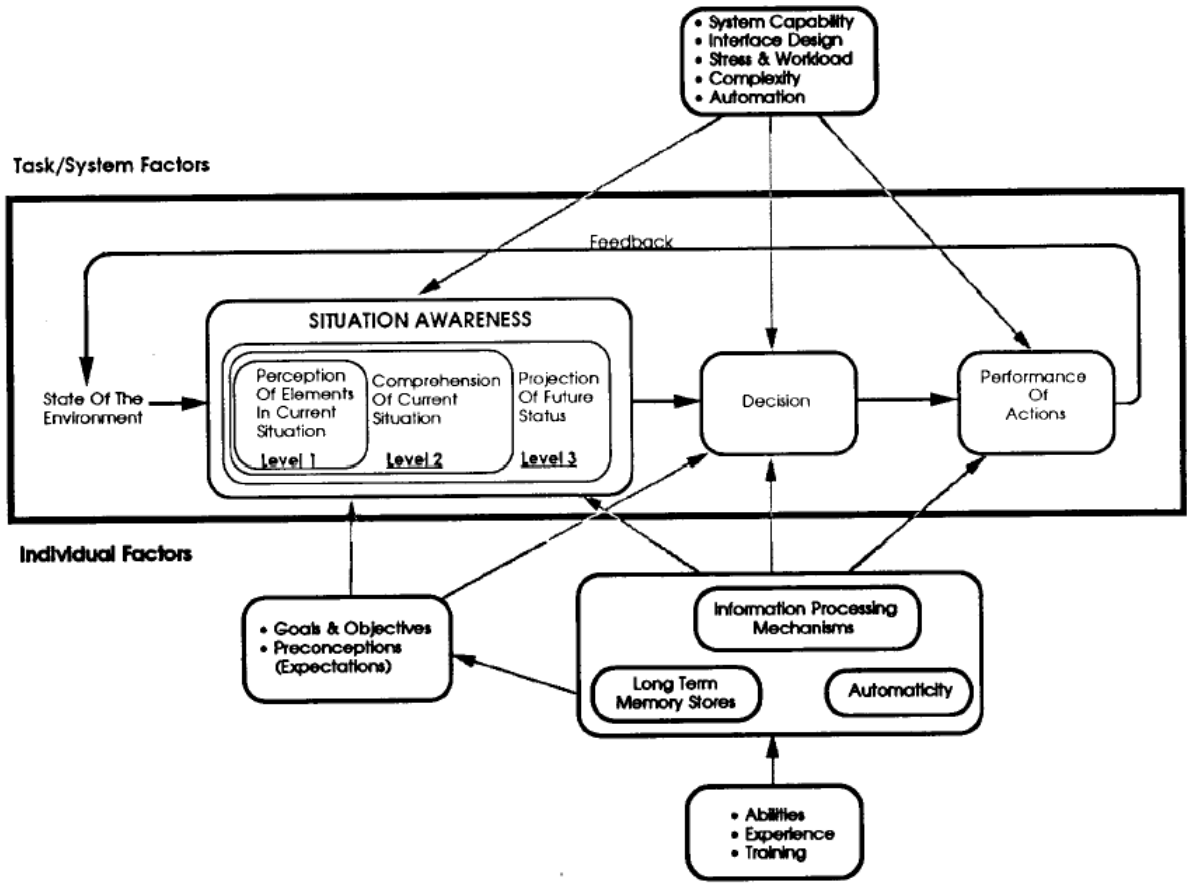


Figure 6. Endsley's situation awareness model. (Reprinted with permission from *Human Factors*, Vol. 37, No. 1, 1995. Copyright 1995 by the Human Factors and Ergonomics Society. All rights reserved.)

This definition helps to explain the importance of SA for ABTA. Level 1 of SA requires the decision maker to assemble the status of relevant elements (e.g., cues, attributes) in the environment (Endsley, 1995). Relevant cue information for ABTA would include body movements, hand signals, clothing, etc. Level 2 of SA requires the decision maker to integrate

information from Level 1 and develop a holistic view of the environment through understanding the significance, relationship, and context of objects and events (Endsley, 1995, 2000b). For ABTA, this will require an understanding of the relationship between nonverbal cues and intention, as well as an understanding of the context in which to expect the nonverbal cues. Finally, Level 3 of SA requires the decision maker to project the future status of the elements in the environment (Endsley, 1995). For ABTA, this would involve anticipating the consequences of an individual's intent via his or her display of nonverbal cues. SA theory predicts that if all levels of SA are achieved at some ideal, the decision maker will hold a high quality state of SA at any given time. However, there may be times when a high or acceptable level of SA cannot be maintained, and in such cases, a search for gaps within the SA model should be pursued. In the case of ABTA, it is hypothesized that a gap currently exists between Levels 1 and 2 of SA.

The achievement of detection rates above 50% when one is deciding true intent will require individuals to perceive relevant cue information from the environment at Level 1 SA. However, studies that have evaluated an individual's ability to detect those with covert mischievous intent (Ekman, 2001; Ekman & O'Sullivan, 1991) have shown that observers often miss relevant situation cues. In addition, observers tend to focus their attention on the wrong cues (Ekman, 2001; Ekman et al., 1991; Ekman & Friesen, 1969b). Level 2 of the SA model is responsible for organizing, combining, weighting (Lehto, 1997), and interpreting environmental information. This understanding of information is achieved through various mechanisms of SA (Figure 7), such as schemata (Endsley, 1995). Schemata store and organize knowledge, facts, experiences, and events held in long-term memory. Each schema contains its own goals, course of action plans, and scripts and is selected based on its match with current situation goals (Endsley, 1995, 2000a). Scripts or "standard event sequences" (Schank & Abelson, 1977, p. 38),

help to provide a reference for the types of events that will occur in a given situation and sometimes the order of those events (Abelson, 1981). After Level 1 SA information is perceived, it is then compared to existing schemata to find a match that fits with the current situation state (Level 2 SA). Klein (1998) labels this process pattern matching and distinguishes it as an important characteristic of NDM and recognition-primed decision making. Thus, we may close the gap between Levels 1 and 2 of SA by finding the strategies that will help an observer to efficiently use the behavioral cues in the environment to gain a complete understanding of his or her situation, which will also help to build and strengthen schemata. Klein (1998) and Endsley (1988) speculate that the ability to see patterns will enhance SA, which in turn will give an individual the ability to rapidly recognize relevant goals and cues for a given situation, thus discriminating novices from experts. Significant development of patterns is critical for obtaining an expertise level of performance in any task domain (Klein, 1998). Once expertise is developed, tasks and decisions within a domain will become automatic via the automatic selection of the appropriate schema (Endsley, 1995), which should reduce decision-making time and errors.

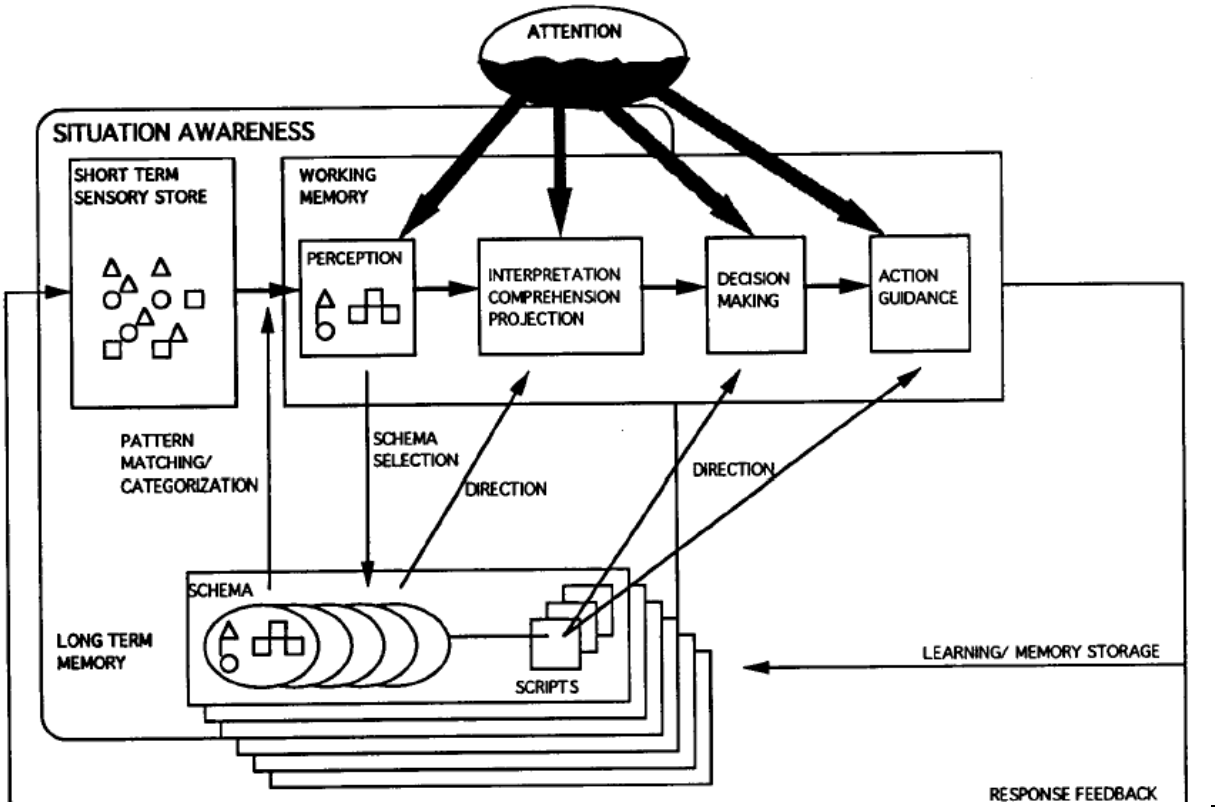


Figure 7. Endsley's mechanisms of situation awareness. (Reprinted with permission from *Human Factors*, Vol. 37, No. 1, 1995. Copyright 1995 by the Human Factors and Ergonomics Society. All rights reserved.)

Endsley (1995) and Klein (1993) discuss two types of decision errors that may occur at any of the three levels of SA: (1) incomplete and (2) inaccurate. An incomplete error occurs when the decision maker has knowledge about some of the elements but not all the elements in the environment. An inaccurate error occurs when the decision maker has knowledge about all the elements in the environment but uses an incorrect source for judging the elements. Incomplete and inaccurate errors can be found at all levels of SA; however, at each level, the cause of occurrence is different (Figure 8). Figure 8 shows that the underlying reason for an incomplete error is missing knowledge in schemata or lack of schemata (Level 2 SA). As

discussed earlier, infantry soldiers, along with most of the population, currently lack pattern recognition skills for judging a threat (Ekman, 2001). If knowledge, facts, events, and experiences in relation to activities of threat do not exist in long-term memory via self-contained schemata and scripts, an observer will have nothing to draw upon for familiarity and pattern matching during judgment and decision making about a threat. How the soldier perceives, interprets, and projects consequences from nonverbal cues during MOUT will directly influence his or her SA and civilian classification choices. Teaching soldiers pertinent strategies helpful in identifying threatening civilians will reduce their knowledge gap regarding how to use nonverbal cues to threat, build their schemata for threat, and increase their SA. Obtaining and maintaining a high degree of SA in MOUT are important to a soldier's survival (Walker, 2002) but are also important in preventing innocent civilians from being harmed or killed.

Thus, this research effort sought to 1) elicit expert strategies regarding how to use nonverbal cues to detect a threat, 2) evaluate the best medium for distinguishing a threat from a non-threat and for highlighting threatening people and nonverbal cues that indicate an imminent threat, 3) evaluate threat detection accuracy rates of experts in the threat detection domain, and 4) design a training development guide for training developers responsible for training the novice in the threat detection domain.

LEVEL 1 – (gathering cues in the environment)

Incomplete SA errors

- fail to visually detect cue(s)
- fail to perceive cue(s)

Inaccurate SA errors

- cue misnomer(s)

LEVEL 2 – (interpreting cues in the environment)

Incomplete SA errors (missing or no information)

- no schema available for current situation
- correct schema with mismatch data

Inaccurate SA errors (wrong information)

- incorrect schema selected for current situation
- failed to update selected schema for current situation

LEVEL 3 – (future projections)

Incomplete SA errors

- projection lacks pertinent information

Inaccurate SA errors

- projection is incorrect

Figure 8. Incomplete and inaccurate SA errors at each level of SA.

3. PHASE 1: THE ELICITATION OF EXPERT STRATEGIES FOR DETECTING THREAT

3.1 Objective

To elicit expert strategies regarding how to use nonverbal cues to detect threatening individuals.

3.2 Selection of Organizations in the Domain of Threat Detection

A list of organizations operating in the domain of threat detection was identified as potential resources for interviewing SMEs. To condense the list further, each organization's location (Baltimore-Washington area) was also considered. Four organizations were identified: Maryland State Police, FBI, Secret Service, and the Baltimore City Police. After reviewing the mission of each organization (Table 2), the author concluded that the sample would represent a range of expertise, experience, and perspectives typically found within the domain of threat detection. U.S. Army infantry soldiers with MOUT experience were also included because of their experience in conducting urban warfare or urban intervention operations among insurgent civilians and groups. The soldiers gained such experience in Iraq, Kosovo, and Bosnia.

Letters were sent to the public relations offices of the Maryland State Police, FBI, Secret Service, and the Baltimore City Police requesting ten SMEs to interview for 1 hour regarding threat and threat detection. Military personnel at Aberdeen Proving Ground were contacted to request the participation of infantry soldiers with MOUT experience. The Maryland State Police and the Baltimore City Police granted the full request. The Secret Service authorized the use of ten agents but for only 30 minutes. The FBI authorized the use of five agents for 1 hour. Only

five infantry soldiers were available to participate during the time the interviews were conducted. Given that the interviews were conducted during normal working hours, each organization's point of contact selected the interview participants and developed a schedule of interview times.

Table 2. Mission statements listed by organization.

Organization	Mission Statement
Maryland State Police	… "to protect the citizens of the State of Maryland from foreign and domestic security threats, to fight crime, and to promote roadway safety by upholding the laws of the State of Maryland." http://www.mdsp.org/
Baltimore City Police	"The preservation of the peace, protection of property and the arrest of offenders…" http://www.baltimorepolice.org/about-us/police-department/history
Secret Service	…"protects the president and vice president, their families, heads of state, and other designated individuals; investigates threats against these protectees; protects the White House, vice president's residence, foreign missions, and other buildings within Washington, D.C.; and plans and implements security designs for designated National Special Security Events." … "investigates violations of laws…" http://www.secretservice.gov/mission.shtml
FBI	"to protect and defend the United States against terrorist and foreign intelligence threats and to enforce the criminal laws of the United States." http://www.fbi.gov/hq.htm

3.3 Participants

Forty SMEs (35 males; 5 females) were interviewed (Table 3); they had a mean age of 38 years (*SD* = 8.23) [range of 24 to 51 years] with a mean of 14 years (*SD* = 6.82) [range of 3 to 26

years] of experience in the domain of threat detection. Participants also had experience in the following law enforcement specialty areas: trooper, criminal investigation, presidential protection, nuclear, biological, and chemical (NBC), detective unit, and intelligence.

Table 3. Number of interview participants listed by organization.

Organization	Number of SMEs
Maryland State Police	10
Baltimore City Police	10
Secret Service	10
FBI	5
U.S. Army	5

3.4 Interview Structure

A 1-hour, semi-structured interview (Appendix A) was used and is specifically helpful for revealing important research issues and understanding the experiences of those who operate in the domain of interest (Weiss, 1994). As a result of the Secret Service allowing only 30 minutes for interviews, a shorter version (minus nine questions) of the original interview (Appendix B) was conducted with Secret Service agents. Interview questions were arranged according to five specific areas related to the threat detection domain: (1) general background, (2) nonverbal cue elicitation, (3) situation awareness, (4) experience and training, and (5) decision making. Because of the range of expertise, several hypothetical questions were included to help the author obtain basic threat detection domain knowledge not necessarily associated with specific job duties and job experience. Unplanned questions were used to probe

SMEs to clarify concepts and techniques not familiar to the interviewers and to relate specific incidents to one of the five interview interest areas.

3.5 Procedures

Four personnel from the U.S. Army Research Laboratory and one person from the Night Vision and Electronic Sensors Directorate participated in the interviews as interviewers, and interviews were conducted on the respective sites of the organizations during normal working hours. All interviewers had previous experience conducting interviews via their job. Each participant was interviewed individually, and interviews lasted for 1 hour. Interviews with Secret Service agents lasted for 30 minutes. The interviews were conducted under an umbrella effort and in accordance with the policies for the protection of human subjects. The participating organizations included the Army Aberdeen Test Center, Army Material Systems Analysis Activity, Army Research Laboratory, Night Vision and Electronic Sensors Directorate, and TRADOC Analysis Center.

3.6 Interview Results

Interview participants from the FBI had more threat detection experience (M = 22 years, SD = 2.07) (Figure 9) than those from the other organizations (U.S. Army [M = 17 years, SD = 3.21], Baltimore City Police [M = 17 years, SD = 8.46], Secret Service [M = 13 years, SD = 3.05], and Maryland State Police [M = 9 years, SD = 6.89]).

The results for the interview questions are shown in Table 4. For each question, the number of responses is given because of missing data. Missing responses are attributable to questions not being relevant to the interviewee, interviewees declining to answer certain

questions, and Secret Service participants being presented with fewer questions because of a 30-minute time restriction for conducting interviews.

Interview question 14 under "Nonverbal Cue Elicitation Questions" asked interviewees how much time they needed to decide whether a person deserved further observation. Fifty-one percent of 37 participants responded very little time was needed for observation, while 43% and 5% responded that there was no set time for observation and a lot of time needed for observation, respectively. Question 16 under "Situation Awareness" asked whether it was harder to achieve SA in some situations as opposed to other situations and 96% of 25 participants responded yes while 4% responded no. In addition, question 19 under "Experience and Training" asked whether certain people were more intuitive than others in detecting suspicious behavior. Of thirty-nine participants, 97% responded yes and 3% responded no.

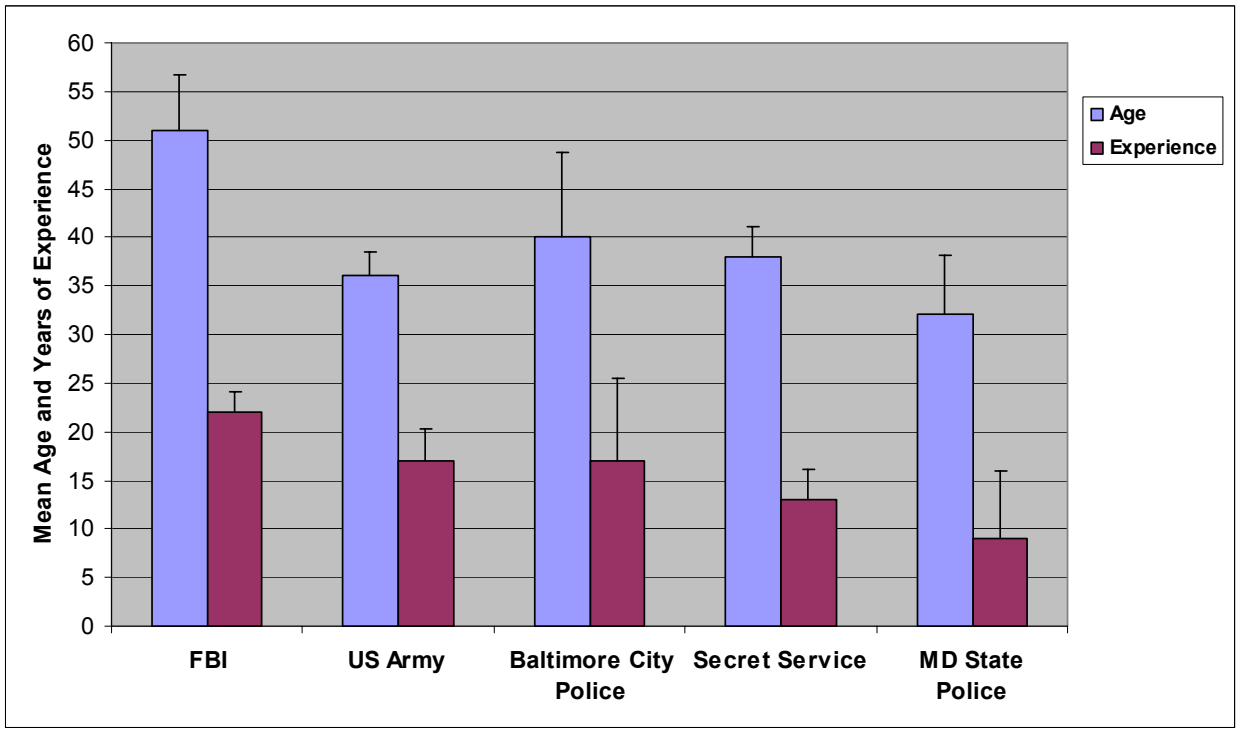


Figure 9. Mean age and years of threat detection experience by organization. Error bars indicate SD.

Table 4. Interview response results.

Interview Questions	Number of Responses	Results
General Background Questions		
1. Do you work mostly as part of a team or alone?	28	Alone – 50%; Team – 32%; Both – 18%
2. Initially, were you trained in observation techniques in order to do your job?	40	Yes – 95%; No – 5%
3. Are you routinely given information about an assignment before performing the assignment?	27	Yes – 67%; No – 26%; Sometimes – 7%
4. Would you say that the majority of your day-to-day duties involve routine or non-routine tasks?	37	Routine – 41%; Non Routine – 35%; Both -24%
5. Even when you're off duty, do you find yourself observing people in crowds?	40	Yes – 87.5%; No – 12.5%
Cue Elicitation		
6. Suppose you are observing the activity of people in a crowded ground or air terminal.		
a. Do you observe groups of people or individuals?	29	Individuals – 93%; Groups – 3.5%; Both – 3.5%

Table 4, con't. Interview response results.

Interview Questions	Number of Responses	Results
Cue ElicitationCon't		
7. Would your monitoring scheme change if it were a different environment (e.g., a city street, stadium event, foreign country)?	26	Yes – 73%; No – 27%
8. Do you think that observation techniques alone can give sufficient information about whether a person is intending to commit a crime?	37	Yes – 35%; No – 49%; Sometimes – 16%
a. Would you need "intelligence" information to spot a suspect?	36	Yes – 89%; No – 11%
9. How accurately do you think you can select a person intending to commit a hostile act?		
a. In a crowd? group?	26	Little – 38%; Somewhat – 31%; Accurate – 31%
b. On an individual basis?	26	Little – 15%; Somewhat – 35%; Accurate – 50%
c . When the group is a different ethnicity from you?	35	Little – 26%; Somewhat – 23%; Accurate – 51%
d . When the group is the same ethnicity as you?	26	Little – 15%; Somewhat – 27%; Accurate – 58%
10. What do you think is the ideal distance you must be from an individual suspect to detect whether he or she may be a potential problem?	35	No Set Distance – 20%; Close – 63%; Far – 17%
11. Do you need physical or verbal interaction with a suspect to determine hostile intentions?	35	Yes – 68.5%; No – 28.6%; Maybe – 2.9%

Table 4, con't. Interview response results.

Interview Questions	Number of Responses	Results
Cue Elicitation Con't		
12. Do you think a person intending to cause harm emits a different "signal" (or displays different behavior) than a person with no intent to cause harm?	37	Yes – 92%; No – 8%
13. In the job of discriminating people with hostile intent from others with no hostile agenda, how important do you think it is to be able to clearly see the faces of those you are observing?	36	Important – 81%; Not Important – 19%
14. About how much time do you think you ought to observe a person to decide whether that person is a suspect and deserves further observation?	37	No Set Time – 43.2%; Little Time – 51.4%; Lot of Time – 5.4%
Situation Awareness		
15. Is SA important in the performance of your job? Identifying hostile people?	37	Yes – 100%; No – 0%
16. Is it harder to achieve SA in some situations as opposed to other situations?	25	Yes – 96%; No – 4%

Table 4, con't. Interview response results.

Interview Questions	Number of Responses	Results
Experience and Training		
17. Do you think that someone can be trained to identify hostile intent cues and go into the field and be effective?	38	Yes – 71%; No – 21%; Sometimes – 8%
18. Do you think experience is an important factor in doing a good job of surveillance?	36	Yes – 100%; No – 0%
19. Do you think certain people are more intuitive than others in detecting suspicious behavior and just are better at the job?	39	Yes – 97%; No – 3%
20. Have you ever received follow-up information about an individual you identified as being suspicious and actually verified your judgment of that individual?	30	Yes – 67%; No – 33%
Decision Making		
21. Describe one particular situation in which you used certain cues to assess the situation but your assessment was false.		
a. Did you use the wrong cues or did you perceive the cues incorrectly?	30	Wrong Cues – 26.7%; Perceive Incorrectly – 40%; Both – 6.6%; Can't think of a situation – 26.7%
b. How often does such a situation occur?	22	Very Often – 4.5%; Often – 18%; Sometimes – 23%; Don't Know – 54.5%

Table 4, con't. Interview response results.

Interview Questions	Number of Responses	Results
Decision Making Con't		
22. When making decisions about a person's intent, do you		
a. perceive a cue and immediately decide on the appropriate action?	20	Yes – 55%; No – 45%
b. choose one action plan from various choices of action plans?	20	Yes – 65%; No – 35%

Note: The Secret Service granted 30 minutes for interviews; therefore, Secret Service participants (n = 10) did not receive the full set of interview questions. Also, some participants declined to answer some questions. The number of responses received for each question is included in the table. Questions with 30 or fewer responses indicate questions that were not included in the Secret Service interviews.

3.7 Discussion

In this phase, the author obtained strategies from experts in the threat detection domain regarding how to use nonverbal cues to detect a threat in an effort to improve threat detection performance for the novice. However, due to the sensitive nature of the information obtained in this phase, the actual nonverbal cues will not be reported. The strategies will only be reported. The author defines strategies as plans, actions, or prescriptions that help to place an observer in an advantageous position to effectively use nonverbal cues to identify threatening people. The strategies to promote the efficient use of nonverbal cues to detect threatening individuals are (Table 5):

1) Evaluate nonverbal cues within a contextual framework (Cues & Context).

2) It is difficult to attend to all the important elements in a crowd; call for backup when necessary (SA in Crowds).

3) Observe each situation for a reasonable amount of time before making a threat/non-threat decision (Time to Evaluate).

4) Constantly seek opportunities for practice to perfect threat detection skills (Practice).

5) Learn from intuitive individuals who are better at threat detection (Learn).

Of all the strategies, strategy 1 (Cues & Context) was inferred from the experts' interview responses and strategies 2, 3, 4, and 5 were obtained directly from the experts' responses. The strategies collapsed into two categories. Category 1 consists of strategies that can be directly applied in the field in the evaluation of real-world situations. Category 2 consists of strategies that have an impact on how successful observers are in applying category 1 strategies when in the field.

In addition to promoting the use of behavioral cues to detect individuals with covert mischievous intentions, Vrij and Mann (2004) promote techniques that are hypothesized to

further improve detection rates for such individuals. The techniques were devised to be used in the typical interview environment in which researchers study the detection of lies and truths. However, only one of the five techniques, cues to examine, appears to be appropriate for use in an environment where verbal communication is not likely before an observer must make a judgment regarding criminal or harmful intent. Cues to examine denote looking at cues in a systematic manner in order to detect individuals with covert mischievous intentions. The strategies found in this project are assumed to be just as important as the techniques put forward by Vrij and Mann (2004), but they were extracted from the experts themselves and structured for use in settings where an individual with threatening intentions must be detected before s/he performs a hostile act. In general, the strategies as a whole should be thought of as an entity that facilitates rapid and successful decisions regarding threat by strengthening an observer's ability to build, evaluate, and recognize patterns of behavior (Figure 10).

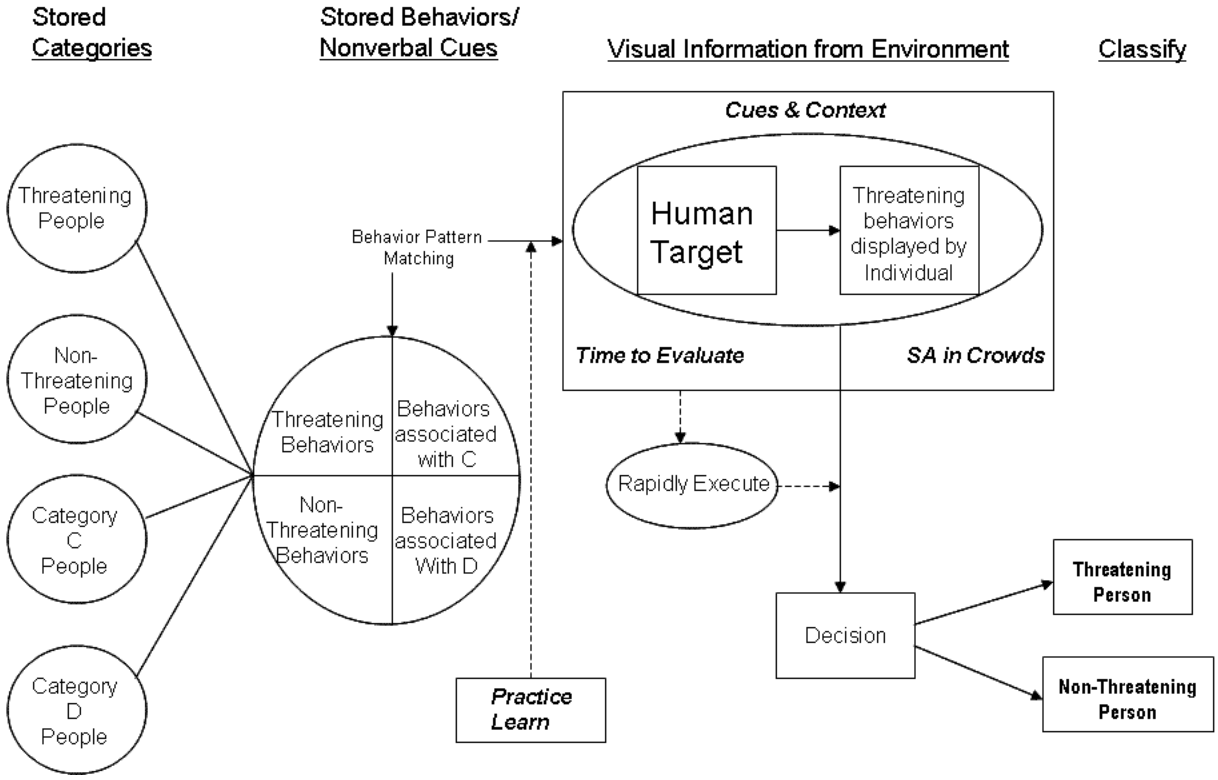


Figure 10. The influence of strategies on the human classification process. (Perceived categories C and D are used as hypothetical receptacles whereby any category of people and their associated behaviors can be substituted. Categories and behaviors are stored in long-term memory.)

Table 5. Expert strategies regarding how to use nonverbal cues to detect a threat.

Strategy	**Facilitated by Interview Question (Qualitative Responses)**	**Plans, Actions, and Prescriptions to Obtain Advantage**
Cues & Context (Category 1)	Inferred from the examples given during the interviews. When experts explained specific concepts regarding how they used nonverbal cues to assess threat, they always provided examples that were associated with the cues.	• Evaluate who, what, where, and when for each situation
SA in Crowds (Category 1)	**Question 16**: Is it harder to achieve SA in some situations as opposed to other situations? • The less information is available, the harder it is to gain SA • When not familiar with the environment • If you don't know what is normal • Big events • When you are an outsider to the environment • Domestic situations • When an observer needs to multi-task • Situation doesn't matter. What matters is the situational details…why are you in the situation, who else is in the situation, who is leading the event, etc. (i.e., the details)	• Be more aware in crowds • Will be difficult to focus, but look at the whole picture • Back up in a situation will allow an individual to focus on more of the situation • Having a mind set of the particular crime will make you more focused and aware of your current surroundings • Acquire knowledge of the roles of the people in the situation • Get the crowd baseline and the bad guy will stick out like a sore thumb • Look for compliance • Look for the unusual • Look for anything inconsistent • Look for extremes • Look for something that looks out of place and doesn't match

Table 5 con't. Expert strategies regarding how to use nonverbal cues to detect a threat.

Strategy	**Facilitated by Interview Question (Qualitative Responses)**	**Plans, Actions, and Prescriptions to Obtain Advantage**
Time to Evaluate (Category 1)	**Question 14**: About how much time do you think you ought to observe a person to decide whether that person is a suspect and deserves further observation? • As long as possible • Depends on cues • Sometimes instantly • The time needed to process situational information • The initial observation usually alerts that a situation is not right • Depends on how fast the situational events unfold • Can't be done instantly unless behavior is blatant • As much time as you can get	• Follow up on first observations to be sure • Observe in a manner not to alert suspect to bias his or her behavior because s/he knows s/he is being watched • Observe until the suspicion is eliminated • Take as long as you need • There is never enough time and sometimes decisions will need to be made in a split second. • If observation is short, cues must be very strong and stand out to make a case for taking action • Trust your suspicion and stick with the suspicion until proven otherwise • You will need more time than you actually have
Practice (Category 2)	**Question 5**: Even when you're off duty, do you find yourself observing people? • You never stop observing • I constantly observe while off the job • I need to because you never know who you will run into • It is what we do • I look more while off the job • I always observe others • I am always looking around	• Be quiet and observe your surroundings • Observe anything unusual • Observe all the time • Observe people's patterns

Table 5 con't. Expert strategies regarding how to use nonverbal cues to detect a threat.

Strategy	**Facilitated by Interview Question (Qualitative Responses)**	**Plans, Actions, and Prescriptions for Use**

Learn
(Category 2)
	Question 19: Do you think certain people are more intuitive than others in detecting suspicious behavior and just are better at the job?
	
	• They are different but I don't know what it is
	• They see more than other people and may process information differently
	• It's innate because during the medal ceremonies, the same guys are always receiving medals
	• I know a few people who are intuitive
	• They can look at someone and immediately tell if s/he is suspicious
	• It's not training and experience
	• Everyone has an intuition about something
	• Intuitive people
	  ◦ are flexible
	  ◦ are detail oriented
	  ◦ possess a depth of knowledge
	  ◦ make wrong decisions but less than those who are not intuitive
	  ◦ have a passion about what they do
	  ◦ attempt to get as much information out of a situation as they can
	  ◦ have higher success rates in detection
	  ◦ are quicker in identifying details in a situation
	  ◦ have experience and training combined with natural ability
		• People can be trained to be intuitive
		• Can be developed
		• Training and experience can get someone to that level
		• If someone can articulate to you what you are to look for, then anyone can achieve that level
		• Those who possess the quality can train others to operate at the intuitive level
		• You can train people to operate at the level but you cannot teach common sense

3.7.1 Strategy 1: Evaluate nonverbal cues within a contextual framework (Cues & Context).

Rarely did SMEs discuss the use of nonverbal cues without thoroughly explaining the environment in which the cue would be found and when a person of interest would be likely to exhibit the cue. This suggests that nonverbal cues should not be defined within a framework that suggests an all-purpose context but a framework that specifically defines the contextual circumstances (i.e., who, what, where, when) surrounding the probable expectation of each individual nonverbal cue. Therefore, if people continue to think that all behavioral cues are broadly applicable for all situations of probable threat, people will continue to find it difficult to grasp how to use nonverbal information to interpret intentions, motives, and impending eventual threat (Ekman, 1999, 2001). The association of nonverbal cues with probable context can be guided by the probability property of the visual perception theory of relational violations (Biederman, Mezzanotte, & Rabinowitz, 1982), in that the visual perception of and comprehension of how to use nonverbal cues to judge threatening intentions should increase when one is able to associate nonverbal cues with the most probable situation in which they will likely appear (Brockmole, Hambrick, Windisch, & Henderson, 2008; Brockmole & Henderson, 2008). The ability to effectively blend nonverbal cues with their proper context will be shaped by experience, past events, and training (Endsley, 1995), which experts emphasized with 100% of 36 experts reporting that experience was an important factor in judging individuals with threatening intentions and 71% of 38 experts reporting that training would be helpful in judging individuals with threatening intentions.

3.7.2 Strategy 2: It is difficult to attend to all the important elements in a crowd; call for backup when necessary (SA in Crowds).

Eighty-five percent of 26 experts thought they would be effectively accurate in selecting an individual with threatening intentions in a non-crowd environment. In contrast, 62% of the same 26 experts thought they would be effectively accurate in selecting an individual with threatening intentions from a crowd. The difference in the percentage of experts reporting efficiency in selecting individuals with threatening intentions in a non-crowd versus a crowd situation supports the experts' opinion (96% of 25 experts) that it is more difficult to achieve SA in some situations. This less-than-ideal state of SA, which is caused by the inherent dynamic of a crowded environment, is revealing, specifically when 66% of 30 experts admit to committing threat detection errors such as using the wrong cues (26%) to evaluate an individual with harmful intentions or perceiving situational cues incorrectly (40%) when assessing potentially harmful situations. The author speculates that the threat detection error of incorrect cue perception is attributable to an incomplete error at Level 1 SA and an inaccurate error at Level 2 SA (Endsley, 1995; Klein, 1993). In a crowd situation, experts may find it difficult to attend to all the pertinent elements available in the environment. Depending on the level of activity in or surrounding a crowd, experts may miss crucial information that is needed to form a complete picture of the situation (Endsley, 1995), thus committing an incomplete error at Level 1 SA. Without knowledge of all the elements in the environment, experts will more than likely choose incorrect schemata to interpret the situation, thus committing an inaccurate error at Level 2 SA. The results were inconclusive about how often such errors were made. Based on a lower percentage of experts reporting efficiency for the detection of threat in a crowd environment, it appears that experts are cautiously aware of the limits they face in such an environment. It also appears that the experts have developed ways to function within this limitation. The experts

agreed (92% of 37) that a person intending to cause harm emits a different signal than someone with no intent to cause harm. Thus, the experts use specific prescriptions (Table 5) to visually detect this signal within a crowd to form behavioral baselines that are associated with pattern matching. Klein (1998) emphasizes that pattern matching is important for recognition-primed decision making which is imperative in the threat detection domain (or other situations) where an observer routinely enters a situation and must rapidly recognize the most significant objectives and cues for that situation.

3.7.3 Strategy 3: Observe each situation for a reasonable amount of time before making a threat/non-threat decision (Time to Evaluate).

Regardless of organization, two similar surveillance strategies emerged. One surveillance strategy emerged concerning how SMEs approach potentially threatening situations. Threat detection experts emphasized the necessity for observing an environment or situation for some period of time in order to decide if a threat is likely. This line of thinking is favorable for giving an observer a behavioral "baseline" to work from to establish what is normal (Ekman, 2001; White & Burgoon, 2001). According to 37 experts, 51% felt that only a little time was needed to detect behaviors considered inconsistent with the known or established baseline for specific situations and to categorize someone as threatening, which counters the baseline technique recommended for use by Vrij and Mann (2004). Vrij and Mann (2004) agree that baselines are helpful in highlighting deviations from the norm but disagree that one's response just before a lie (or hostile act) is a legitimate comparison with the response when there is speculation of a lie. Instead, they recommend comparing an individual's response in a lie situation with the same individual's response in a truthful situation but only if the two situations are of similar context. Therefore, Vrij and Mann (2004) do not recommend the use of baselines

for the detection of threatening individuals in crowds since it is assumed that the observer is unfamiliar with the individuals in the crowd. However, based on the above average performance of the Secret Service (Ekman & O'Sullivan, 1991) in detecting deceit in individuals they did not know, the use of baselines is important to consider.

3.7.4 Strategy 4: Constantly seek opportunities for practice to perfect threat detection skills (Practice).

Another surveillance strategy common for interview participants involves interview question 5 under "General Background Questions" (Table 4): "Even when you're off duty, do you find yourself observing people in crowds?" Eighty-seven percent of the 40 SMEs answered yes to this question, which shows that people working in the threat detection domain are not limited to "the office" for improving detection skills. The same experts added that it is automatic to always be on guard and they cannot turn it off, which may suggest that persons in the threat detection domain practice their skill not just on the job but in every aspect of their lives. They also explained that they were always scanning their environment for threatening people outside the job environment in places such as restaurants and during family outings. Two SMEs went as far as saying that they sleep in certain positions to give themselves an advantage if they should be confronted by a threatening person when sleeping. Thus, it appears that experts may cultivate their threat detection skill 365 days of the year. Endsley (1995) theorizes that training is a factor that helps to automate the decision process and practice obtained off the job (i.e., off-the-job training) may be just as important for expert performance in the threat detection domain since the off-the-job environments are virtually similar to the environments that experts in the domain encounter on the job.

3.7.5 Strategy 5: Learn from intuitive individuals who are better at threat detection (Learn).

Finally, 97% of 39 experts reported that certain people are more intuitive than others in detecting suspicious behavior. The experts also discussed colleagues who were thought to be inherently intuitive and situations that the colleagues were involved in that gave evidence of their intuitive abilities. In addition, explaining the concept of intuition as it applied to the skill of threat detection was not easy for the experts, but it was easy for them to articulate that the intuitive individuals they discussed seemed to always make correct assessments and decisions when involved in threatening situations.

Surprisingly, 65% of 20 experts admitted to sometimes choosing one action plan from various choices of action plans when entering a situation and making a decision about an individual's threat status. However, it was not determined how frequently experts used the decision-making strategy. Such a mode of decision making is in direct contrast to NDM (Salas & Klein, 2001) and the RPD model (Figure 4) which posits that experts make quick and automatic decisions based on their interpretation of the situational cues in the environment. It is thought that novices choose from various action plans to make a decision when they are new to a specific domain and gradually move into the expertise mode of decision making in which a decision is made automatically based on the perception of situational cues in the environment. Thus, the strategies obtained are information tools that can be used to help experts and novices make rapid and successful decisions regarding threat based on their interpretation of the situational cues in the environment.

3.8 Limitations

One limitation of this phase is the use of a structured interview which may not have provided the experts an opportunity to discuss other methods and strategies they use to judge the intentions and motives of potentially threatening people. The constraint of interview time may have also prohibited the experts from discussing other methods and strategies they use to judge the intentions and motives of potentially threatening people. In addition, experts may have been somewhat intimidated by several interviewers being present and may not have been fully open with their responses. Another limitation of this phase concerns the structure of the interview questions and the use of probes. Some of the interview questions may have had an influence on responses by biasing experts to respond in agreement/disagreement with the question. For example, if experts perceived a question as having a favorably negative viewpoint of the subject, the experts may have been inclined to report a negative response. While the use of probing questions helps to decrease irrelevant information during an interview, these types of questions have the potential to produce biased responses. Probes can sometimes provide hints about what aspects of a subject are thought to be important (even if the interviewee never considered as such) and cause alterations in an interviewee's original mode of thought (Ericsson & Simon, 1980).

3.9 Transition -- Phase 1 to Phase 2

One strategy (Time to Evaluate) was incorporated into the methodology that was used for the assessment of threat detection accuracy in Phase 2. Also, the strategies found in this phase were used in Phase 3 to design a training guide for training developers responsible for training the novice in the threat detection domain.

4. PHASE 2: ASSESSMENT OF EXPERT THREAT DETECTION ACCURACY

4.1 Objectives

- To evaluate the best medium for distinguishing a threat from a non-threat and for highlighting threatening people and nonverbal cues that indicate an imminent threat.
- To evaluate threat detection accuracy rates of experts in the threat detection domain.

4.2 Participants

Fourteen law enforcement officers (11 males; 3 females) were recruited for this study and were paid $60 each for their participation. All participants had at least 20/20 acuity (corrected or uncorrected) in both eyes. The mean age of participants was 37 years (*SD* = 8.81) [range of 25 to 55 years] with a mean of 13 years (*SD* = 6.55) [range of 3.5 to 23 years] of experience in the domain of threat detection. Participants had experience in the following law enforcement specialty areas: patrol, executive protection, community relations, detective unit, narcotics, and vice.

4.3 Stimuli and Apparatus

Real-life scenarios of various threatening and non-threatening situations were used as experimental stimuli: five threatening scenarios and two non-threatening scenarios. Visual scenarios were field developed with actors in a shopping mall in the Baltimore metropolitan area. Each threatening scenario consisted of people engaging in everyday activities and events at the mall with actors embedded in the scene who displayed nonverbal cue(s) that were relevant for a specific threat situation. For non-threatening scenarios, actors displayed no nonverbal cues.

Each visual scenario was 1 minute long (Figure 11). Written scenarios were developed, based on the content of the visual scenarios. Each of the seven visual scenarios was described in written form via a "story" format (Appendix C). Scenario footage was placed on a CD and loaded on a standard laptop. Scenario images were projected to a 6- by 8-foot viewing screen with the use of an Epson LCD Projector (Model, EMP-500). Participants were seated 12 feet from the viewing screen (viewing distance within the recommendations of the Society of Motion Pictures and Television Engineers; http://www.practical-home-theater-guide.com/Tv-viewing-distance.html).

4.4 Experimental Design and Statistical Analyses

A 2 x 2 within-subjects design (Table 6) was used to determine the effect of Scenario Type (threat, non-threat) and Scenario Medium (visual, written) on Overall ID accuracy. Condition orders for Scenario Medium (visual, written) were alternated. Seven of the fourteen participants received the visual scenarios for the first condition and the written scenarios for the second condition. In contrast, the other seven participants received the written scenarios for the first condition and the visual scenarios for the second condition. In addition, participants were assigned to one of two scenario viewing orders (Table 7). Seven scenarios were given for each scenario medium, of which, five were threatening scenarios and two were non-threatening scenarios (Table 8). A repeated measures analysis of variance (ANOVA) was used to analyze Overall ID accuracy.

a. Independent Variables

Scenario Type (threat, non-threat)
Scenario Medium (visual, written)

b. Dependent Variable

Overall ID accuracy (the percentage of correctly identified scenarios)

Table 6. Layout of 2 x 2 within-subject design for Scenario Medium and Scenario Type.

	Scenario Medium	
Scenario Type	Visual	Written
Threat	Subject 1 - 14	Subject 1 - 14
Non-Threat	Subject 1 - 14	Subject 1 - 14

Table 7. Scenario viewing orders.

Viewing Sequence 1	Viewing Sequence 2
Scenario 6	Scenario 5
Scenario 3	Scenario 3
Scenario 2	Scenario 2
Scenario 7	Scenario 1
Scenario 5	Scenario 4
Scenario 1	Scenario 6
Scenario 4	Scenario 7

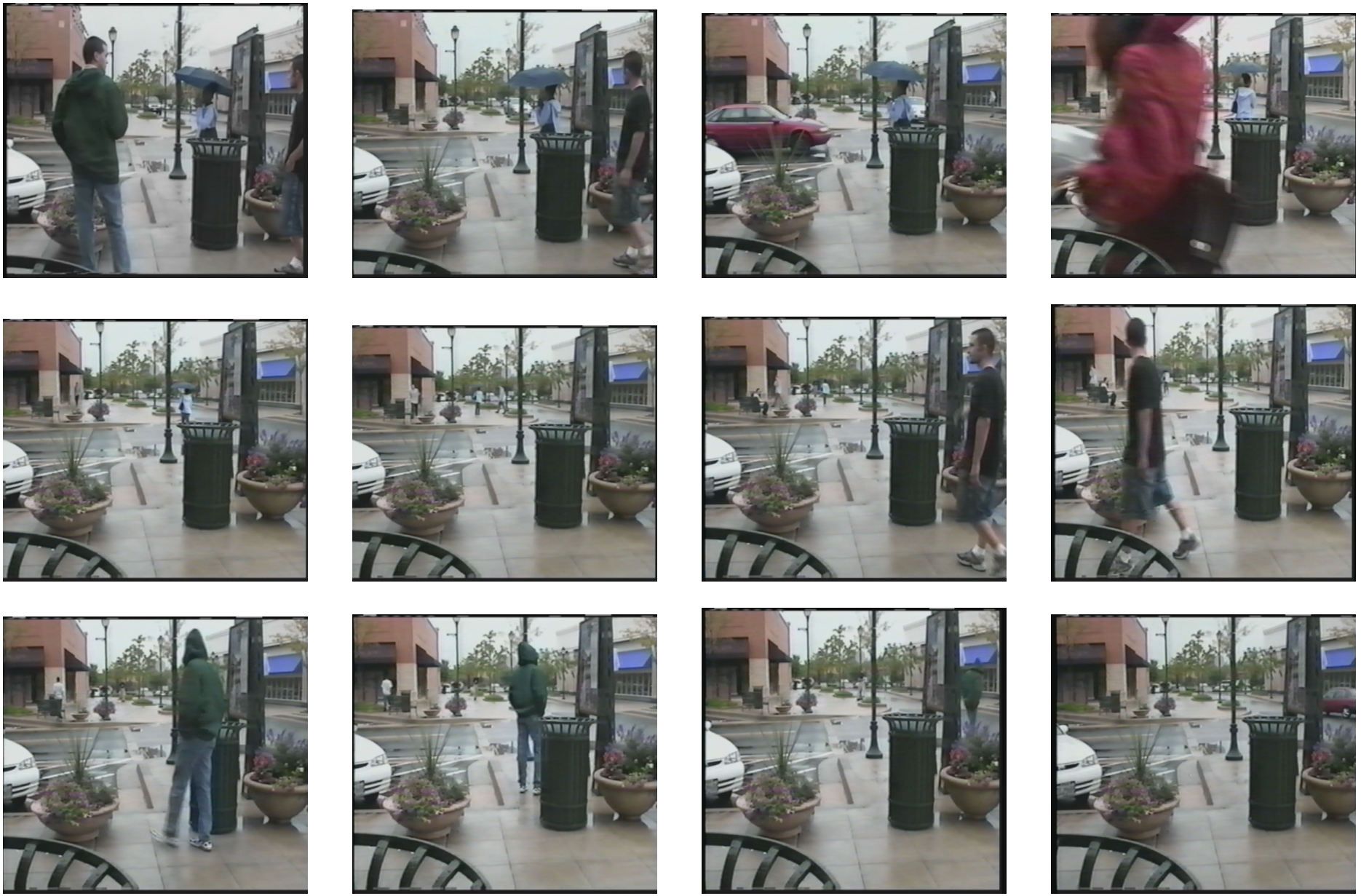


Figure 11. Example of a 1-minute visual scenario in still layout.

Table 8. Number of scenarios presented for each treatment.

	Scenario Medium	
Scenario Type	Visual	Written
Threat	5	5
Non-Threat	2	2

A t-test was used to evaluate the effect of Scenario Medium (visual, written) on Whom ID accuracy (the percentage of correctly identified persons), Cue ID accuracy (the percentage of correctly identified nonverbal cues), and the number of cues named (the total number of cues named, correct and incorrect). Whom ID accuracy, Cue ID accuracy, and the number of cues named were assessed for the threatening scenarios only. Each threatening scenario contained one threatening person and one specific nonverbal cue of interest. An alpha level of 0.05 was used for all statistical tests.

A t-test was used to evaluate the effect of experience (< 13 yrs. experience, > 13 yrs. experience) on Overall ID accuracy, Whom ID accuracy, Cue ID accuracy, and the number of cues named.

It was hypothesized that the visual medium would be most effective for distinguishing a threat from a non-threat and for highlighting threatening people and nonverbal cues that indicate an imminent threat.

4.5 Procedures

Each participant read and signed a consent form (Appendix D). Next, a Snellen visual acuity test was administered (in a dark room with an Optec vision tester) to ensure that all participants had at least 20/20 acuity (corrected or uncorrected) in both eyes. Each written scenario was arranged on individual sheets of paper, and participants silently read the scenarios to themselves. Each visual scenario (with no sound) was 1 minute long and participants were given 4 minutes to record a response. The experimenter did not control the time for each individual written scenario but gave participants 35 minutes to complete all written scenarios self-paced. The total time given to complete the seven written scenarios was based on the viewing time (1 minute) and response time (4 minutes) given for each visual scenario. All participants completed the written task within 20 minutes. For each visual and written scenario, participants identified the scenario as threatening or non-threatening. If participants identified a scenario as threatening, they were also instructed to identify the threatening person(s) in the scenario and the nonverbal cue(s) associated with the threatening individual(s). A flow chart of the decision response is shown in Figure 12.

Participant Decision-Response Matrix

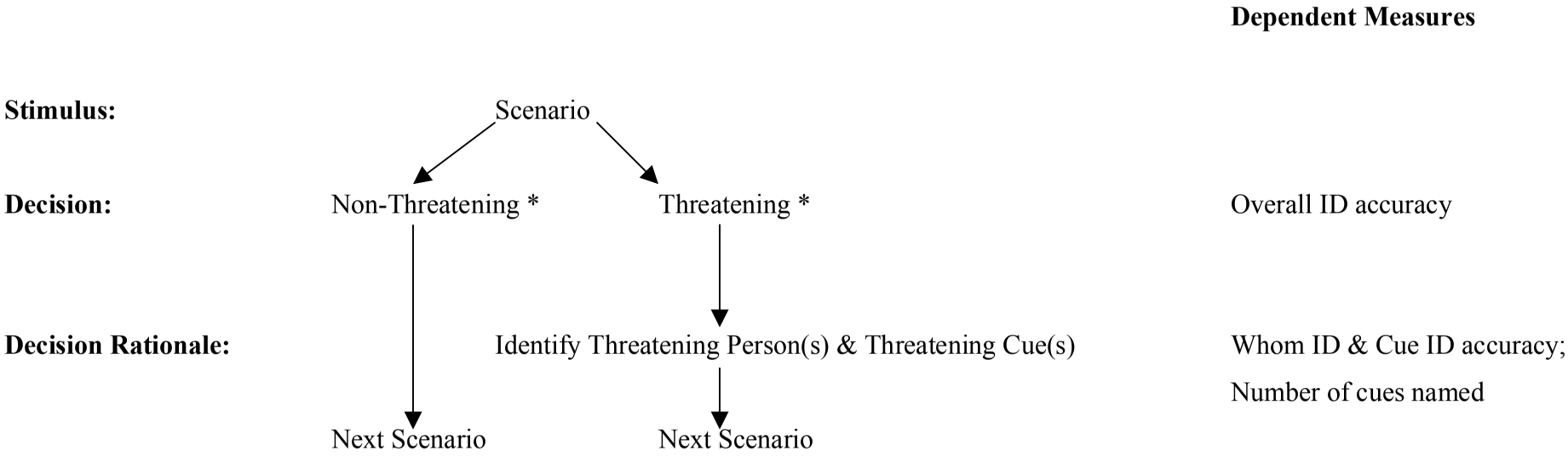


Figure 12. The procedural flow of the decision response for each scenario.

4.6 Results

4.6.1 Overall ID Accuracy

The hypothesis stating that the visual medium would be best for distinguishing a threat from a non-threat was not confirmed. A repeated measures ANOVA revealed no main effect for Scenario Medium, F (1, 13) = .44, p = .52, which indicated that Overall ID accuracy rates were the same for the visual and written media (Table 9). However, a significant main effect for Scenario Type, F (1, 13) = 31.27, p < .01, indicated that experts correctly identified a higher percentage of non-threatening scenarios (M = 91%) than threatening scenarios (M = 46%) (Figure 13). No interaction effect was found, F (1, 13) = 3.11, p = .10.

Table 9. ANOVA table for Overall ID accuracy.

Source	df	SS	MS	F
Between-Subjects				
Subjects (S)	13	12830.36	986.95	
Within-Subject				
Scenario Medium (M)	1	87.50	87.50	.44
M x S	13	2587.50	199.04	
Scenario Type (T)	1	28801.79	28801.79	31.27*
T x S	13	11973.21	921.02	
M x T	1	516.07	516.07	3.11
M x T x S	13	2158.93	166.07	

* p < .01

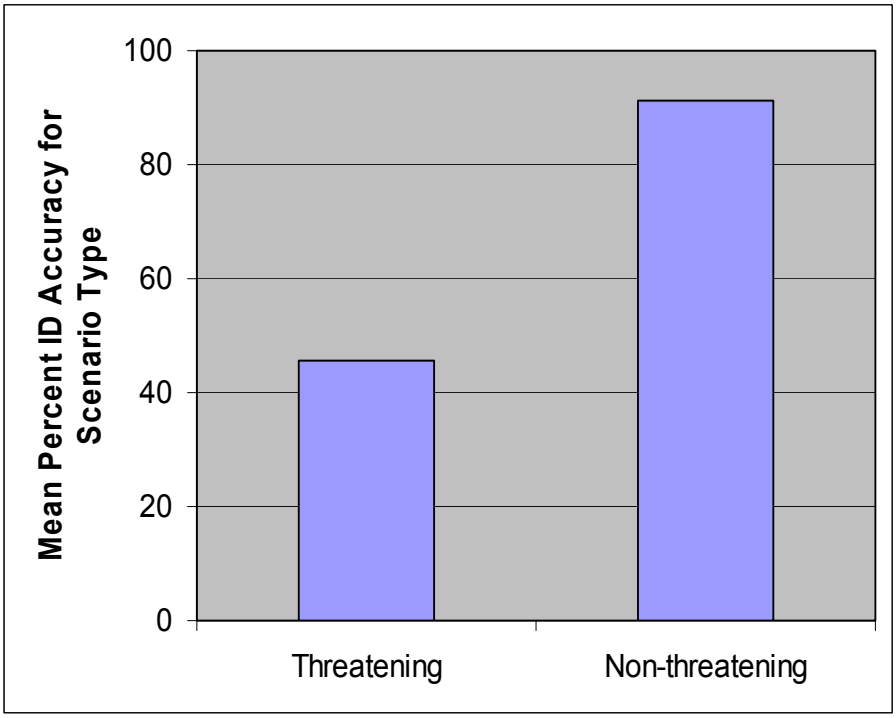


Figure 13. Percentage of correctly identified threatening and non-threatening scenarios.

To test the hypothesis that experts would achieve overall threat detection accuracy rates significantly above 50% or chance, a one-sample t-test was performed. The t-test indicated that overall threat detection accuracy rates obtained by experts in the visual medium (61%) approached significance for labeling above 50%, t (13) = 2.13, p = .05 (Table 10). However, overall threat detection accuracy rates obtained by experts in the written medium (56%) were not significantly above 50%, t (13) = 1.07, p = .31.

Table 10. One sample t-test for accuracy rates in the visual and written media.

	Test Value = 50					
	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
VISUAL	2.13	13	.053	11.21	-.16	22.59
WRITTEN	1.07	13	.305	6.07	-6.20	18.34

4.6.2 Whom ID Accuracy

The hypothesis stating that the visual medium would be best for the identification of threatening people was not confirmed. A paired t-test indicated that Whom ID accuracy rates did not significantly differ across Scenario Medium, t (13) = 1.08, p = .30.

4.6.3 Cue ID Accuracy

The hypothesis stating the visual medium would be best for the identification of nonverbal cues that indicate an imminent threat was not confirmed. A paired t-test indicated that Cue ID accuracy rates did not significantly differ across Scenario Medium, t (13) = .49, p = .64.

4.6.4 Cues Listed for Decision Making

The number of cues named is the number of cues listed for threatening scenarios, regardless of whether the cues were the correct cues displayed in the scenario. A paired t-test indicated that the number of cues named did not significantly differ across Scenario Medium, t (13) = 2.11, p = .06. Figure 14 shows the mean number of cues experts named for the visual and written media.

4.6.5 Experience Level Effect

Experts with more than 13 years of experience (n = 7) were compared with experts with 13 years or less experience (n = 7) in the threat detection domain. Independent sample t-tests indicated that years of domain experience had no effect on Overall ID accuracy, $t(12) = .48$, $p = .64$; Whom ID accuracy, $t(12) = .24$, $p = .82$; Cue ID accuracy, $t(12) = .34$, $p = .74$ or the number of cues named, $t(12) = .26$, $p = .80$.

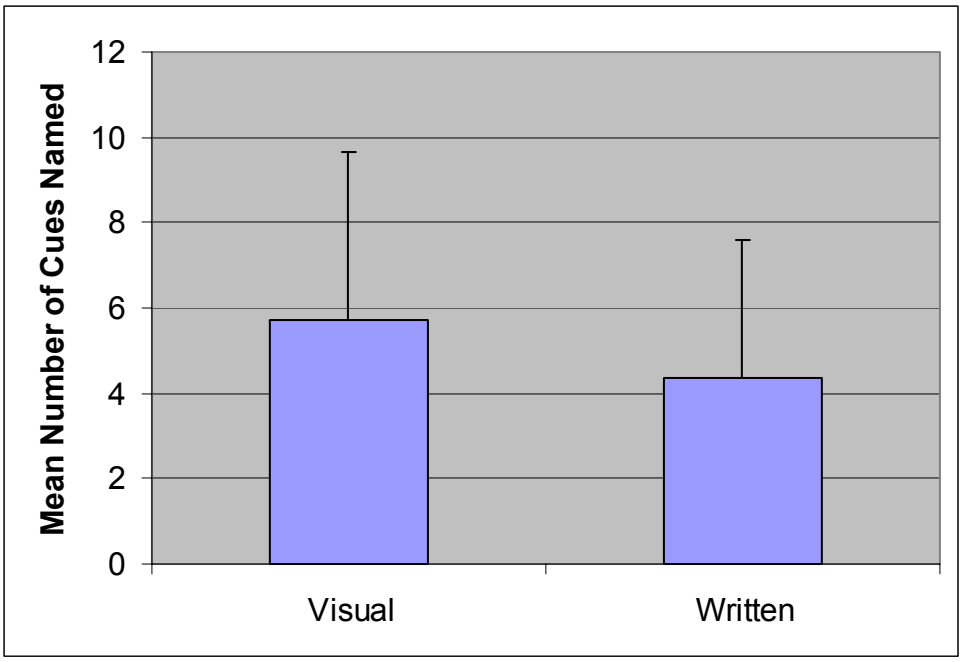


Figure 14. Mean number of cues named for the visual and written media. Error bars indicate SD.

4.6.6 Additional Findings

Of the 14 participants in this phase, 3 participants obtained accuracy scores that were consistently higher than the mean performance for all accuracy measures. Figure 15 contains the performance profiles for the three participants (Participant 4, Participant 7, and Participant 13).

Also, the three participants named approximately four times the number of nonverbal cues as a basis for decision making than participants with the poorest accuracy scores (Figure 16). In addition, participants 7 and 13 had more than 13 years of experience and participant 4 had less than 13 years of experience in the threat detection domain.

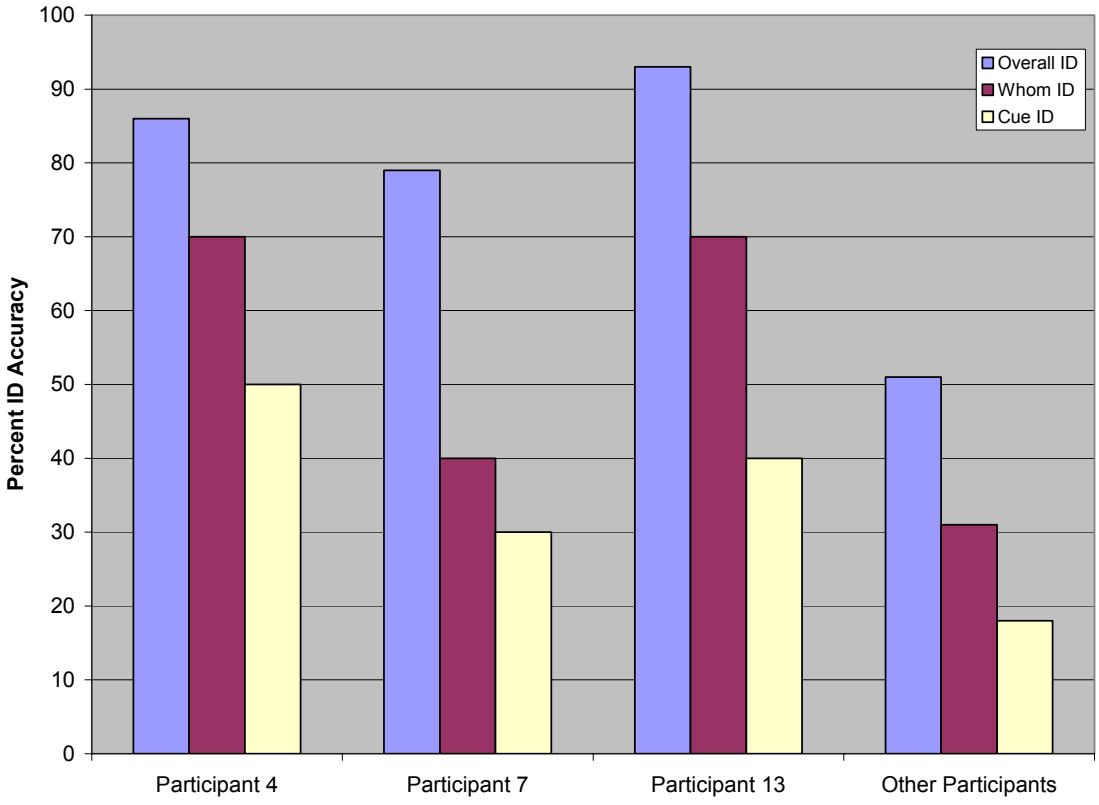


Figure 15. Performance profiles for the top three performing experts compared with the performance for the other experts.

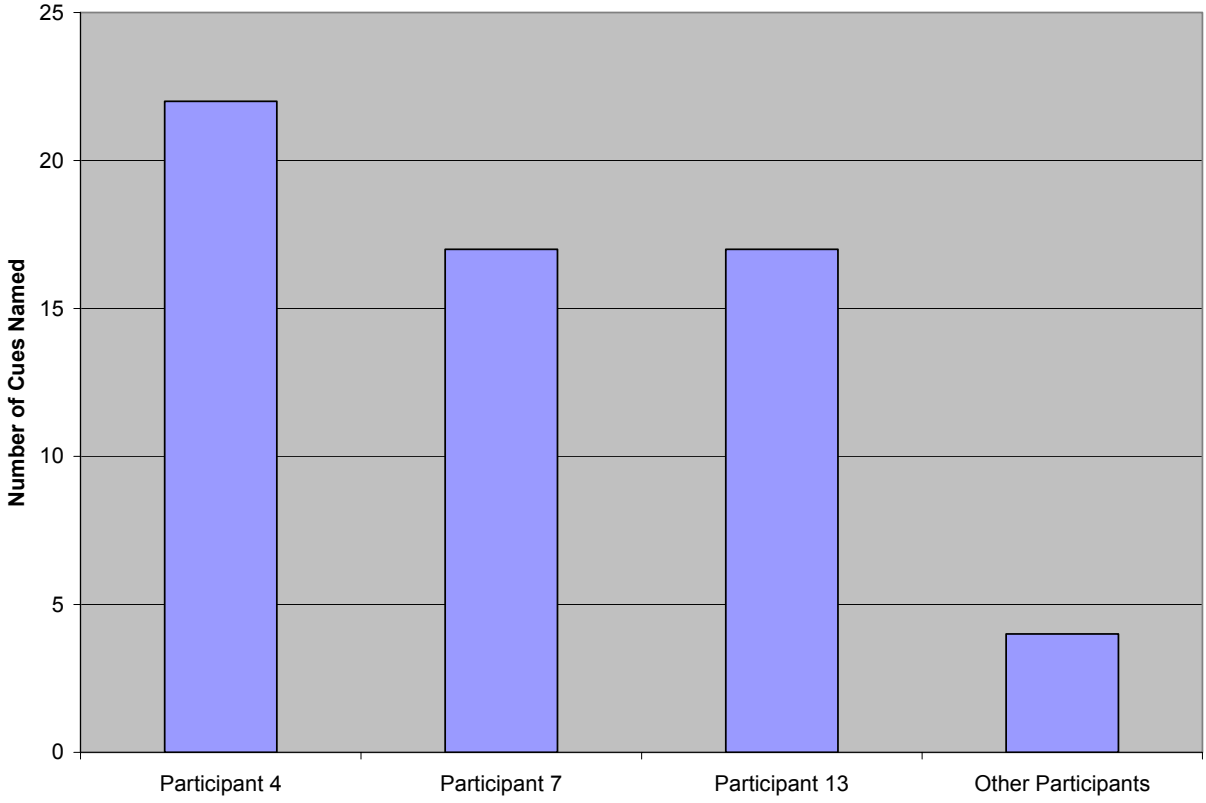


Figure 16. The number of cues named for the top three performing experts compared with the number of cues named for the other experts.

4.7 Discussion

In this phase, it was hypothesized that the visual medium would have an advantage over the written medium for distinguishing a threat from a non-threat and for highlighting threatening people and nonverbal cues that indicate a threat. This hypothesis was not confirmed. It is possible that at some level of expertise (acquired via experience and on/off- the-job practice), expert performance is not affected by the media or setting in which the threat is presented. The literature is consistent in reporting that accuracy rates for threat detection are approximately 50% (Levine et al., 1999; Vrij, 1994) and most of those reports are for settings that are different than

the crowd settings used in this research. According to a one-sample t-test performed for Overall ID accuracy rates, accuracy rates were found to be significantly above 50% for the visual medium (61%) but not for the written medium (56%). The performance level of experts in this study is comparable to the performance level found in the literature for similar detection tasks and represents only moderate performance (50% to 69%) in the threat detection domain (Atkins & Norris, 2004). It appears that the experts had more trouble accurately identifying threatening situations (46%) than situations with no threat (91%). This finding is consistent with Levine et al. (1999) who found lower accuracy rates for the detection of a lie than a truth. Phase 1 experts explained that it is more difficult to achieve SA in crowd/group settings than in settings with one or a few individuals. In a crowd situation, a number of things are happening and in an attempt to focus on what is important, the observer may miss pertinent information that is needed to make an informed decision regarding the threat status of the situation. This inability to achieve a high status of SA through the perception and comprehension of all situational cues may lead to the incorrect assignment of threat status. The moderate performance obtained by experts for the detection of a threat highlights the urgency for experts in the threat detection domain to use the strategy of evaluating nonverbal cues within a contextual framework. The plans, actions, and prescriptions listed for the Cues & Content and SA in Crowds strategies may be solutions for improving accuracy rates in the domain.

Confidence level in one's decision may be another contributing factor to the low accuracy rates for threatening situations. In situations of imminent threat, the goal is to identify the threat before it comes to fruition, and this may require more evidence for an observer to declare a threat. The findings in Phase 1 may support the concept of confidence in evidence since only 35% of 37 experts reported confidence in using observation techniques alone to

identify threatening people. Eighty-nine percent of 36 experts in Phase 1 reported that in addition to observation techniques, intelligence information was needed to identify threatening people. It is clear from the former statistic that there is a good amount of work that remains in building confidence in experts that observation alone can aid in identifying individuals with hostile intentions. However, in defense of the experts' trepidation regarding the use of observation techniques only to identify threatening individuals, Tversky and Kahneman (1981) acknowledge that the frame of a decision (i.e., visual perspective of a scene) can change over time, and making a choice (e.g., threat/non-threat) can be difficult because of the inconsistencies produced by different frames or perspectives over time. In addition, because high stakes (e.g., death, injury) are synonymous with the threat detection domain, the manner in which experts frame acts (i.e., shoot/no-shoot) and outcomes (i.e., death, injury) associated with a particular choice may reveal a rejection of responsibility for certain consequences (Tversky & Kahneman, 1981). Low confidence that a threat actually exists will more than likely lead to a decision with minimal consequences (i.e., non-threat). Increasing the experts' confidence in evidence will require more of the right type of evidence in which the expert is willing to accept responsibility for the acts and outcomes deemed necessary for the current perspective. The plans, actions, and prescriptions listed for the Practice strategy may help to cultivate the right type of evidence necessary to build confidence in evidence for an observer of threat.

The amount of nonverbal cue information extracted from a situation to make a judgment regarding threat may be a predictor of accuracy. The Information–Use Hypothesis assumes that experts use more information than non-experts for judgment and decision making. Yet, Shanteau (1992) disagrees and instead believes that experts use the same or fewer cues as the novice. However, he emphasizes that the information used by the expert is more relevant. The

three top performing experts identified in this phase named 17 to 22 nonverbal cues for decision making compared to an average of five nonverbal cues named by the remainder of the experts (Figure 16). The latter finding is similar to the findings of Sullivan and Siegel (1972) who found that police officers used an average of five pieces of information before making a decision. Sullivan and Siegel (1972) also found that less experienced officers required 6.1 pieces of information to make a decision compared to 3.8 pieces of information for the more experienced officers. This is in contrast to the results reported in this phase, which show that the experts with the highest accuracy rates named more cues to reach a decision. Perhaps this may imply that the Information-Use Hypothesis may be highly relevant for threat detection since it has been reported that most people, including experts, miss or ignore relevant cues for detecting threat (O'Sullivan, 2005). It may be true that the more information one can extract from a situation (albeit relevant), the higher the probability of being accurate in detecting threat. Thus, the plans, actions, and prescriptions listed for the Time to Evaluate strategy may be solutions to making experts aware of the actual time required for gathering as much information as possible to evaluate a situation.

In general, experts obtained the highest accuracy rates for Overall ID; however, accuracy rates for Whom ID and Cue ID were notably lower, with the poorest performance for Cue ID (Figure 15). This suggests that it may be possible to have a sense that a situation is threatening without successfully identifying the correct person(s) or behavioral cue(s) associated with the sense of threat, which may mean the shooting or detaining of innocent civilians. Gavin de Becker (1997), world-renowned security expert and author of "The Gift of Fear," discussed this phenomenon, stating that there are warning signs or pre-incident indicators to violence [or threat] and human intuition will detect them. He also argues that although we as humans try to analyze

the warning signs, sometimes we will come away with a concept of a situation without knowing why. According to the literature (Ekman, 1996), the SME interviews in Phase 1, and Overall ID accuracy rates found in this phase, it appears that approximately 1 minute or less is sufficient to detect the warning signs of a threat. Yet, more time may be required for experts to evaluate a situation to correctly extract Whom ID and Cue ID information. During the study, some participants requested to see a few scenarios a second time (the request was not granted), and in comparing accuracy rates, it appears the extra time was needed to extract more detailed information for Whom ID and Cue ID. The plans, actions, and prescriptions listed for the Cues & Content strategy may help to raise Overall and Cue ID accuracy rates while the plans, actions, and prescriptions listed for the Time to Evaluate strategy may help to raise Whom and Cue ID accuracy rates.

In Phase 1 of this project, interview question 19 under "Experience and Training" (Table 4) reads, "Do you think certain people are more intuitive than others in detecting suspicious behavior and just are better at the job?" Ninety-seven percent of 39 experts answered "yes" to this question. The performance profiles for those identified with exceptional accuracy rates consistently exceeded mean performance for the total sample on all accuracy measures (Figure 15). It is also apparent that those who are exceptional at detecting a threat are also able to extract much more information from their environments and to successfully integrate the information with previously acquired and stored knowledge, which is necessary for making rapid and effective decisions via the RPD approach (Figure 16). What is still not clear, however, is what specific strategies did the exceptional experts use to extract relevant information from the scenarios and do they match the strategies reported in Phase 1? Also, are there specific encounters of experience (rather than experience in general) that are more conducive for

improving threat detection? In addition, the plans, actions, and prescriptions listed for the Learn strategy appears to be a promising solution in improving average performance to superior performance in the domain.

4.8 Limitations

One limitation of this phase is the small sample size which may have contributed to the failure to find significance for Scenario Medium. Because of the low accuracy rates found for Whom ID and Cue ID, another limitation of this phase concerns the criteria for the selection of threat detection experts within an organization. Participants in this phase listed experience in a number of specialty areas, and detection accuracy rates may range from exceptional to poor depending upon the routine tasks required of an expert within an area. Thus, future criteria for threat detection expert selection should also include specialty area membership (Malhotra, Lee, & Khurana, 2007; Sullivan & Siegel, 1972). A third limitation of this phase was the limited amount of time allotted for information exposure for the visual scenarios. In an actual event, an observer might scan, rescan, and review a situation for more than 1 minute, perhaps making the laboratory situation highly unrealistic. This was evident since some of the experts requested to see a few of the scenarios a second time. Finally, the failure to control the written and visual scenarios in the same way (self-paced vs. not self-paced) may have affected this study's internal validity.

4.9 Transition -- Phase 2 to Phase 3

Concepts drawn from the literature, expert findings in Phase 1, and expert performance in Phase 2 were the basis for developing heuristics for a training development guide in Phase 3 named "Heuristics for Novice Training Development in the Threat Detection Domain".

5. PHASE 3: DEVELOPMENT AND EVALUATION OF TRAINING GUIDE

5.1 Objective

The objective of this phase is to design a training development guide for training developers in the threat detection domain. The training development guide contains heuristics (i.e., rules of thumb) that will help the novice to quickly integrate domain knowledge (i.e., use of nonverbal cues and strategies) and real-world situations. In other words, novices should be able to take what they have learned about the domain and go into the field and successfully distinguish threatening individuals from non-threatening individuals. The guide was designed to be used by training developers in the domain to design a new training program or update an existing training program to ensure that the program includes the basic rules of thumb that experts agree are important and relevant for training the novice to detect a threat.

5.2 Participants

Eight new law enforcement officers (3 males; 5 females) were recruited for this study and paid $60 each for their participation. The mean age of participants was 44 years (*SD* = 11.14) [range of 25 to 58 years] with a mean of 20 years (*SD* = 9.33) [range of 2 to 33 years] of experience in the domain of threat detection. Participants had experience in the following law

enforcement specialty areas: patrol, executive protection, community relations, detective unit, narcotics, vice, hostage negotiation, and call center.

5.3 Apparatus

A training development guide named "Heuristics for Novice Training Development in the Threat Detection Domain" was developed (Table 11) where the heuristics are not listed in order of importance. Concepts drawn from the literature and experts in Phases 1 and 2 were the basis for developing the heuristics in the training guide. Concepts deemed to increase SA, strengthen the perception of threat, aid in the comprehension of environmental elements, or strengthen the learning of domain information for the novice were included as heuristics in the training guide (Table 12). For example, Heuristic 1 (Define Situation) helps to increase SA by building one's understanding of non-verbal cues that indicate a threat and pairing appropriate non-verbal cues with specific situations. A clear definition of the elements for many situations will help to match the novice's "level of expectation" of what will happen in the field with what really happens in the field. Heuristic 5 (Multiple Scenario Showings) strengthens the perception of threat and aids in the comprehension of environmental elements by allowing novices to strengthen their mental model and elements within the model for any particular situation with each repeated viewing of a scenario. Heuristic 6 (Reasons for Decision) strengthens the learning of domain information by allowing novices to correct errors in the decision-making process. Based on the reasons novices give for making decisions, training instructors can help novices to change, correct, and reorganize domain information to correct decision making errors.

The heuristics in the training guide were also developed to support the use of the strategies obtained in Phase 1 (Table 13). The guide will help domain personnel in designing effective

threat detection training programs. The guide will also help personnel to improve existing threat detection training programs.

Table 11. Training development guide for designing effective threat detection training programs.

Heuristics for Novice Training Development in the Threat Detection Domain	
Heuristic 1 (Define Situation)	Clearly define the situation.
Heuristic 2 (Visual Content)	Visual versus written or oral scenarios are best for portraying a non-verbal threat.
Heuristic 3 (Portray Non-Threat)	Incorporate visual scenarios that contain no threat.
Heuristic 4 (Include Lectures)	Incorporate lecture-type teaching sessions to teach why and how specific non-verbal cues are associated with specific situations.
Heuristic 5 (Multiple Scenario Showings)	Show visual representation or scenarios more than once.
Heuristic 6 (Reasons for Decision)	Require new personnel to include reasons for decisions made…why that decision?
Heuristic 7 (Refresh Skills)	Refresh threat detection skills and knowledge for all personnel, especially new recruits, as often as permitted.
Heuristic 8 (Identify High Performers)	Identify and keep cumulative training records for above-average performing personnel.
Heuristic 9 (Improve Content)	Continuously improve the content of visual scenarios.

Table 12. Rationale for the inclusion of heuristics in the training development guide.

Heuristic	Inclusion Rationale	Supporting Source
1. Clearly define the situation.	• Builds understanding of non-verbal cues that do/do not indicate a threat • Increases situation awareness. • Non-verbal cues of threat are situation specific. • Used to build some "level of expectation".	• Endsley, 1988, 1995 • Klein, 1998 • Hedlund, Antonakis, & Sternberg, 2002 • Colwell et al., 2006
2. Visual versus written or oral scenarios are best for portraying a non-verbal threat.	• Visual stimuli strengthen the visual perception of a threat. • Visual perception strengthens an individual's understanding of the environment. • An understanding of the relationship between nonverbal cues and specific environmental settings strengthens the visual perception and comprehension of the environmental elements.	• Biederman et al., 1982 • Endsley, 1988, 1995 • Klein, 1998 • Lievens & Sackett, 2006 • Fiore et al., 2003 • Colwell et al., 2006
3. Incorporate visual scenarios that contain no threat.	• Needed as a contrast to threat to teach new recruits what situations with no threat look like. • Personnel cannot always be in "on" mode so recognition of non-threatening situations gives brief periods to operate in "safe" mode. • Helps personnel to focus on relatively more probable situations of threat.	• Phase 1: (Question 5 of General Background Questions; Appendix A); 35 of 40 experts admitted they observe people off duty; even during family outings. • Bond & DePaulo, 2006

Table 12 con't. Rationale for the inclusion of heuristics in the training development guide.

Heuristic	Inclusion Rationale	Supporting Source
4. Incorporate lecture-type teaching sessions to teach why and how specific non-verbal cues are associated with specific situations.	• Provide the specific non-verbal cue(s). • Place the non-verbal cue in context. • When a visual stimulus of the non-verbal cue is presented, it will strengthen what was learned in the lecture.	• deTurck & Miller, 1990 • Vrij, 1994
5. Show visual representations or scenarios more than once.	• Some new recruits will need to see visual representations more than once. • Presenting the visual scenarios a number of times will aid new recruits in practicing how to establish "normal" baseline behaviors for specific situations.	• Phase 1: Experts stated the need to establish a "baseline" for determining threat. • Phase 2: Experts requested to view specific scenarios more than once. • Ekman, 1996, 2001 • White & Burgoon, 2001
6. Require new personnel to include reasons for decisions made…why that decision?	• Answers will reveal information about the new recruit's decision-making process. • The training instructor will have some idea of how to help the recruit change, correct, and reorganize situational and cue-related information to correct SA errors.	• Ekman, 2001

Table 12 con't. Rationale for the inclusion of heuristics in the training development guide.

Heuristic	Inclusion Rationale	Supporting Source
7. Refresh threat detection skills and knowledge for all personnel, especially new recruits, as often as permitted.	• Refresher training will reinforce knowledge that has been previously learned and acquired through experience. • Permits personnel to modify and update their knowledge base to maintain a high level of SA.	• Phase 1: (Question 2 of General Background Questions; Appendix A); experts must take, as a requirement for the job, a certain number of hours of training each year. • Colwell et al., 2006
8. Identify and keep cumulative training records for above-average performing personnel.	• Opportunity to learn from successful individuals in the domain. • Recruit this group of personnel to help design and update training modules and materials. • Excellent personnel choice to facilitate training sessions. • Difficult-to-explain domain concepts may be easier to teach with real-world examples. Above-average personnel are likely to possess relevant examples.	• Ekman, 2001 • O'Sullivan, 2005 • Hedlund et al., 2002
9. Continuously improve the content of visual scenarios.	• As new tactics are developed by the enemy, visual scenarios should be updated to include these tactics. • Opportunity to learn from actual incidents. • Exposure to examples of the visual tactics will allow personnel and new recruits to transfer this training to real-world situations and immediately identify the new tactical behaviors and events as they unfold in the field. • Helps in maintaining a high level of SA.	• Phase 1: One expert explained that criminals and law enforcement officers often mirror each other via behavior. Each side often changes tactics based on what the other does. • Hedlund et al., 2002

Table 13. Heuristic support for strategy use.

	STRATEGY				
HEURISTIC	**Cues & Context**	**SA in Crowds**	**Time to Evaluate**	**Practice**	**Learn**
Define Situation	- Situation context defined (who, what, where, when) - Cue(s)/situation match - Develop/store behavior patterns				
Visual Content	- Visual memory map of cues with context - Develop/store behavior patterns	- Visual memory map of the dynamic of crowds - Develop/store behavior patterns			
Portray Non-Threat		- Visual contrast to threatening situations - Less time spent on non-relevant information			
Include Lectures	Can promote the notion that cues are not isolated but have contextual substance				
Multiple Scenario Showings	Develop/store behavior patterns		Realistic view regarding how much time is actually required for situation assessment		

Table 13 con't. Heuristic support for strategy use.

	STRATEGY				
HEURISTIC	**Cues & Context**	**SA in Crowds**	**Time to Evaluate**	**Practice**	**Learn**
Reasons for Decision					Instructor is instrumental in helping the novice to change, correct, and reorganize situational and cue-related information to correct errors
Refresh Skills				- Reinforce former knowledge - Integrate newly acquired knowledge - Modify/update knowledge connections	
Identify High Performers					- Novices learn from successful individuals in the domain - Instructors teach and explain complex domain concepts
Improve Content		Help in building a large repertoire of crowd behavior patterns			

5.4 Training Guide Evaluation

Eight experts in the threat detection domain evaluated the training development guide. The purpose of the evaluation was to obtain quantitative data about the importance and relevance of the training guide. The evaluation methodology, known as expert validation, was based on work by Bos, van Gurp, Verpoorten, and Brinkkemper (2005). Bos et al. (2005) extended Nielsen's (1994) set of heuristics for a content management system (CMS)[2] and recruited SMEs in the CMS domain to validate whether the new heuristics were relevant to the domain. The Heuristic Validation Questionnaire (Appendix E) included five constructs: three constructs used by Bos et al. (2005) (i.e., Relevance, Importance, and Violation) and two constructs (i.e., Integration and Universal Domain Use) that provided information about the use of the heuristics across the domain of threat detection. The relevance, importance, and violation constructs were chosen because their operational definitions were universally intuitive, they provided direct feedback regarding expert opinion, and they were advantageous in support of the specific content of each individual heuristic. Data obtained from the evaluation helped to refine the content of the training development guide by identifying changes necessary for training guide improvement, specifically the deletion of heuristics not deemed relevant by experts.

5.5 Procedures

Each participant read and signed a consent form (Appendix F). Participants were given the Heuristic Validation Questionnaire which contained the nine heuristics from the "Heuristics for Novice Training Development in the Threat Detection Domain". Each participant was instructed to evaluate each of the nine heuristics for relevance, importance, violation, integration, and universal domain use, using a 5-point scale (Table 14). Participants were also instructed to

add new heuristics to the original list if deemed critical for training novices in the area of threat detection.

Table 14. Construct questions and scale anchors for the heuristic evaluation.

Importance:

How important do you think this heuristic is to follow as a "rule of thumb" when one is designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

Relevance:

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

Violation:

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

Integration:

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

Universal Domain Use:

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

[2] CMS is a web application used for organizing, storing, and managing information for a web site.

5.6 Results

The hypothesis was confirmed which stated that a training development guide of heuristics for the development of threat detection programs for novices in the threat detection domain would be considered important and relevant by domain experts. In general, a high percentage of responses (across heuristics) for importance (89%) (Figure 17), relevance (93%) (Figure 18), and integration (89%) (Figure 19) consisted of ratings on the high end of the rating scale (i.e., ratings of 4 and 5). The percentage of responses (across heuristics) for violation (Figure 20) and universal domain use (Figure 21) are also shown. The percentage of expert responses contained in the 4 and 5 rating categories for violation (54%) and universal domain use (64%) were moderate and may highlight the need to adjust or delete heuristics. Domain experts also suggested the addition of three new heuristics: gather background information about recruit's prior experience, require longer training time in the field, and select highly qualified personnel to teach. Of all the heuristics, Heuristic 8 (Identify High Performers) is identified for possible adjustment or deletion. Figure 22 shows the percentage of expert responses for each construct by rating category for the heuristic. Graphs of each of the other heuristics showing the percentage of expert responses for each construct by rating category are presented in Appendix G.

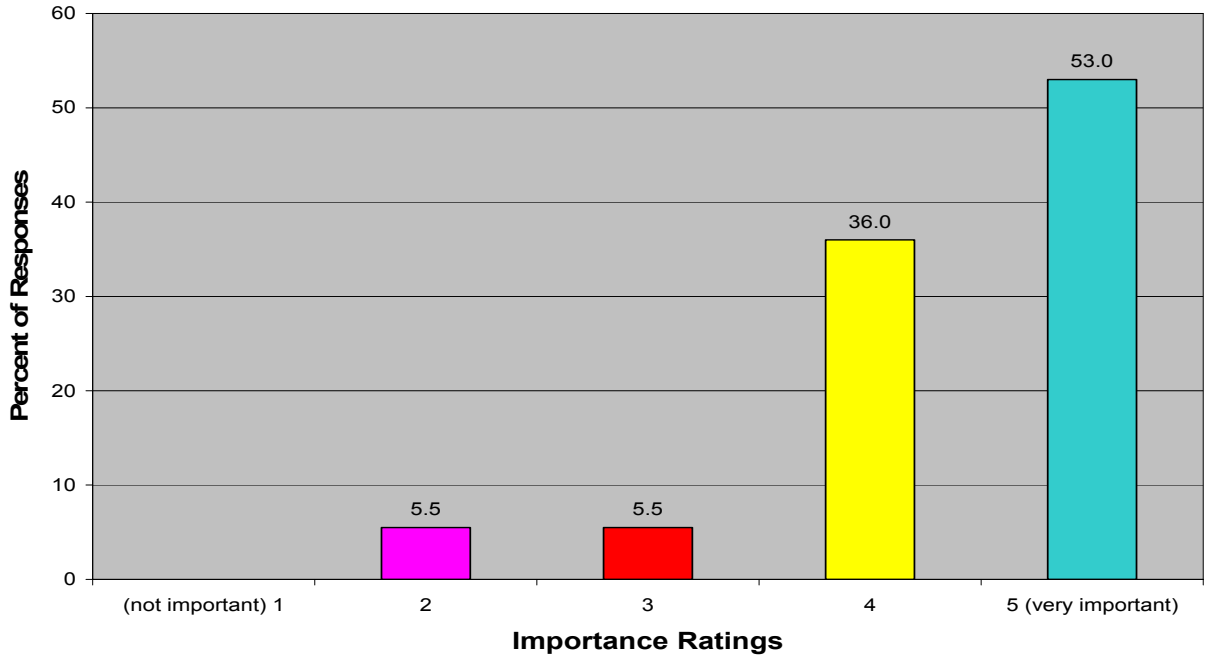


Figure 17. The percentage of responses (across heuristics) for each rating level of the importance construct. (Total responses = 72.)

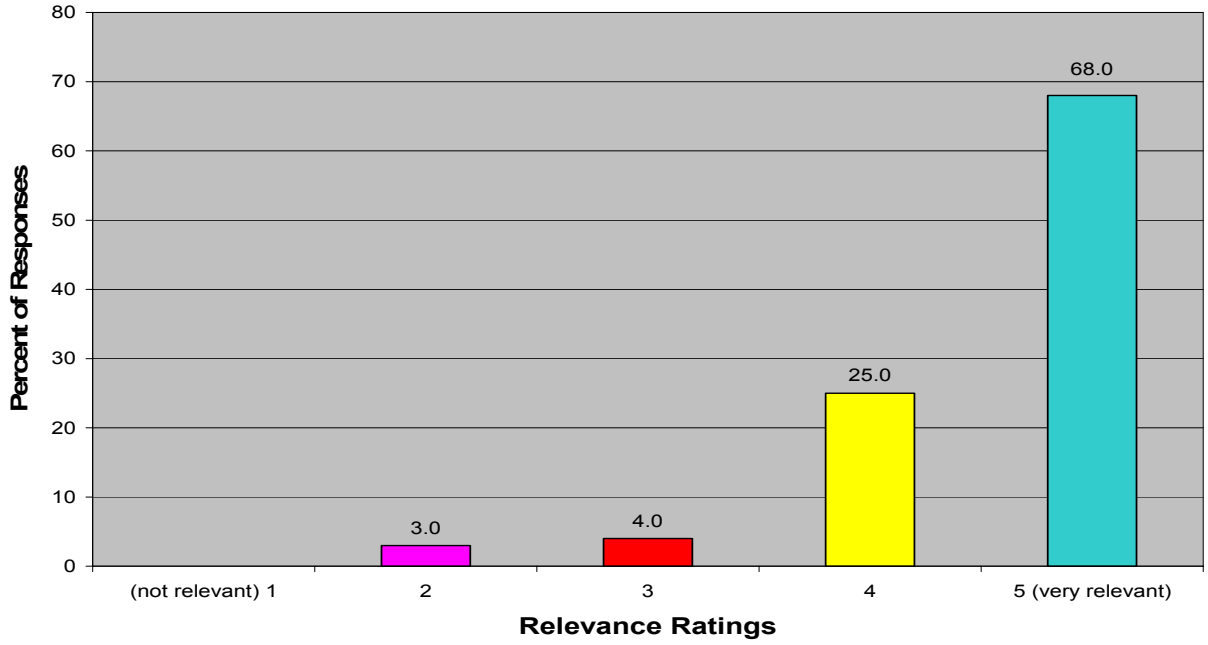


Figure 18. The percentage of responses (across heuristics) for each rating level of the relevance construct. (Total responses = 72.)

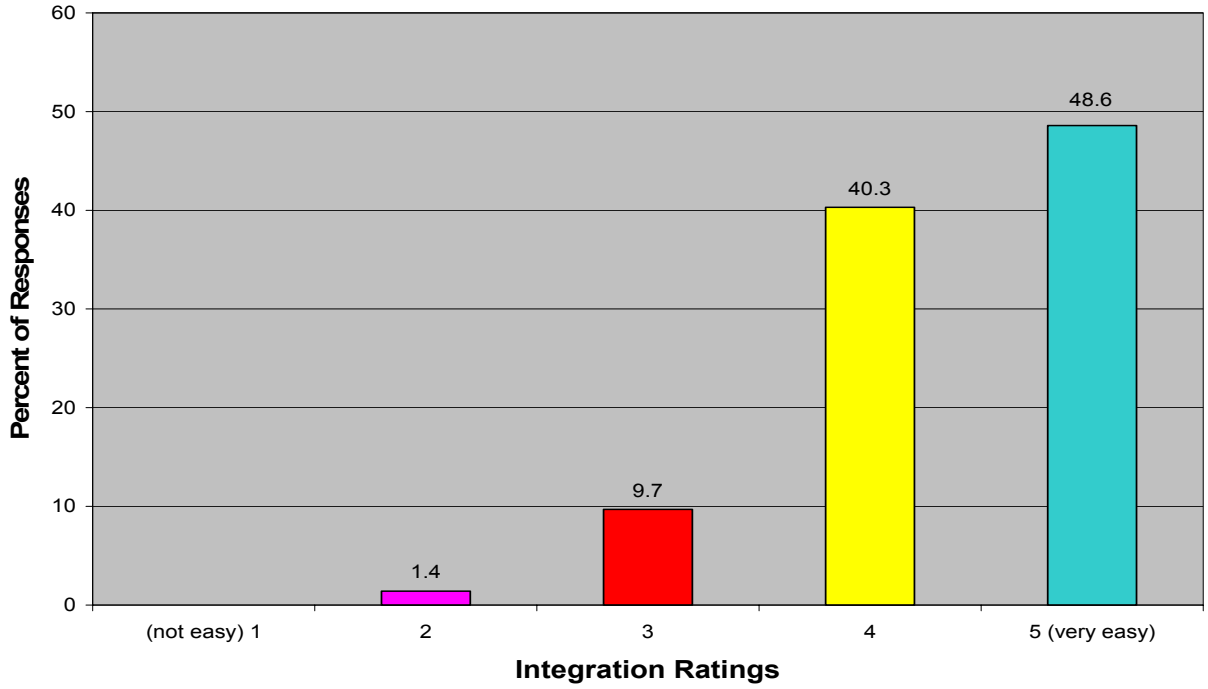


Figure 19. The percentage of responses (across heuristics) for each rating level of the integration construct. (Total responses = 72.)

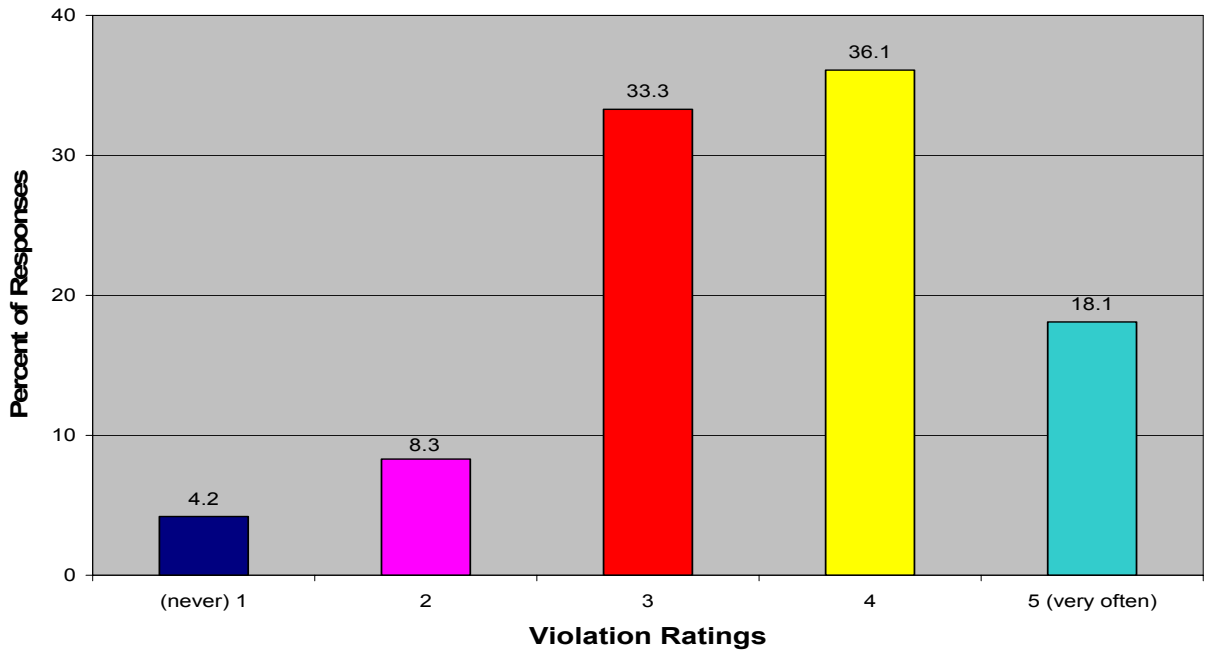


Figure 20. The percentage of responses (across heuristics) for each rating level of the violation construct. (Total responses = 72.)

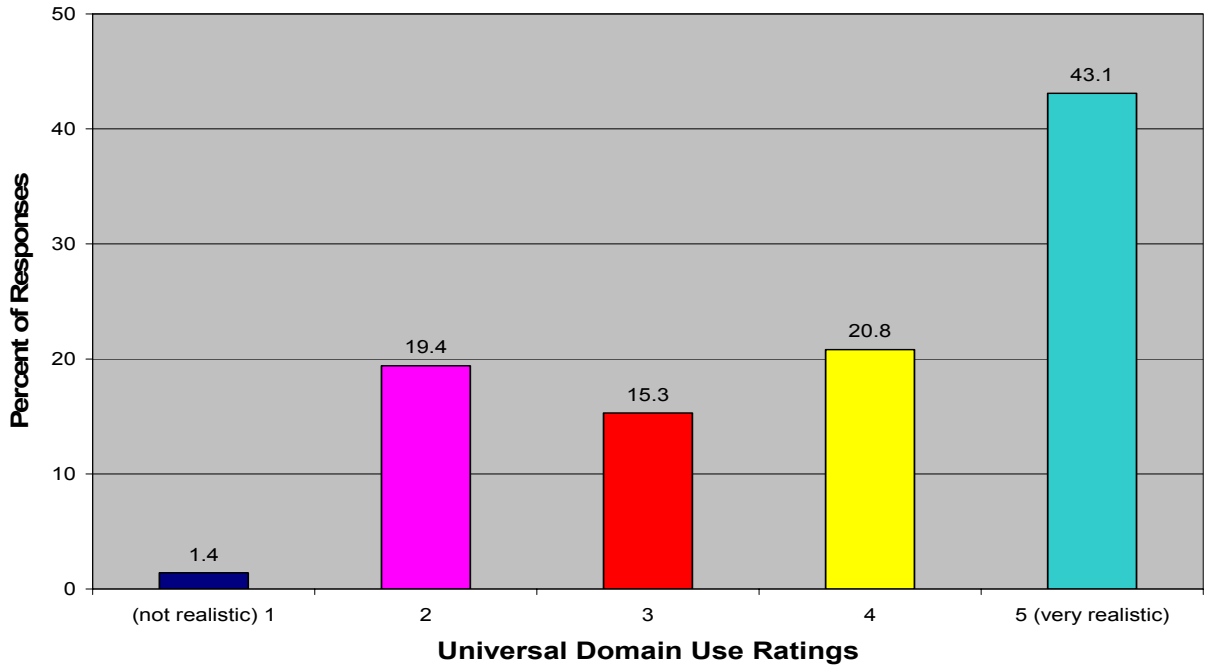


Figure 21. The percentage of responses (across heuristics) for each rating level of the universal domain use construct. (Total responses = 72.)

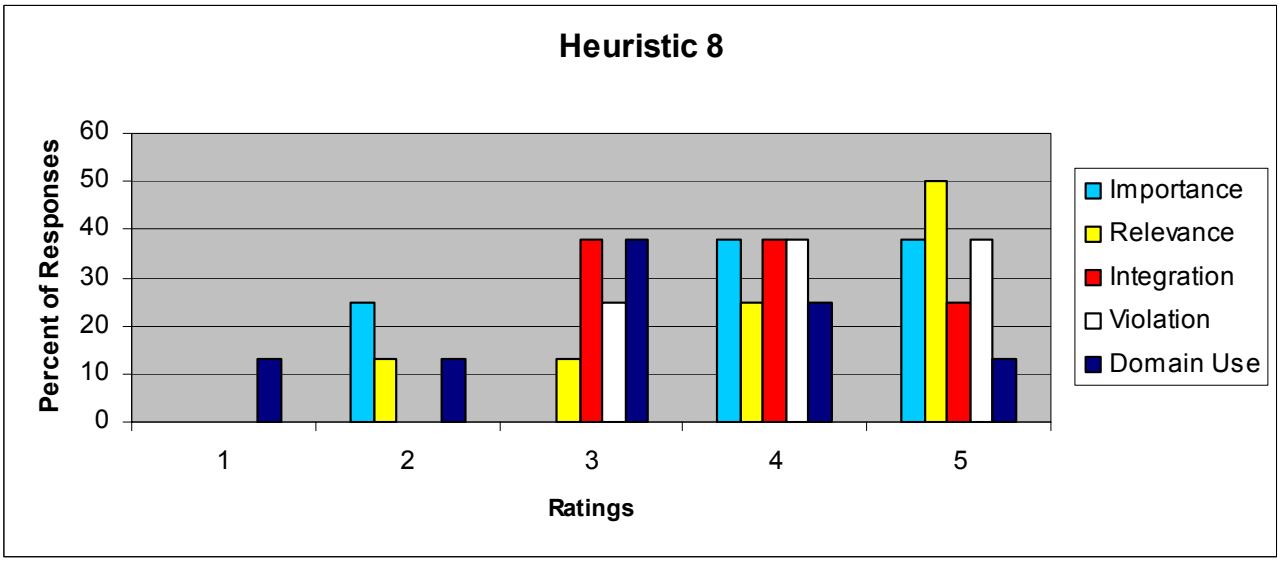


Figure 22. The percentage of expert responses for each construct by rating level for Heuristic 8 (Identify High Performers). (Total responses for each construct = 8).

5.7 Discussion

A high percentage of expert responses revealed that adherence to the set of training rules included in the "Heuristics for Novice Training Development in the Threat Detection Domain" is important (89%) and relevant (93%). A high percentage of expert responses also revealed that the heuristics are easy to integrate (89%) into an existing threat detection training program. The percentage of responses for importance and relevance in this study is similar to the percentage of responses found in other studies for the same constructs (Cuddy et al., 2004; Reardon, Lenz, & Folsom, 1998; Rossing, Hansen, Krass, & Traulsen, 2003). Rossing et al. (2003) evaluated pharmacist importance ratings (1 = vitally important to 5 = not important) for informing patients about 10 medicine-related problems when dispensing medication. They concluded that the pharmacists rated 2 of the 10 problems as most important based on 84% and 91% of the responses for those problems being rated as vitally or very important. Likewise, Reardon et al. (1998) assessed the relative importance (1 = very important to 4 = less important) that employers place on student participation in non-classroom activities. They too based their findings on the percentage of respondent ratings and concluded that of eight non-classroom activities, employers viewed job-related work experience (89%) and a leadership role in a student organization (86%) as most important. Cuddy et al. (2004) used similar methodology to assess the validity of the United States Medical Licensing Examination (USMLE) Step 2 Clinical Knowledge (CK) examination. They assessed the degree to which physicians (i.e., experts) viewed the exam content (150 multiple-choice questions) as relevant to one's ability to safely and effectively practice medicine. Based on 92% of the judgments indicating relevance, Cuddy et al. (2004) believed the exam's content to be relevant to clinical practice.

The percentage of high ratings across the nine heuristics for importance, relevance, and integration validate that the heuristics are important to follow as "rules of thumb" when one is designing a training program to help novices acquire the skill of threat detection, relevant for teaching novices to detect threats, and easy to integrate into an existing threat detection training program. The responses for the violation construct show that experts felt that the heuristics were sometimes or often violated in threat detection training programs and because the experts also thought the heuristics were relevant and important for training, this helps to highlight the significance of fielding the training guide. The responses for the universal domain use construct show that experts thought the heuristics were at least realistic for use by most law enforcement agencies in designing a threat detection training program.

Of all the heuristics, a higher percentage of experts rated Heuristic 8 (Identify High Performers) the least favorable for importance, relevance, integration, and universal domain use. Seventy-six percent of the experts also rated the heuristic high for violation. Other than Heuristic 3 (Portray Non-Threat), violation ratings for Heuristic 8 (Identify High Performers) were higher than all the other heuristics, so it appears that the other heuristics were rated as rules of thumb being regularly practiced in current programs but with a moderate amount of violation. However, it appears the opposite is true for Heuristic 8 (Identify High Performers) since it is often violated. Therefore, if a heuristic is often violated in a training program, it is concluded that domain personnel will have limited experience with the rule and will judge the rule as not being relevant or important. In other words, if experts do not practice a particular phenomenon within their domain, it will not be relevant to them for completing job tasks. Experts judged Heuristic 8 (Identify High Performers) as not being a common practice in the domain of threat detection and judged it lower than the other heuristics as being important and relevant. This

unfamiliarity with the practice of Heuristic 8 (Identify High Performers) may be responsible for the wide range of construct ratings for the heuristic and highlights the urgency for experts in the threat detection domain to use the strategy of learning from the intuitive individuals in the domain. This strategy may be another solution for improving accuracy rates in the threat detection domain. Heuristic 8 (Identify High Performers) was included in the "Heuristics for Novice Training Development in the Threat Detection Domain" based on Interview question 19 (Table 4) and the 97% of positive responses for the question. Because most experts thought that certain people are more intuitive than others in detecting threats and are better at the job, Heuristic 8 (Identify High Performers) will remain (with no adjustments) as a heuristic to employ this talent to teach. The heuristic will also remain to facilitate the view that it is an important rule of thumb and strategy for improving performance in threat detection.

Of the importance, relevance, integration, and domain use constructs, a higher percentage of expert responses was concentrated at the lower end of the rating scale for universal domain use. Eighty-seven percent of the experts rated Heuristics 1 (Define Situation), 2 (Visual Content), and 7 (Refresh Skills) (Appendix E) as very realistic to use by most law enforcement agencies in designing a threat detection program. By contrast, at least 50% of the experts gave low to moderate ratings for more than half of the remaining six heuristics in the construct. Ratings for the remaining six heuristics are puzzling since all the heuristics are general and not specific to any organization or specialized area within the domain. However, a few explanations are offered. In Phase 1 of this project, it was stated that there are a number of organizations working in the threat detection domain, and in Phase 2, it was stated that within the domain of threat detection, there are a number of specialty areas within the threat detection domain. It is possible that these factors had an impact on expert ratings for universal domain use by

contributing to a limited perspective in connecting how the heuristics may work outside one's specific organization or division. Rating rules of thumb from a domain perspective forced experts to think outside their organization and to map their experience onto areas that may have been unfamiliar. Experts may have found this difficult to do and thus explains the low to moderate scoring across the realistic scale for universal domain use. Limited knowledge about another organization's practices, coupled with the uncertainty of how things are done in other organizations, may be the cause for high variability in the domain use ratings.

5.8 Limitations

Limitations for this phase included the absence of objective test and evaluation data to report the effectiveness of using the "Heuristics for Novice Training Development in the Threat Detection Domain" to design actual training programs in the threat detection domain. This could include (a) redesigning a current threat detection program that does not adhere to the heuristics and (b) evaluating the performance of novices in the domain with the existing and redesigned program. Also, the effectiveness of the training development guide can be evaluated by a comparison of accuracy rates for novices whose training program was developed with heuristics from the training guide and accuracy rates for novices whose training program was developed with training recommendations from deTurck and Miller (1990), Druckman and Bjork (1991), and Vrij (1994). Another limitation is that this project does not address threat detection when coupled with other technologies (e.g., automated threat detection systems); therefore, heuristics for such conditions were not included in the training guide and would have no impact for organizations that may be currently using such technologies in their threat detection training programs.

6. CONCLUSIONS

Researchers who have an interest in detecting individuals with covert mischievous intentions base their work upon the detection of lies and truths. This approach to detecting an individual's true intent relies on verbal communication from a possible suspect. However, there are circumstances when verbal communication is impossible (e.g., war, terrorist hiding in a crowd) before an observer must make a judgment regarding criminal or harmful intent. In such a case, it is crucial for the observer to rely on nonverbal cues to judge intent because the consequences associated with an intended threat may be death or mass destruction. This research was based on the latter perspective of judging intent and asserts that an individual with threatening intentions can be detected before the execution of a hostile act. In assessing expert judgments of threat using complex, dynamically changing situations of individuals with harmful intent among crowds, this project attempted to extract underlying factors that influence threat detection performance and strategies of expert decision making in the threat detection domain.

6.1 Contextual Importance of Nonverbal Cues

One underlying factor found in this study that appears to influence threat detection performance is the lack of contextual information that is associated with nonverbal cues that indicate threat. In general, when nonverbal cues are mentioned, or mentioned as a useful tool for the identification of threat, rarely is a context given for the expectation of the cues. Many in the literature (e.g., DePaulo et al., 2003; Martin, 2002; Vrij, 1994) that address cues of deception or deception detection performance fail to list the context or situations in which the cues of interest might appear outside the test setting. Ekman (1997, 2001) makes the important point that for cues to be of any value for uncovering deception, they must be evaluated within some context.

Thus, experts who miss pertinent cues when they are subtle or displayed briefly (O'Sullivan, 2005) are likely to miss them because they have no context from which to expect the cues (Endsley, 1988, 1995).

Failing to teach that these are the nonverbal cues most likely to appear in a shoplifting situation or these are the nonverbal cues most likely to appear in a situation where a person is concealing a weapon does not support the acquisition and use of tacit knowledge in the field. If training does not help the expert in recognizing relevant versus irrelevant cues for specific situations in the field, many individuals in the domain will continue to lack the tacit knowledge needed to increase their threat detection accuracy rates above chance (Hedlund et al., 2002). The expert is not totally without contextual information for nonverbal cues that indicate threat since the experts in this research showed some basis for contextual categorization of nonverbal cues. For one threatening scenario in Phase 2, all participants who judged the scenario as threatening also listed the correct nonverbal cues as the reason for their decision. This finding implies that it may be possible to specifically tie certain nonverbal cues to certain situations (DePaulo, Rosenthal, Rosenkrantz, & Green, 1982; O'Sullivan, 2003), which will help to build simple mental models for novices regarding the recognition of pertinent cues and threat.

Since all experts who answered one scenario correctly also gave the correct nonverbal cue as the basis for their decision, it is assumed that the situation was also encountered in training and in the field accompanied by the cue mentioned. Thus, when the experts were confronted with the situations in this study, the patterns shown were consistent with the patterns they had already acquired via training and experience. Pattern recognition often separates the expert from the novice, providing the expert with an advantage in quickly recognizing the relevant aspects of a situation and making rapid decisions while operating in the situation (Gobet

& Chassy, 2008; Klein, 2008). However, it appears that a good amount of information regarding how nonverbal cues inform the presence of impending threat is still not integrated into current mental models for average performing experts in the domain of threat detection. Presently, formed mental models in this domain could also benefit from integrating information about how combinations of nonverbal cues inform the presence of impending threat. Since people with mischievous intent rarely leak one cue as an indicator of such intent, taking what has been learned about individual cues and expanding training to include "this combination of nonverbal cues is most likely to appear in this situation" may go a long way in strengthening the patterns needed for experts to improve their behavioral cue recognition skills and detection accuracy rates. Vrij and Mann (2004) also advocate the systematic use of a combination of behavioral cues to improve threat detection rates based on results (Vrij et al., 2000) that showed detection rates did not improve when behavioral cues were used individually as a basis for threat.

Contrary to what has been stated in the literature, perhaps threat detection accuracy rates are no better than chance because experts are using the "right cues" with no contextual basis as a guide for judging impending threat. Contextually based nonverbal cues will be easier to learn and recognize and may decrease the time needed to build efficient threat mental models in the domain. In addition, the learning of cues in context will increase the effectiveness of training and will probably be more profound for novice performance. More importantly, contextually based cues will be instrumental in providing novices a paradigm for making judgments about threat. If the argument that nonverbal cues can be used to identify an impending threat is to be strengthened, a contextual basis must be found for most of the nonverbal cues that indicate a threat.

A constructivist approach to learning contextually based nonverbal cues during training would be most beneficial in that experts and new recruits would have control in constructing their own knowledge and understanding of the concepts. According to this approach, the learner acquires knowledge and understanding by actively participating in the learning activities and interacting with visual representations of the concepts (Chen, 2003; Ten Dam & Volman, 2004). Hands-on participation provides each learner the opportunity to reflect on, challenge, and update previously held conceptual knowledge which may lead to the reorganization of information and the construction of new mental models (Chen, 2003). Thus, a constructivist training approach is a mechanism for the acquisition of competence to effectively participate in the threat detection domain (Ten Dam & Volman, 2004) which is measurable via the transfer of acquired knowledge to real-world problem solving (Price, 1998). The constructivist view argues against a passive learning environment where instructors teach material content via lectures and learners memorize the content (Chen, 2003). However, a blend of both training approaches would be beneficial for the novice in the domain. Practice is initiated using prior knowledge regarding basic domain concepts which should be continually updated (integration of old and new conceptual knowledge) as the learner moves through different stages of a practice task. A novice in the threat detection domain will require initial exposure to domain concepts (Wolff, 2007) before practicing the use of the concepts, and a lecture-based learning environment is considered appropriate for the objective. For lectures, PowerPoint can be used to introduce domain concepts and these should consist of a mix of text, diagrams, models, and video scenarios. Discussion between instructor and student should occur throughout the lectures. Role players, computer-based training simulators, and shoot/no-shoot simulators can be used to facilitate active participation and hands-on training in the threat detection domain.

6.2 Intuitive Mode of Thought and Exceptional Threat Detection Performance

Interestingly, although experts were able to distinguish a threat from a non-threat at a rate above chance for the visual medium, they did poorly in distinguishing the persons and cues associated with the threat. Cue identification was worse than person identification when experts attempted to associate specific cues and people with threat judgments. It appears that a correct identification of impending threat is not guaranteed to yield a correct identification of the person(s) or cue(s) involved, which leaves many questions. These findings imply that there are still gaps in the decision-making strategies of experts in the threat detection domain (Vrij, 2004). For as much as we know, there is still a lot we do not know. According to Bond and DePaulo (2006), "Rather than marveling at the outliers in this literature, we are more impressed by the regularity of the results obtained" (p. 231). To explain the mistakes that the average performing experts in this domain make and to close the gaps in the decision-making strategies, the performance of detection "wizards" (O'Sullivan, 2005) in this domain may be the answer. What is it that they see, how do they process what they see, and what mental models have they formed to surpass the detection performance levels of the average performing experts in the domain?

Although moderate accuracy rates for detecting individuals with covert mischievous intentions are widely recorded in the literature, as with the three experts identified in Phase 2 of this study, there is evidence that there are a few experts whose performance is well above chance. O'Sullivan (2005) defines these experts as "wizards" and describes the wizards with the use of characteristics such as they are more aware of nonverbal behaviors and base judgments on the behaviors frequently, they use nonverbal behavior descriptors that are more sophisticated and unusual than those of non-wizards, and they possess knowledge of many kinds of people in many

kinds of situations. Bond (2008) found that "wizards" are more aware of the nonverbal cues in their environment; thus, it can be assumed that they have learned and organized the contextual foundations and meaningful patterns associated with the nonverbal cues that indicate threat (Myers, 2002). The "wizards" not only recognize the nonverbal cues when present but they also are aware of the connections that exist between specific cues and specific situations as well as the connections between the cues in specific situations and what they reveal about that situation (Myers, 2002). In other words, they are skilled at making sense of unpredictable situations by connecting the abstract with contextual and concrete cues (Weick, Sutcliffe, & Obstfeld, 2005). In an attempt to make such connections, "wizards" may engage in sense-making activity which is needed at such point that what is perceived is different from what is expected (Feldman & Chesley, 1984; Weick et al., 2005) or as the experts in Phase 1 revealed "when something is not in compliance or is inconsistent". The extent to which the "wizards" gain a sense of their situation depends upon their ability to continually update the abstract information (guided by mental model formation) in the environment by questioning, reconsidering, and elaborating on the inconsistencies of the data encountered (Klein, Moon, & Hoffman, 2006; Weick et al., 2005). This challenge of pattern inconsistencies produces situations that are more comprehensive and more resilient in the face of criticism (Weick et al., 2005) which Klein (2008) believes is an intuitive process. Klein (2008) states "a purely intuitive strategy relying only on pattern matching would be too risky…[due to] flawed options. A completely deliberative and analytical strategy would be too slow" (p. 458). It appears that "wizards" are able to establish a balance between the intuitive and analytical modes of thought because of the nature of expertise in which decisions are made automatically and rapidly. Reliance on intuition or the intuitive mode of

thought may also separate those experts with phenomenal detection accuracy rates from those with chance detection accuracy rates.

Bond (2008) refutes the theory that the competent use of the intuitive mode of thought separates individuals with phenomenal detection accuracy rates from individuals with chance detection accuracy rates. Instead, he suggests that "wizards" primarily use the nonverbal cues in their environment to make successful decisions regarding threat. The author cannot agree that "wizards" do not use the intuitive mode of thought to make decisions about a threat based on the method that Bond (2008) used to obtain intuition cues. Because intuition cues were not obtained concurrently with the lie or truth decision, it is not for certain that the lack of intuition cues collected during the second showing of the stimuli also existed when the participants first viewed the stimuli. The author also speculates that Bond (2008) found a lack of intuition cues to support lie/truth decisions because of the strict rules of evidence that govern convictions (Gigerenzer, 2007) in a court of law. Individuals who work in the threat detection domain have probably suppressed verbalizing that they sometimes use the intuitive mode of thought to make decisions regarding threat to avoid the dismissal of cases before going to court. Intuitive judgments are made rapidly, without much reflection or evidence and usually surface during periods of severe time pressure, information overload, and acute danger (Hodgkinson, Langan-Fox, & Sadler-Smith, 2008; Kahneman, 2003; University of Leeds, 2008). In contrast, analytical judgments are made more slowly, with deliberate effort. To effectively operate in situations of acute danger, the "wizards" in this domain must rapidly evaluate situations to generate optimal decisions concerning what to do next in order to avoid injury and/or death. It is also believed that the optimal decisions are those that are generated first (Klein, 2008). The exceptional threat detection rates achieved by the three "wizards" identified in Phase 2 speak to the quality of their

judgments with a balance of both the intuitive and analytical modes of thought. This may suggest that for individuals to be successful in the domain of threat detection, they must be receptive to information processed intuitively.

Alter, Oppenheimer, Epley, and Eyre (2007) found that people tend to use the intuitive mode of thought for decision making when information is processed easily, and they use the analytical mode of thought when information is processed with some degree of difficulty. In addition, information processed via the intuitive mode is affected by intuitive confidence (Simmons & Nelson, 2006). This may explain the performance of those in the domain with average detection accuracy rates. Since non-wizards are lacking contextual information associated with nonverbal cues that indicate a threat, the pattern-matching connections are not fully developed, which may lead to difficulty in processing the environmental data. This difficulty is likely to lead non-wizards to doubt the intuitive information received, thus lowering intuitive confidence which results in a deliberate switch to the analytical mode of thought. Analytical judgments are not desired in this domain for obvious reasons and may lead non-wizards to choose from a list of possible responses instead of generating one optimal response. Sixty-five percent of 20 experts in this project revealed some evidence of this in the interview phase by reporting that they make decisions by choosing among various options.

Gigerenzer (2007) explains that officers of the law must adhere to strict objective reasons as rationale for decisions, which may suppress the intuitive mode of thought in the threat detection domain. The objective reasons are mandatory for testimony in a court of law and any hint of an intuitive reason as evidence will likely be dismissed. Although the intuitive mode of thought appears to be essential for decision making in this domain, it also seems to be discouraged for the protection of citizens' civil liberties (de Becker, 1997; Gigerenzer, 2007).

Intuition may play a role in expanding our understanding of the experts' strategy in this domain and is worth further evaluation. Thus, "wizards" will be a valuable and crucial link in helping us to understand the connection between the intuitive mode of thought and successful threat detection performance.

6.3 Training in the Threat Detection Domain

After approximately interview number 10 in Phase 1, three-quarters of the information stated by participants in the later interviews had already been stated by participants in the earlier interviews. This duplication of information may reveal a similarity of schema among the experts and specifically that the experts have similar strategies and prescriptions for solving problems regarding threat (Klein, 1998). Perhaps this suggests that using nonverbal cues to detect a threat is a skill that can be taught. The strategies used by experts in this domain are crucial for the novice but especially for infantry soldiers because they do not have the luxury of time (as do new recruits in law enforcement agencies) to sharpen their skills in threat detection. Infantry soldiers will more than likely only use their skills in threat detection during times of civil unrest and war, if at all, and therefore will need to master and use these skills quickly. Training for the novice in the threat detection domain should focus on helping the novice to strengthen his or her repertoire of contextual tacit knowledge and helping novices to confidently manage a balance between the intuitive and analytical modes of thought.

The author asserts that an understanding of schema similarity within the threat detection domain should lead to improved training and subsequently to improved performance in the domain. From an opposite perspective, Kassin and Fong (1999) demonstrated that training can be an influential factor in shaping schema similarity in groups. They theorized that long-

standing training practices (i.e., Reid technique) in the threat detection domain may have helped to contribute to the inaccurate/incomplete mental models that are still universal today. Not only does this finding seem probable in explaining the inaccurate/incomplete mental models shared by experts in the domain, it may also present as one of the underlying reasons that detection rates are low to average. Kassin and Fong (1999) specifically blame the Reid technique for chance detection rates (also found in this study in Phase 2) across the domain because they believe the technique perpetuates behavioral cues that have not been diagnostically proven to indicate threat in past research.

Meissner and Kassin (2002) demonstrated that training and prior experience did not improve threat detection accuracy but appeared to increase the experts' willingness to classify an individual as threatening (i.e., threat bias). Bond (2008) also found that law enforcement participants exhibited a bias toward classifying an individual as threatening. Bond, Malloy, Arias, Nunn, and Thompson (2005) found that prisoners were biased toward classifying an individual as threatening and speculated that physical safety, self-protection, the need to always be on guard, and the fear of getting injured or dying were contributing factors for the observed threat bias. Like prisoners, experts in this domain face similar dangers and are well aware that the cost of mistaking a threat for a non-threat is too high (Bond et al., 2005). Unfortunately, the result is more threat judgments than non-threat judgments and is manifested as heightened suspicion or observers being more skeptical (Bond & DePaulo, 2006; Porter, Woodworth, & Birt, 2000). In contrast to the widespread finding of threat biases, the experts in Phase 2 of this project were more willing to classify scenarios as non-threatening (i.e., non-threat bias). This finding is similar to the findings of Zuckerman, Koestner, Colella, and Alton (1984) and is believed to be how most people judge their situation and that of others (O'Sullivan, 2003).

Furthermore, the author believes the non-threat bias observed in this study may be attributed to the nonverbal cues in the scenarios not being salient enough to raise the suspicion of the experts or again, the rejection of responsibility for consequences in light of low confidence in evidence. Notably, if current training practices and the potential for training to produce a threat response bias play a role in reducing detection accuracy rates, it is possible that we have broaden our understanding of one phenomenon that drives the shared mental models in this domain and can use this knowledge to modify current training practices to indirectly influence threat detection performance.

It is anticipated that the strategies obtained from the domain experts in Phase 1 and the heuristics designed in Phase 3 will become feasible solutions to strengthen the patterns needed for rapid decision making and will improve detection accuracy and correct myths currently endorsed in this domain regarding the use of nonverbal cues to detect a threat (Colwell et al., 2006). The heuristics in this project were developed to help training personnel in the domain of threat detection to design training programs that will aid the novice in building and strengthening mental associations between specific real-world situations and the expected nonverbal cues for those situations. In addition, the author provides guidance for how the heuristics can be incorporated into an existing or new training program. Recommendations are given regarding how to implement each heuristic into a training program and to assess the impact of implementing specific heuristics (Table 15). Assessment measures include human performance measures and training process measures. Also, recommendations for implementation and assessment were devised with the author mindful of the declining training budgets and resources for organizations in the threat detection domain (Griffith, 2008; Wolff, 2007), particularly local law enforcement departments and the military. Training developers in other arenas, (e.g.,

shoplifting, transportation, and general security) who may be fortunate to use iterative, instructional systems design (ISD) models such as the ADDIE (Analysis, Design, Development, Implementation, Evaluation) model to design training programs, can also use the recommendations in Table 15. For example, specific recommendations for heuristic implementation and assessment can be used for specific phases of the ADDIE model (Table 16). Recommendations for the implementation and assessment of Heuristic 4, 7, and 8 can be used during the design phase of the ADDIE model.

Table 15. Recommendations for the implementation and assessment of the heuristics.

Heuristic	Implementation	Assessment
1. Clearly define the situation.	Situation "Setup" - Verbally describe the situation in as much detail as possible (without divulging nonverbal cues or persons of interest) before showing the visual version of the situation. • Include the who, what, where, when Example of Situational Descriptors: • Who: Two known groups that frequent the area (give names); Ages of members in the group • What: An impending armed robbery during a concert • Where: Outdoor concert; name of concert performers; concert venue; number of people in attendance; demographic profile of fans; information regarding other events in the area • When: season; month; time of day	Questionnaire • Recruit "wizards" in the organization and instruct them to rate how well the narratives match the actual content of the scenario. • "Wizards" possess knowledge of many kinds of people in many kinds of situations (O'Sullivan, 2005). • Reassess as changes are made. • Assess for all new scenarios.
2. Visual versus written or oral scenarios are best for portraying non-verbal threat.	Create scenarios using one of the following: • Immersive environment with CAVE technology (McKenzie et al., 2003). • DI-Guy Scenario (http://www.diguy.com/diguy/scenario_home.htm) • Scenarios filmed with real actors.	Questionnaire • Recruit "wizards" in the organization and instruct them to rate how realistic and salient the nonverbal cues are in each scenario. • Reassess as changes are made. • Assess for all new scenarios.
3. Incorporate visual scenarios that contain no threat.	Create scenarios using one of the following: • Immersive environment with CAVE technology (McKenzie et al., 2003). • DI-Guy Scenario (http://www.diguy.com/diguy/scenario_home.htm) • Scenarios filmed with real actors.	Questionnaire • Recruit "wizards" in the organization and instruct them to rate the degree to which the scenario is absent of nonverbal cues or patterns of threat. • Reassess as changes are made. • Assess for all new scenarios.

Table 15 con't. Recommendations for the implementation and assessment of the heuristics.

Heuristic	Implementation	Assessment
4. Incorporate lecture-type teaching sessions to teach why and how specific non-verbal cues are associated with specific situations.	Design a 2-day training program • Classroom instruction on first day. • Multimedia instruction on second day; PC Simulation (Bhowmick et al., 2007; Wolff, 2007). <u>Classroom Instruction*</u> • Teach cues and cue descriptions. • Teach cues in context (why and how they are associative). • Show practice scenarios; participants decide if scenarios are threatening or non-threatening and list cues to support decision of threat or non-threat. • Corrective feedback (discussion about what is wrong with performance, why performance is wrong, and what needs to be modified to correct performance (Colwell et al., 2006; Klein et al., 2006). • Include time for questions from participants. * Based on ideas from Druckman & Bjork (1991) <u>Multimedia Instruction</u> • Material should be interactive and reinforce what was learned in the classroom. • Opportunity for individuals to review material at own pace and expand understanding of material. • Conclude with a video-based scenario test; measure responses for accuracy.	Human Performance Measures • Evaluate the percentage of participants achieving accuracy rates above 50%. • If budget permits, conduct an experimental test to evaluate performance for the 2-day instruction vs. multimedia instruction only. Use data to possibly recommend 2-day instruction every 5 years and multimedia instruction only in between. Multimedia Instruction Process Measures • Time accessing modules • Time spent on modules • Bhowmick et al., 2007 Questionnaire • User satisfaction with classroom and multimedia instruction.
5. Show visual representations or scenarios more than once.	• For classroom instruction, the instructor needs to strategically incorporate in the lesson. Possibly use as a tool for review. • Multimedia instruction: the learner should be permitted to review scenarios as many times as needed.	• Evaluate the optimal number of times scenarios can be shown to achieve some acceptable measure of accuracy.

Table 15 con't. Recommendations for the implementation and assessment of the heuristics.

Heuristic	Implementation	Assessment
6. Require new personnel to include reasons for decisions made…why that decision?	Implement during classroom instruction as a mechanism of giving feedback to the participants. See the specifics listed for Heuristic 4.	User satisfaction with method of feedback.
7. Refresh threat detection skills and knowledge for all personnel, especially new recruits, as often as permitted.	• Implement according to the organization's budget and resources. • Create a database that keeps a record of each individual's completed training (e.g., courses taken; completion dates). • Include next time frame for refresher training. • Make records accessible to personnel.	Review once a year.
8. Identify and keep cumulative training records for above-average performing personnel.	• Create a database that keeps a record (last 5 years) of each individual's objective performance measures for completed training. • Incorporate information from supervisor evaluations.	Review every 2 years to update roster.
9. Continuously improve the content of visual scenarios.	• Solicit actual past incidents from personnel. • For selected incidents, pursue with the individual to make sure all nonverbal cue and contextual details for the situation are included. • Create a visual scenario of the incident.	Questionnaire • Recruit "wizards" in the organization and instruct them to rate how realistic and salient the nonverbal cues are in each scenario. • Reassess as changes are made. • Assess for all new scenarios.

Table 16. Recommended heuristic implementation and assessment for specific phases of the ADDIE model.

ADDIE Model Phase	Heuristic Implementation and Assessment
Analysis	The heuristics developed in this project are not recommended for implementation in this phase of the ADDIE model. The content in this phase will depend on the training goals and objectives of the specific training area.
Design	Heuristic 4 (Include Lectures) Heuristic 7 (Refresh Skills) Heuristic 8 (Identify High Performers)
Development	Heuristic 1 (Define Situation) Heuristic 2 (Visual Content) Heuristic 3 (Portray Non-Threat) Heuristic 4 (Include Lectures) Heuristic 5 (Multiple Scenario Showings) Heuristic 6 (Reasons for Decision) Heuristic 9 (Improve Content)
Implementation	Heuristic 1 (Define Situation) Heuristic 4 (Include Lectures) Heuristic 5 (Multiple Scenario Showings) Heuristic 6 (Reasons for Decision)
Evaluation	Heuristic 4 (Include Lectures) Heuristic 7 (Refresh Skills) Heuristic 8 (Identify High Performers)

6.4 Revision of the RPD Model for ABTA

The global objective of this project was to elicit information from experts and evaluate expert performance in the threat detection domain to develop training heuristics for novices in the domain, especially infantry soldiers who are not afforded the opportunity to hone their skills over an extensive period of time. To achieve these objectives, the RPD model was selected as a framework for its potential in helping to identify gaps in the decision-making process of experts currently operating in the threat detection domain which is reported in the literature as chance detection accuracy rates (which is also reported as a finding in this project). The model theorizes that experts make decisions based on the recognition of situations as typical and familiar by recognizing the salient cues, causal dynamics, and expectancies within the situations (Klein, 1998; Klein et al., 1989) in environments characterized as complex, dynamic, time constrained, and cue learning (Lipshitz et al., 2001; Orasanu & Connolly, 1993).

In phase 2 of this project, experts were shown scenarios that were representative of such characteristics and made decisions regarding individuals' threat status. The experts achieved chance accuracy rates for distinguishing a threatening individual from a non-threatening individual and below chance accuracy rates for the identification of the cue-related information that was associated with the decisions. The RPD model posits that effective decisions are made by mapping what is seen in the environment to recognizable and prototypical mental schemas held in long-term memory and the author speculates that the poor accuracy rates achieved by the experts in phase 2 are a result of a lack of cue and context association held in existing schemas. The wizards' superior performance in phase 2 is assumed to be a result of the number and complexity of nonverbal cues they named. It is assumed that the cues were held in long-term

memory and were retrieved as recognizable patterns when they were seen in the scenarios. In contrast, those experts who obtained average performance levels did not have as many recognizable patterns to retrieve from long-term memory to match with the information in the scenarios and obtained lower performance profiles than the wizards. These findings validate the theory of pattern matching in the RPD model. The strategies found in phase 1 have the potential to improve expert accuracy rates for detecting a threat by expanding the cue and context foundation needed for matching behavior patterns seen in the environment with behavior patterns held in schemas. In addition, the strategies are one form of support that will hopefully aid in the quick development of expertise in the threat detection domain so that novices in the domain can go into the field and successfully apply what they have learned to the challenges they will face (Salas & Klein, 2001).

Because it is imperative that infantry soldiers quickly master and use threat detection skills successfully in urban environments, the RPD model has been updated to reflect the expert strategies that are deemed important for effective decision making in the detection of a threat (Figure 23). According to the original model, observers in the threat detection domain should be capable of making effective decisions in the field by using current situation cues to visually perceive the situation, mapping the cues to recognizable and typical mental schemas, and automatically selecting the appropriate course of action based on prior experience and current situation information. The revised model focuses on developing and expanding the repertoire of behavioral patterns stored in schema so that the patterns are effortlessly accessed by observers to match with patterns encountered in the environment, converting unfamiliar situations into typically recognizable situations. Specifically, the goal of expanding the repertoire of behaviors in schema is to convert the anomaly of a crowd environment into a typical situation which would

be evident by less decision making errors and higher accuracy rates (≥ 70%) (Atkins & Norris, 2004).

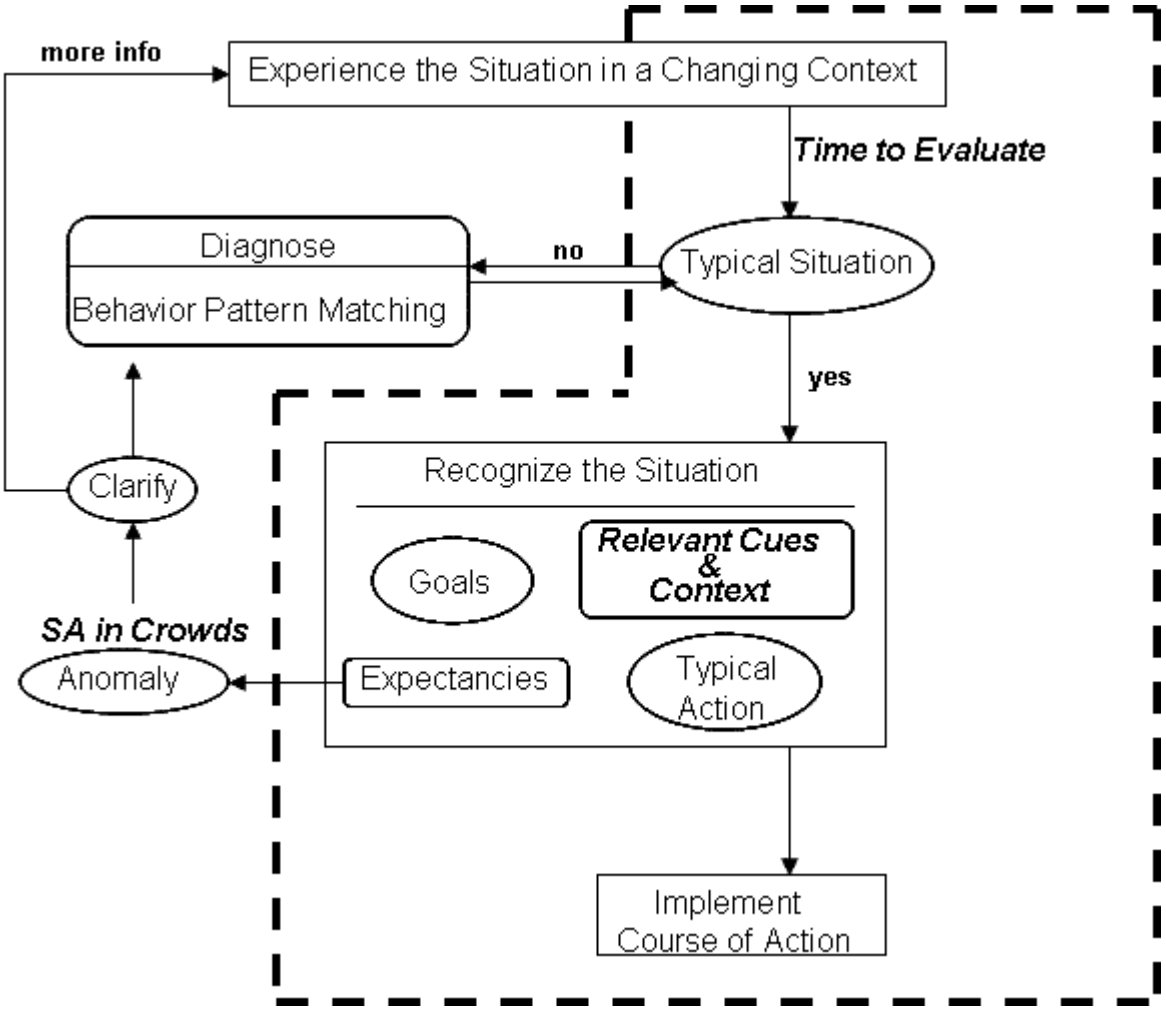


Figure 23. RPD model revised for ABTA. RPD model revised to reflect effective decision making regarding a threat in urban environments.

According to the revised model, observers in the threat detection domain should be capable of making effective decisions in the field by using current situation cues to visually

perceive the situation while realistically knowing how much time is required[3] to analyze the situation cues (Time to Evaluate). The ideal amount of time to evaluate the situation will enable the observer to analyze the situation cues and the appropriate context (i.e., who, what, where, when) associated with the situation cues (Cues & Context). This information leads the observer to identify the situation as a typical occurrence based on prior experience and training (behavior/context pattern matching between situation and schema) and leads the observer to automatically choose the correct course of action. This decision process culminates with accurate and successful classification and is highlighted in the bold, dotted box in Figure 23. However, violations in situation expectation will lower SA and the observer will require more information about the situation to make a decision (SA in Crowds). When the search for more information is unsuccessful because the behavior/context patterns are not available in schema, the result will be low accuracy rates for the classification of threat status. The Practice and Learn strategies are not shown in Figure 23 but they affect how well an observer is able to diagnose a threatening situation and will be evident by the observer's decision accuracy rates. The Practice strategy will help observers to reinforce former knowledge, integrate newly acquired knowledge, and modify/update these knowledge connections for storage in schema. The Learn strategy will provide observers the opportunity to learn complex domain concepts from successful individuals in the domain and receive feedback in order to change, correct, and reorganize situational and cue-related information to correct errors.

[3] The time required to analyze a situation still needs to be determined. This research effort only reports that 1 minute is insufficient to analyze a situation.

6.5 Application Areas

Expert strategies regarding how to use nonverbal cues to detect a threat and "Heuristics for Novice Training Development in the Threat Detection Domain" are useful tools for Army officials in developing improved enemy identification training for the soldier in MOUT. However, the importance of and need for these tools are just as evident outside the military environment. This is especially true for airport security screening. Miami International Airport currently uses an Aggressive Behavioral Screening Program (borrowed from the Israelis) to look for potential terrorists among thousands of people passing through the airport (Sanders, 2006). The program is designed to spot probable terrorists by looking at how they act via behavioral cues and body language that are not normal. Airport officials have also trained janitors and restaurant workers to help spot terrorists and report a 25% reduction in crime since fielding the program. The program is also being used in Minneapolis, Boston, and San Francisco airports. The behavior detection programs that are in use at a number of airports are part of the larger Screening of Passengers by Observation Technique (SPOT) program under the Transportation Security Administration (TSA) (Phillips, 2007). The purpose of the SPOT program is to train "officers to scan airport crowds, looking for body language that could signal malevolent intent" (p. 17) (Phillips, 2007). The use of contextually based cues and the intuitive mode of thought may help to reduce the rate of false alarms that officials may be encountering. Implementation of the "Heuristics for Novice Training Development in the Threat Detection Domain" may help to improve threat detection rates for civilian employees (e.g., janitors, restaurant workers) required to use the Aggressive Behavioral Screening Program.

From a perspective of personal security, the U.S. Department of State (2008) warns citizens to be aware of "the continuing threat of terrorist actions and violence against

Americans". With the world, particularly the United States, on high alert for acts of terrorism, the information found in this project will also be beneficial for civilians. Law enforcement cannot be everywhere and citizens are now asked to be vigilantly aware for suspicious individuals. For example, a message from the Maryland State Police (2007) contained in a brochure informs citizens that they play a vital role in helping to keep the state safe. A 1-800 number is provided and encourages people to call and provide information about suspicious persons or circumstances related to terrorism. However, if civilians are to be of any help in this area, they will need training in threat detection just as new law enforcement officers receive. The "Heuristics for Novice Training Development in the Threat Detection Domain" can be used to design an appropriate threat detection training module for the average civilian, and the module can become a standard for training the average civilian in threat detection techniques.

Finally, automated threat detection systems are on the horizon for helping to detect threatening individuals and situations. The systems are designed to augment the human's ability to detect nonverbal cues to threat. Johns Hopkins University security specialists, monitoring scenes from 89 campus cameras, are alerted to real-time suspicious behavior with the help of behavior recognition software (Roylance, 2007). The software is developed by Cernium Corporation, an electronic security firm in Reston, Virginia. The software, used by the Department of Homeland Security, the Pentagon, and professors at the University of Maryland, essentially analyzes patterns of behaviors by comparing the behaviors to a criterion of 18 suspicious behaviors. If a pattern of behavior is found to match the suspicious behaviors, an alert is sent to the observer. ObjectVideo, another company in Reston, also designs software solutions capable of object detection and tracking. Meservy et al. (2005) are also working on a threat detection system for potential homeland security applications and hope the technology can make

the human more effective at detecting threats. Specifically linking most cues with probable expected situations could help to enlarge the pattern criterion for these software packages and systems.

6.6 Future Research

The situations that researchers currently study in the literature where the detection of individuals with covert mischievous intentions are of interest are not valid for the infantry soldier in MOUT, the average citizen on alert for suspicious behavior, or the security of our national infrastructure. In current studies that evaluate the detection of individuals with covert mischievous intentions, the offender is already known. Circumstances such as the three specific circumstances mentioned are the focus of this research in which the identification of the threatening offender is the responsibility of the observer before consequences of a hostile act are realized. The identification of nonverbal cues that indicate a threat in these circumstances does not permit communication with or require cooperation from an offender. Concealed, threatening intentions aimed at our national infrastructure are not verbal and will rarely be evaluated in face-to-face communications or interviews. Threatening intentions in these circumstances will occur in everyday, social situations when the observer least expects. More studies are needed to address the factors that assist in the successful identification of threats in social situations such as crowds and social events. In addition, in a 19-study meta-analysis conducted by Bond and DePaulo (2006), no evidence was found to support the idea that experts are superior to non-experts in threat detection. Perhaps future studies aimed at extracting tacit knowledge from "wizards" (O'Sullivan, 2005) regarding threat detection in the domain and finding the link between the intuitive mode of thought and the accuracy of detecting imminent threat will help to

reverse this finding which is prevalent throughout the literature. However, to build an understanding of the latter, studies that develop methods for the measurement of intuition are also recommended. More field studies are also suggested since chance accuracy rates may be attributable to the limitation of evaluating threatening behaviors in the laboratory (Vrij, 2004). Therefore, it is imperative that methods for the assessment of threat detection performance involve more realistic settings (Atkins & Norris, 2004; Mann, Vrij, & Bull, 2004). With the exception of video-based scenarios, but perhaps more so, field studies can provide the realistic consequences associated with incorrect judgments regarding an individual's threat status.

REFERENCES

Abelson, R.P. (1981). Psychological status of the script concept. *American Psychologist*, 36(7), 715-729.

Al-Simadi, F.A. (2000). Jordanian students' beliefs about nonverbal behaviors associated with deception in Jordan. *Social Behavior and Personality*, 28(5), 437-441.

Alter, A.L., Oppenheimer, D.M., Epley, N., & Eyre, R.N. (2007). Overcoming intuition: Metacognitive difficulty activates analytic reasoning. *Journal of Experimental Psychology: General*, 136(4), 569-576.

Atkins, V.J., & Norris, W.A. (2004). Survival Scores Research Project. FLETC Research Paper. Federal Law Enforcement Training Center. U.S. Department of Homeland Security. Glynco, GA, April. http://www.fletc.gov/reference/research-papers/survival_scores_research.pdf/view

Baldwin, D.A., & Baird, J.A. (2001). Discerning intentions in dynamic human action. *TRENDS in Cognitive Sciences*, 5(4), 171-178.

Bar, M., Neta, M., & Linz, H. (2006). Very first impressions. *Emotion*, 6(2), 269-278.

Bhowmick, A., Khasawneh, M.T., Bowling, S.R., Gramopadhye, A.K., & Melloy, B.J. (2007). Evaluation of alternate multimedia for web-based asynchronous learning. *International Journal of Industrial Ergonomics*, 37, 615-629.

Biederman, I., Mezzanotte, R.J., & Rabinowitz, J.C. (1982). Scene perception: Detecting and judging objects undergoing relational violations. *Cognitive Psychology*, 14, 143-177.

Bond, G.D. (2008). Deception detection expertise. *Law and Human Behavior*, 32, 339-351.

Bond, C.F. Jr., & DePaulo, B.M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, 10(3), 214-234.

Bond, G.D., Malloy, D.M., Arias, E.A., Nunn, S.N., & Thompson, L.A. (2005). Lie-biased decision making in prison. *Communication Reports*, 18(1), 9-19.

Bos, R., van Gurp, J., Verpoorten, J.H., & Brinkkemper, S. (2005). Heuristic Evaluation of Content Management Systems: CMS Specific Heuristics. In P. Isaias and M.B. Nunes (Eds.) Proceedings of the IADIS International Conference WWW/Internet, Volume II, pp. 247-254.

Brister, D.S. (1997). *Exposing the Enemy*. Harvey, LA: Second Printing.

Brockmole, J.R., Hambrick, D.Z., Windisch, D.J., & Henderson, J.M. (2008, January 16). The role of meaning in contextual cueing: Evidence from chess expertise. *Quarterly Journal of Experimental Psychology*, *iFirst*, 1-11. DOI: 10.1080/17470210701781155

Brockmole, J.R., & Henderson, J.M (2008). Prioritizing new objects for eye fixation in real-world scenes: Effects of object-scene consistency. *Visual Cognition*, 16, 375-390.

Brown, Capt. K. W. (1997). The urban warfare dilemma – U.S. casualties vs. collateral damage. *Marine Corps Gazette*, 81(1), 38-40.

Cathcart, J.M., Doll, T.J., & Schmieder, D.E. (1989). Target detection in urban clutter. *IEEE Transactions on Systems, Man, and Cybernetics*, 19(5), 1242-1250.

Cathcart, J.M., Doll, T.J., & Schmieder, D.E. (1988). Observer detection performance in urban clutter. Air Force Wright Aeronautical Laboratories, Avionics Laboratory. (DTIC report AD-B122 931, LIMITED).

Chen, C. (2003). A constructivist approach to teaching: Implications in teaching computer networking. *Information Technology, Learning, and Performance*, 21(2), 17-27.

Cockburn, P. (2005, April 24). Terrified US soldiers are still killing civilians with impunity. *The Independent on Sunday*. http://findarticles.com/p/articles/mi_qn4159/is_20050420/ai_n14598652

Colwell, L.H., Miller, H.A., Lyons, P.M. Jr., and Miller, R.S. (2006). The training of law enforcement officers in detecting deception: A survey of current practices and suggestions for improving accuracy. *Police Quarterly*, 9(3), 275-290.

Congressional Statement (2002). The terrorist threat confronting the United States. Washington, D.C.: Federal Bureau of Investigation, 6 February. http://www.fbi.gov/congress/congress02/watson020602.htm

Cuddy, M.M., Dillon, G.F., Clauser, B.E., Holtzman, K.Z., Margolis, M.J., Mcellhenney, S.M., & Swanson, D.B. (2004). Assessing the validity of the USMLE Step 2 clinical knowledge examination through an evaluation of its clinical relevance. *Academic Medicine*, 79(10), S43-S45.

Davis, A., Pereira, J., & Bulkeley, W.M. (2002, August 15). Security concerns bring new focus on body language. *The Wall Street Journal*, pp. A1, A6.

Davis, A., Pereira, J., & Bulkeley, W.M. (2002, October). The telltale twitch: Law-Enforcement officials zero in on body language to sniff out terrorists. *The Wall Street Journal, Classroom Edition.* http://www.wsjclassroomedition.com/archive/02oct/POLI.htm

de Becker, G. (1997). *The Gift of Fear*. New York, NY: Dell Publishing.

Department of the Army (2008). FM 3-0. Operations. Washington, D.C.: 27 February.

Department of the Army (2006). FM 3-06. Urban Operations. Washington, D.C.: 26 October.

Department of the Army (2002). FM 3-06.11. Combined Arms Operations in Urban Terrain. Washington, D.C.: 28 February.

Department of the Navy (1998). MCWP 3-35.3. Military Operations on Urbanized Terrain (MOUT). Washington, D.C.: 26 April.

DePaulo, B.M., Lindsay, J.J., Malone, B.E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin*, 129(1), 74-118.

DePaulo, B.M., & Pfeifer, R.L. (1986). On-the-job experience and skill at detecting deception. *Journal of Applied Social Psychology*, 16(3), 249-267.

DePaulo, B.M., Rosenthal, R., Rosenkrantz, J., & Green, C.R. (1982). Actual and perceived cues to deception: A closer look at speech. *Basic and Applied Social Psychology*, 3(4), 291-312.

Desch, M.C. (2001). Why MOUT now? In M. C. Desch (Ed.) Soldiers in Cities: Military Operations on Urban Terrain. Strategic Studies Institute, U.S. Army War College, pp. 1-15. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB294.pdf

deTurck, M.A., & Miller, G.R. (1990). Training observers to detect deception: Effects of self-monitoring and rehearsal. *Human Communication Research*, 16(4), 603-620.

Doll, T.J., Schmieder, D.E., & McWhorter, S.W. (1992). Simulation of human visual search and detection. In *Proceedings of the 3rd Annual Ground Target Modeling and Validation Conference*, 247-255, Ann Arbor, MI. (DTIC report AD-B171 616, LIMITED).

Druckman, D., & Bjork, R.A. (Eds.). (1991). *In the Mind's Eye: Enhancing Human Performance*. Washington, D.C.: National Academy Press.

Dupont, D.G. (1998). Inner-city violence. *Scientific American*, 279(4), 39-40.

Edwards, S.J.A. (2000). *Mars Unmasked: The Changing Face of Urban Operations*. MR-1173-A. Santa Monica, CA: RAND.

Ekman, P. (2001). *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. New York, NY: W.W. Norton.

Ekman, P. (1999). Basic emotions. In T. Dalgleish and M. Power (Eds.). *Handbook of Cognition and Emotion*. Sussex, U.K.: John Wiley & Sons.

Ekman, P. (1997). Lying and deception. In N.L. Stein, P.A. Ornstein, B. Tversky, and C. Brainerd (Eds.). *Memory for Everyday and Emotional Events*. Mahwah, NJ: Lawrence Erlbaum Associates.

Ekman, P. (1996). Why don't we catch liars? *Social Research*, 63(3), 801-817.

Ekman, P. (1988). Lying and nonverbal behavior: Theoretical issues and new findings. *Journal of Nonverbal Behavior*, 12(3), 163-176.

Ekman, P., & Friesen, W.V. (1976). Measuring facial movement. *Environmental Psychology and Nonverbal Behavior*, 1(1), 56-75.

Ekman, P., & Friesen, W.V. (1974). Detecting deception from body or face. *Journal of Personality and Social Psychology*, 29, 288-298.

Ekman, P., & Friesen, W.V. (1969a). The repertoire of nonverbal behavior: Categories, origins, usage, and coding. *Semiotica*, 1, 49-98.

Ekman, P., & Friesen, W.V. (1969b). Nonverbal leakage and clues to deception. *Psychiatry*, 32, 88-105.

Ekman, P., Friesen, W.V., & Ellsworth, P. (1972). *Emotion in the human face: Guidelines for research and an integration of findings*. New York: Pergamon Press.

Ekman, P., Friesen, W.V., & O'Sullivan, M. (1988). Smiles when lying. *Journal of Personality and Social Psychology*, 54, 414-420.

Ekman, P., & O'Sullivan, M. (1991). Who can catch a liar? *American Psychologist*, 46(9), 913-920.

Ekman, P., O'Sullivan, M., Friesen, W.V., & Scherer, K.R. (1991). Face, voice and body in detecting deceit. *Journal of Nonverbal Behavior*, 15(2), 125-135.

Endsley, M.R. (2000a). Theoretical underpinnings of situation awareness: A critical review. In Endsley, M.R. and Garland, D.J. (Eds.). *Situation Awareness Analysis and Measurement*. Mahwah, NJ: Lawrence Erlbaum Associates.

Endsley, M.R. (2000b). Situation models: An avenue to the modeling of mental models. In Proceedings of the 14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society.

Endsley, M.R. (1995). Towards a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32-64.

Endsley, M.R. (1988). Design and evaluation for situation awareness enhancement. In Proceedings of the Human Factors Society 32nd Annual Meeting, 97-101.

Ericsson, K.A., & Simon, H.A. (1980). Verbal reports as data. Psychological Review, 87(3), 215-251.

Feldman, R.S., & Chesley, R.B. (1984). Who is lying, who is not: An attrrbutional analysis of the effects of nonverbal behavior on judgments of defendant believability. *Behavioral Sciences & The Law*, 2(4), 451-461.

Fiore, S.M., Cuevas, H.M., & Oser, R.L. (2003). A picture is worth a thousand connections: the facilitative effects of diagrams on mental model development and task performance. *Computers in Human Behavior*, 19, 185-199.

Gerwehr, S., & Glenn, R.W. (2000). *The Art of Darkness: Deception and Urban Operations.* MR-1132-A. Santa Monica, CA: RAND.

Gigerenzer, G. (2007). *Gut Feelings: The Intelligence of the Unconscious*. New York: Penguin Group.

Glenn, R.W. (1999). *We Band of Brothers: The Call for Joint Urban Operations Doctrine.* Santa Monica, CA: RAND.

Gobet, F., & Chassy, P. (2008). Towards an alternative to Benner's theory of expert intuition in nursing: A discussion paper. *International Journal of Nursing Studies*, 45(1), 129-139.

Granhag, P.A., & Stromwall, L.A. (2002). Repeated interrogations: Verbal and non-verbal cues to deception. *Applied Cognitive Psychology*, 16, 243-257.

Grau, L.W., & Kipp, J.W. (1999). Urban combat: Confronting the specter. *Military Review*, 79(4), 9-17.

Griffith, D. (2008). State of American Law Enforcement: Teaching to the Test. Police Magazine. http://www.policemag.com/Articles/2008/03/State-of-American-Law-Enforcement-Teaching-to-the-Test.aspx

Groves, J.R (1998). Operations in urban environments. *Military Review*, 78(4), 31-40.

Hahn II, R.F., & Jezior, B. (1999). Urban warfare and the urban warfighter of 2025. *Parameters*, Summer, 74-86.

Hancock, P.A. (2002). Quo vadis homeland security. *In Proceedings of the Human Factors and Ergonomics Society, 46th Annual Meeting.* Baltimore, MD: Human Factors and Ergonomics Society.

Hedlund, J., Antonakis, J., & Sternberg, R.J. (2002). Tacit Knowledge and Practical Intelligence: Understanding the Lessons of Experience. ARI Research Note 2003-04. Army Research Institute for the Behavioral and Social Sciences: Alexandria, VA, October.

Hodgkinson, G.P., Langan-Fox, J., & Sadler-Smith, E. (2008). Intuition: A fundamental bridging construct in the behavioural sciences. *British Journal of Psychology*, 99(1), 1-27.

Hogarth, R.M. (2001). *Educating Intuition*. Chicago: University of Chicago Press.

Johnson, J.J. (2002, October 15). DC Sniper: Real Americans weigh in (attention Washington area residents). *Sierra Times*. http://www.sierratimes.com/02/10/15/arjj101502.htm

Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9), 697-720.

Karadsheh, J., & Damon, A. (2007, April 24). U.S. military: Suicide bombers kill 9 U.S. soldiers in Iraq. *CNN.com*. http://www.cnn.com/2007/WORLD/meast/04/23/iraq.main/index.html

Kassin, S.M., & Fong, C.T. (1999). "I'm innocent!": Effects of training on judgments of truth and deception in the interrogation room. *Law and Human Behavior*, 23, 499-516.

Klein, G. (2008). Naturalistic decision making. *Human Factors*, 50(3), 456-460.

Klein, G. (1998). Sources of Power: How People Make Decisions. Cambridge: MIT Press.

Klein, G. (1993). Sources of error in naturalistic decision making tasks. In Proceedings of the Human Factors and Ergonomics Society 37th Annual Meeting, 368-371.

Klein, G.A., Calderwood, R., & Cirocco, A.C. (1986). Rapid decision making on the fire ground. In Proceedings of the Human Factors Society 30th Annual Meeting, 576-580. Dayton, OH: Human Factors Society.

Klein, G.A., Calderwood, R., & Macgregor, D. (1989). Critical decision method for eliciting knowledge. *IEEE Transactions on Systems, Man, and Cybernetics*, 19(3), 462-472.

Klein, G., Moon, B., & Hoffman, R.R. (2006). Making sense of sensemaking 2: A macrocognitive model. *Intelligent Systems*, 21(5), 88-92.

Koopman, B.O. (1980). *Search and Screening: General Principles with Historical Application*s. New York: Pergamon Press.

Krauss, R.M., Chen, Y.S., & Chawla, P. (1996). Nonverbal behavior and nonverbal communication: What do conversational hand gestures tell us? *Advances in Experimental Social Psychology*, 28, 389-450.

Lakhani, M., & Taylor, R. (2003). Beliefs about cues to deception in high- and low-stake situations. *Psychology, Crime & Law*, 9(4), 357-368.

Lehto, M.R. (1997). Decision making. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics* (2nd ed.). New York: John Wiley.

Levine, T.R., Park, H.S., & McCornack, S.A. (1999). Accuracy in detecting truths and lies: Documenting the "veracity effect". *Communication Monographs*, 66(2), 125-144.

Lievens, F., & Sackett, P.R. (2006). Video-based versus written situational judgment tests: A comparison in terms of predictive validity. *Journal of Applied Psychology*, 91(5), 1181-1188.

Lipshitz, R., Klein, G., Orasanu, J., & Salas, E. (2001). Taking stock of naturalistic decision making. *Journal of Behavioral Decision Making*, 14(5), 331-352.

Mabry, R.L., Holcomb, J.B., Baker, A.M., Cloonan, C.C., Uhorchak, J.M., Perkins, D.E., Canfield, A.J., & Hagmann, J.H. (2000). United States Army Rangers in Somalia: An analysis of combat casualties on an urban battlefield. *The Journal of TRAUMA Injury, Infection, and Critical Care*, 49(3), 515-529.

Maier, N.R.F., & Thurber, J.A. (1968). Accuracy of judgments of deception when an interview is watched, heard, and read. *Personnel Psychology*, 21, 23-30.

Malhotra, V., Lee, M.D., & Khurana, A. (2007). Domain experts influence decision quality: Towards a robust method for their identification. *Journal of Petroleum Science and Engineering*, 57(1-2), 181-194.

Mann, S., Vrij, A., & Bull, R. (2004). Detecting true lies: Police officer's ability to detect suspect's lies. *Journal of Applied Psychology*, 89, 137-149.

Martin, C. (2002, December 23). Nonverbal communications: Escape the pitfalls. MSN.com http://interview.monster.com/review/actions

Maryland State Police (2007). *An Important Message For You: Fairness, Integrity, & Service.* [Brochure]. MSP 225 (6-07). http://www.mdsp.org/downloads/225.pdf

Matloff, M. (1989). Introduction. *In American Military History: Army Historical Series*. Washington, D.C.: Center of Military History, US Army.

McKenzie, F.R., Scerbo, M., Catanzaro, J., & Phillips, M. (2003). Nonverbal indicators of malicious intent: affective components for interrogative virtual reality training. *International Journal of Human-Computer Studies*, 59, 237-244.

Medin, D.L., & Schaffer, M.M. (1978). Context theory of classification learning. *Psychological Review*, 85(3), 207-238.

Meissner, C.A., & Kassin, S.M. (2002). "He's guilty!": Investigator bias in judgments of truth and deception. *Law and Human Behavior*, 26(5), 469-480.

Meitzler, T., Jackson, W., Bednarz, D., & Collins, P. (1992). A semi-empirical study of the correlation of background clutter with several parameters. In *Proceedings of the 3rd Annual Ground Target Modeling and Validation Conference*, 370-375, Ann Arbor, MI. (DTIC report AD-B171 616, LIMITED).

Meservy, T.O., Jensen, M.L., Kruse, J., Burgoon, J.K., Nunamaker, J. F. Jr., Twitchell, D.P., Tsechpenakis, G., & Metaxas, D.N. (2005). Deception detection through automatic, unobtrusive analysis of nonverbal behavior. *IEEE Intelligent Systems*, 20(5), 36-43.

Murray, F.J. (2002, August 17). NASA plans to read terrorist's minds at airports. *The Washington Times*. http://www.maebrussell.com/Articles%20and%20Notes/NASA%20to%20read%20minds%20at%20airports.html

Myers, D.G. (2002). *Intuition: Its Powers and Perils*. New Haven, CT: Yale University Press.

Nemko, M. (2003, January 31). Become a human lie detector. *MSN.com* http://content.msn.monster.com/articles/lying

Neufeldt, V., & Guralnik, D.B. (Eds.). (1988). *Webster's New World Dictionary* (3rd College ed.). New York: Webster's New World.

Nielsen, J. (1994). Enhancing the explanatory power of usability heuristics. Proceedings of ACM CHI'94, pp. 152-158.

O'Connor, J.D., O'Kane, B.L., Royal, C.K., Ayscue, K.L., Bonzo, D.E., & Nystrom, B.M. (1996). Recognition of human activities using handheld thermal systems. Night Vision and Electronic Sensors Directorate, Fort Belvoir, VA.

O'Hanlon, M.E., & Campbell, J.H. (2007). Iraq Index: Tracking Variables of Reconstruction & Security in Post-Saddam Iraq. Washington, D.C.: The Brookings Institution. http://www.brookings.edu/iraqindex

O'Neil, J. (2002, October 23). Some tips for would-be tipsters. *CNN.com* http://www.cnn.com/2002/US/South/10/12/tips.glance.ap/index.html

O'Sullivan, M. (2005). Emotional intelligence and deception detection: Why most people can't "read" others, but a few can. In R.E. Riggio and R.S. Feldman (Eds.). *Applications of Nonverbal Communication*. Mahwah, NJ: Lawrence Erlbaum Associates.

O'Sullivan, M. (2003). The fundamental attribution error in detecting deception: The boy-who-cried-wolf effect. *Personality and Social Psychology Bulletin*, 29, 1316-1327.

Oglesby, C. (2002, October 9). This is like a war zone: Recurring terror in D.C. *CNN.com* http://www.cnn.com/2002/US/South/10/08/shootings.coping

Orasanu, J., & Connolly, T. (1993). The reinvention of decision making. In G.A. Klein, J. Orasanu, R. Calderwood, & C.E. Zsambok (Eds.). *Decision Making in Action: Models and Methods*, Norwood, CT: Ablex.

Partlow, J. (2008, March 11). Five soldiers die in attack on U.S. patrol in Baghdad. *The Washington Post.* http://www.washingtonpost.com/wpdyn/content/article/2008/03/10/AR2008031000683.html

Peters, R. (2000). The human terrain of urban operations. *Parameters*, Spring, 4-12.

Phillips, Z. (2007). Criminal cues. *Government Executive*, 39(6), 17-18.

Physicians for Human Rights (1991). Operation "Just Cause": The Human Cost of Military Action in Panama. Boston, MA: October. http://physiciansforhumanrights.org/library/documents/reports/operation-just-cause.pdf

Porter, S., Woodworth, M., & Birt, A.R. (2000). Truth, lies, and videotape: An investigation of the ability of federal parole officers to detect deception. *Law and Human Behavior*, 24(6), 643-658.

Pretz, J.E., & Totz, K.S. (2007). Measuring individual differences in affective, heuristic, and holistic intuition. *Personality and Individual Differences*, 43, 1247-1257.

Price, B. (1998). The importance for preservice teachers to have practice experiences to apply theory to reality. *Electronic Journal of Science Education*, 2(3). http://ejse.southwestern.edu/

Reardon, R., Lenz, J., & Folsom, B. (1998). Employer ratings of student participation in non-classroom based activities: Findings from a campus survey. *Journal of Career Planning & Employment*, 58(4), 36-39.

Ross, K.G., Klein, G.A., Thunholm, P., Schmitt, J.F., & Baxter, H.C. (2004). The recognition-primed decision model. *Military Review*, 84(4), 6-10.

Rossing, C., Hansen, E.H., Krass, I., & Traulsen, J.M. (2003). Pharmaceutical care in Denmark: perceived importance of medicine-related problems and participation in postgraduate training. *Pharmacy World and Science*, 25(2), 73-78.

Roylance, F.D. (2007, January 5). Recognizing odd behavior. *The Baltimore Sun*, pp. 1D, 5D.

Rozelle, R.M., & Baxter, J.C. (1975). Impression formation and danger recognition in experienced police officers. *The Journal of Social Psychology*, 96, 53-63.

Russell, R.A., Russell, J.R., & Benke, K.K. (1996). Subjective Factors in Combat Simulation: Correlation between Fear and the Perception of Threat. DSTO-TR-0410. Aeronautical and Maritime Research Laboratory: September.

Salas, E., & Klein, G. (2001). Expertise and naturalistic decision making: An overview. In E. Salas & G. Klein (Eds.), *Linking Expertise and Naturalistic Decision Making*. Mahwah, NJ: Lawrence Erlbaum.

Sanders, K. (2006, June 1). Aggressive Behavioral Screening Program (A Video Report). The Today Show. http://video.msn.com/v/us/v.htm?g=ff7a5f22-dbdf-4336-b4a1-59e2c7508547&f=06/64&fg=email

Schank, R.C., & Abelson, R.P. (1977). *Scripts, Plans, Goals, and Understanding: An Inquiry into Human Knowledge Structures*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Schweitzer, M.E., Brodt, S.E., & Croson, R.T.A. (2002). Seeing and believing: Visual access and the strategic use of deception. *The International Journal of Conflict Management*, 13(3), 258-275.

Secord, P.F., Backman, C.W., & Slavitt, D.R. (1976). *Understanding Social Life: An Introduction to Social Psychology*. New York, NY: McGraw-Hill.

Shanteau, J. (1992). How much information does an expert use? Is it relevant? *Acta Psychologica*, 81, 75-86.

Shoemaker, D.J., & South, D.R. (1978). Nonverbal images of criminality and deviance: Existence and consequence. *Criminal Justice Review*, 3, 65-80.

Shoemaker, D.J., South, D.R., & Lowe, J. (1973). Facial stereotypes of deviants and judgments of guilt or innocence. *Social Forces*, 51, 427-433.

Simmons, J.P., & Nelson, L.D. (2006). Intuitive confidence: Choosing between intuitive and nonintuitive alternatives. *Journal of Experimental Psychology: General*, 135(3), 409-428.

Spencer-Rodgers, J., Hamilton, D.L., & Sherman, S.J. (2007). The central role of entitativity in stereotypes of social categories and task groups. *Journal of Personality and Social Psychology*, 92(3), 369-388.

Sternberg, R.J. (1999). Cognitive Psychology (2nd ed). Fort Worth, TX: Harcourt Brace College Publishers.

Stromwall, L.A., & Granhag, P.A. (2003). Affecting the perception of verbal cues to deception. *Applied Cognitive Psychology*, 17, 35-49.

Sullivan, D.C., & Siegel, L.J. (1972). How police use information to make decisions: An application of decision games. *Crime and Delinquency*, 18, 254-262.

Ten Dam, G., & Volman, M. (2004). Critical thinking as a citizenship competence: teaching strategies. *Learning and Instruction*, 14, 359-379.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, 211(4481), 453-458.

United Nations (2001). *World Urbanization Prospects: the 2001 Revision*, Population Division, New York, 2002.

United Nations (1999). *World Urbanization Prospects: the 1999 Revision*, Population Division, New York, 2000.

United Nations (1994). *World Urbanization Prospects: the 1994 Revision*, Population Division, New York, 1995.

University of Leeds (2008, March 6). Go With Your Gut – Intuition Is More Than Just A Hunch, Says New Research. ScienceDaily. http://www.sciencedaily.com/releases/2008/03/080305144210.htm

U.S. Department of State (2008). Worldwide Caution. 17 January. http://travel.state.gov/travel/cis_pa_tw/pa/pa_1161.html?css

U.S. Department of State (1998). Patterns of Global Terrorism. http://www.state.gov/www/global/terrorism/1998Report/1998index.html

Vaughan, B.D. (2006). Soldier-in-the-Loop Target Acquisition Performance Prediction Through 2001: Integration of Perceptual and Cognitive Models. ARL-TR-3833. Army Research Laboratory: Aberdeen Proving Ground, MD, July.

Vrij, A. (2004). Invited article: Why professionals fail to catch liars and how they can improve. *Legal and Criminological Psychology*, 9, 159-182.

Vrij, A. (1994). The impact of information and setting on detection of deception by police detectives. *Journal of Nonverbal Behavior*, 18(2), 117-136.

Vrij, A., Edward, K., Roberts, K.P., & Bull, R. (2000). Detecting deceit via analysis of verbal and nonverbal behavior. *Journal of Nonverbal Behavior*, 24(4), 239-263.

Vrij, A., & Mann, S. (2004). Detecting deception: The benefit of looking at a combination of behavioral, auditory and speech content related cues in a systematic manner. *Group Decision and Negotiation*, 13, 61-79.

Vrij, A., Semin, G.R., & Bull, R. (1996). Insight into behavior displayed during deception. *Human Communication Research*, 22(4), 544-562.

Walker, J.F. (2002). Situational awareness: How to stay alive…anywhere! *Armor*, 111(2), 34-35.

Weick, K.E., Sutcliffe, K.M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, 16(4), 409-421.

Weiss, R.S. (1994). *Learning From Strangers: The Art and Method of Qualitative Interview Studies.* New York, NY: The Free Press.

White, L. (2002). Suspicious? What's that? *CNN.com.* http://www.cnn.com/2002/US/07/03/terror.mos.story

White, C.H., & Burgoon, J.K. (2001). Adaptation and communicative design: Patterns of interaction in truthful and deceptive conversations. *Human Communication Research*, 27(1), 9-37.

Wiener, M., Devoe, S., Rubinow, S., & Geller, J. (1972). Nonverbal behavior and non-verbal communication. *Psychological Review*, 79(3), 185-214.

Wolff, R.S. (2007). Computer-based simulation: The road ahead. FLETC Journal, 5(1), 24-34. http://www.fletc.gov/reference/reports/fletc-journals/FLETC_Journal_Spring2007.pdf/view

World Resources Institute (1998-99). Population and human well-being: Urban growth. Retrieved October 8, 2002. http://www.wri.org/wr-98-99/citygrow.htm

World Resources Institute (1996-97). A Guide to the Global Environment: The Urban Environment. Retrieved October 8, 2002. http://www.wri.org/wri/wr-96-97/ud_txt2.htm

Zuckerman, M., Koestner, R., Colella, M.J., & Alton, A.O. (1984). Anchoring in the detection of deception and leakage. *Journal of Personality and Social Psychology*, 47(2), 301-311.

APPENDIX A: Interview Questions

Interview Opening

We're from the US Army Research Laboratory (ARL) at Aberdeen Proving Grounds, MD. We have been tasked, as one agency among many others, to collect information on what civilian and military observers look for in order to detect potentially dangerous individuals in different sized crowds of people. Such individuals may be intent upon committing hostile or violent acts. We need to learn better ways of recognizing them prior to such acts by their appearance and behavior. With the help of experienced observers like you we hope to learn more about the kinds of cues that can be used to detect potentially dangerous individuals. This knowledge will help us to help soldiers who will eventually deal with high-risk situations in urban environments.

All information will be completely confidential. No personal information will be collected or used. We are only interested in your experience, not in your identity.

General Background Questions

Age:_____ Job Title:_____ Gender:_____

How long have you been in this business (law enforcement)?

1. Do you work mostly as part of a team or alone? (If "alone", go to #2)

    a. Do you confer with the other team members while on a job? How many others?

    b. If you observe suspicious behavior of a person in a crowd do you confer with others in your team about that person before taking action?

    c. How do you communicate to another team member exactly which person or persons you are concerned about in a crowd?

    d. Do you ever have to work as an observer without conferring with others and make your own decisions about potential danger concerning a suspect?

2. Initially, were you trained in observation techniques in order to do your job?

3. Are you routinely given information about an assignment before performing the assignment?

4. Would you say that the majority of your day-to-day duties involve routine or non-routine tasks?

5. Even when you're off duty, do you find yourself observing people in crowds?

Cue Elicitation

We'd like to ask you specifically about the kinds of things you look for when you're observing people as part of your job.

6. Suppose you are observing the activity of people in a crowded ground or air terminal.

   a. Do you observe groups of people or individuals?

   Probing questions
   1. How they're dressed? Their age? Do they look different from others?
   2. What they're carrying?
   3. How they move through the crowd?
   4. How they behave?
   5. Body language?

7. Would your monitoring scheme change if it were a different environment (e.g., a city street, stadium event, foreign country)?

8. Do you think that observation techniques alone can give sufficient information about whether a person is intending to commit a crime?

   a. Would you need "intelligence" information to spot a suspect?

9. How accurately do you think you can select a person **intending** to commit a hostile act?

   a. In a crowd? group?
   b. On an individual basis?
   c . When the group is a different ethnicity from you?
   d . When the group is the same ethnicity as you?

10. What do you think is the ideal distance you must be from an individual suspect to detect whether he or she may be a potential problem?

11. Do you need physical or verbal interaction with a suspect to determine hostile intentions?

12. Do you think a person intending to cause harm emits a different "signal" (or displays different behavior) than a person with no intent to cause harm?

13. In the job of discriminating people with hostile intent from others with no hostile agenda, how important do you think it is to be able to clearly see the faces of those you are observing?

14. About how much time do you think you ought to observe a person to decide whether that person is a suspect and deserves further observation?

Situation Awareness

15. Is SA important in the performance of your job? Identifying hostile people?

16. Is it harder to achieve SA in some situations as opposed to other situations?

Experience and Training

17. Do you think that someone can be trained to identify hostile intent cues and go into the field and be effective? How much and what kind of training?

18. Do you think experience is an important factor in doing a good job of surveillance?

19. Do you think certain people are more intuitive than others in detecting suspicious behavior and just are better at the job?

20. Have you ever received follow-up information about an individual you identified as being suspicious and actually verified your judgment of that individual?

Decision-Making

21. Describe one particular situation in which you used certain cues to assess the situation but your assessment was false.

    a. Did you use the wrong cues or did you perceive the cues incorrectly?
    b. How often does such a situation occur?

22. When making decisions about a person's intent, do you

    a. perceive a cue and immediately decide on the appropriate action?
    b. choose one action plan from various choices of action plans?

Interview Closing

We are finished with our questions. Is there anything else you would like to add? Do you have any questions? This interview has been very informative, we appreciate your participation, and we thank you for your time.

APPENDIX B: Interview Questions for the Secret Service

Interview Opening

We're from the US Army Research Laboratory (ARL) at Aberdeen Proving Grounds, MD. We have been tasked, as one agency among many others, to collect information on what civilian and military observers look for in order to detect potentially dangerous individuals in different sized crowds of people. Such individuals may be intent upon committing hostile or violent acts. We need to learn better ways of recognizing them prior to such acts by their appearance and behavior. With the help of experienced observers like you we hope to learn more about the kinds of cues that can be used to detect potentially dangerous individuals. This knowledge will help us to help soldiers who will eventually deal with high-risk situations in urban environments.

All information will be completely confidential. No personal information will be collected or used. We are only interested in your experience, not in your identity.

General Background Questions

Age:_____ Job Title:_____ Gender:_____

How long have you been in this business (law enforcement)?

2. Initially, were you trained in observation techniques in order to do your job?

4. Would you say that the majority of your day-to-day duties involve routine or non-routine tasks?

5. Even when you're off duty, do you find yourself observing people in crowds?

Cue Elicitation

We'd like to ask you specifically about the kinds of things you look for when you're observing people as part of your job.

8. Do you think that observation techniques alone can give sufficient information about whether a person is intending to commit a crime?

   a. Would you need "intelligence" information to spot a suspect?

9. How accurately do you think you can select a person **intending** to commit a hostile act?

   c . When the group is a different ethnicity from you?

10. What do you think is the ideal distance you must be from an individual suspect to detect whether he or she may be a potential problem?

11. Do you need physical or verbal interaction with a suspect to determine hostile intentions?

12. Do you think a person intending to cause harm emits a different "signal" (or displays different behavior) than a person with no intent to cause harm?

13. In the job of discriminating people with hostile intent from others with no hostile agenda, how important do you think it is to be able to clearly see the faces of those you are observing?

14. About how much time do you think you ought to observe a person to decide whether that person is a suspect and deserves further observation?

Situation Awareness

15. Is SA important in the performance of your job? Identifying hostile people?

Experience and Training

17. Do you think that someone can be trained to identify hostile intent cues and go into the field and be effective? How much and what kind of training?

18. Do you think experience is an important factor in doing a good job of surveillance?

19. Do you think certain people are more intuitive than others in detecting suspicious behavior and just are better at the job?

Interview Closing

We are finished with our questions. Is there anything else you would like to add? Do you have any questions? This interview has been very informative, we appreciate your participation, and we thank you for your time.

APPENDIX C: Examples of Written Scenarios

You are sitting on a bench in a shopping mall observing people as they walk by. Two teenage boys walk by wearing long t-shirts. One is wearing pants and the other is wearing shorts. The boy wearing pants also wears a baseball cap, with the brim positioned at the back of the head. As the two boys continue walking out of view, nearby you see a little boy enter the steady stream of walking traffic and stand there. At about the same time, two women walk by pushing baby strollers. One woman is pushing a stroller with one hand and carrying a bag and a baby on the hip with the other hand. You see another woman walking by, but must maneuver around the small child still standing in the path of walking traffic. She appears to be eating something from a small bag. Your attention then shifts to a woman and two men standing in the path of walking traffic while holding a conversation. While observing these three individuals conversing, a man, wearing a light-colored buttoned-down shirt and stripped tie walks by. He is wearing a black electronic gadget attached to his right hip. Just as he walks out of view, you see a man pushing an empty stroller while a toddler follows close behind. The toddler becomes interested in another child that passes on his right. While observing what the toddler finds so interesting, you observe a man walking by using two crutches.

You are in a shopping mall and decide to watch people as they walk by. You observe a man and a woman approach a table and place bags in the nearest chair. The man then removes his wallet from his back pocket while talking with the woman. He looks straight ahead while the woman looks to her right. The man takes something from his wallet, hands it to the woman and the woman walks away. The man places his wallet back in his pocket and sits down. You then observe a man walking by. He stops and stands waiting for a woman to catch up with him. Meanwhile, you see an elderly man and woman slowly walk while talking to each other. As they walk out of view a young woman, walking alone, walks by quickly. At just about the same time, a young gentleman wearing a black t-shirt and jeans walks by casually. Your eyes then shift to a man, approximately 6 ft. 3 in. and 300 lbs. with a long ponytail. He is carrying a soda cup in his left hand. He is wearing a black t-shirt with no sleeves, black pants, and boots. His pants are tucked into his boots. He looks to his left while walking straight. You then observe a young woman getting up from a table and walking. She stops and hesitates as a man walks into her path. She stops. She waits until the man passes before continuing to walk. She approaches a trash can and tosses something into the can. She turns back around and begins to walk into the direction from which she had come.

APPENDIX D: Consent Form for Phase 2

Informed Consent for Participant's in Research Projects Involving Human Subjects

Title of Project: Activity-Based Target Acquisition Methods for Use in Urban Environments
Investigator(s): Tonya L. Smith-Jackson, Kimberly Myles

Purpose of the Research

The purpose of the research is to help provide the novice in the threat detection domain with the skill to identify and categorize persons as friend or foe. Such skills will allow novices to identify threatening people who are not otherwise identifiable by any other method in urban environments.

Procedures

This study will require that you read and sign a consent form. The study will require you to report on two different days. On Day 1 you will either receive 7 visual scenarios or 7 written scenarios. On Day 2 you will receive the treatment not received on Day 1. At least one day will need to pass between Day 1 & Day 2 of testing.

For each visual and written scenario, you will identify the scenario as threatening or non-threatening. If you think the scenario is threatening, you will also need to identify the threatening person(s) in the scenario and write down the nonverbal cues associated with the threatening individual(s). You will receive each written scenario on individual sheets of paper. You will be given one written scenario at a time and will be asked to read the scenario to yourself.

After all participants for this study have been tested the experimenter will compile a list of all the nonverbal cues collected. The experimenter will email you the written scenarios and a list of nonverbal cues. Each written scenario will be associated with its own set of nonverbal cues. You will be asked to rank order the cues from most important to least important in identifying that particular scenario as a threatening situation.

Your total time commitment will be 1 hour, 30 minutes – 30 minutes on the day that visual scenarios will be given and 40 minutes on the day that written scenarios will be given. Time commitments given for each day include 10 minutes for administrative concerns. The time commitment estimated to rank order cues sent by email is 20 minutes.

Risks

This study may present minimal risk associated with engaging in everyday activities.

Benefits

There is no immediate benefit to you for participating in this study other than the assurance you may feel that this research may improve how soldiers conduct missions in urban environments.

Confidentiality

The information gained in this research project will be kept strictly confidential. At no time will the researcher release the results of the study to anyone other than individuals working on the project without your written consent.

Data will be stored securely and will be made available only in the context of research publications and discussion. No reference will be made in oral or written reports which could link you to the data nor will you ever be identified as a participant in the project.

Compensation

You will be paid $60 for participation in the entire study. However, you are free to withdraw from this study at any time without penalty. If you choose to discontinue your participation at any time, you will be paid at a rate of $10.00 per hour for the time you have expended. Compensation will be paid at the end of the study. You will be paid with a check and it will be mailed to you.

Freedom to Withdraw

You are free to withdraw from this study at any time without penalty. You are also free not to answer any questions or respond to experimental situations that you choose without penalty.

Contacts for Additional Assistance

If you have questions at any time about the project or the procedures, you may contact the principal investigator, Tonya Smith-Jackson at 540-231-4119 or smithjack@vt.edu (519-H Whittemore).

If you feel you have not been treated according to the descriptions in this form, or your rights as a participant have been violated during the course of this project, you may contact David Moore, Chair of the Institutional Review Board Research Division at 540-231-4991.

Participant's Permission

I do hereby volunteer to participate in the research project described in this document. The implications of my voluntary participation, duration, and purpose of the research project, the methods and means by which it is to be conducted, and the inconveniences and hazards that may reasonably be expected have been explained to me. I have been given an opportunity to ask questions concerning this research project. Any such questions were answered to my full and complete satisfaction. I understand that any published data will not reveal my identity. If I choose not to participate, or later wish to withdraw from any portion of it, I may do so without penalty.

Printed Name Of Volunteer (First, MI., Last)	
Today's Date (Month, Day, Year)	*Signature Of Volunteer*

APPENDIX E: Heuristic Validation Questionnaire

Heuristic #1: Clearly define the situation.

- Increases "situational" awareness.
- Non-verbal cues of threat are situation specific.
- Used to build some "level of expectation".

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #2: Visual versus (Written or Oral) scenarios are best for portraying non-verbal threat.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #3: Incorporate visual scenarios that contain no threat.

- Needed as a contrast to threat to teach new recruits what situations with no threat look like.
- Personnel cannot always be in "on" mode so recognition of non-threatening situations gives brief periods to operate in "unbiased" mode.

==========

1. **Relevance**

   How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

   1 2 3 4 5

   not relevant at all very relevant

2. **Importance**

   How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

   1 2 3 4 5

   not important at all very important

3. **Violation**

   How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

   1 2 3 4 5

   never very often

4. **Integration**

   How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

   1 2 3 4 5

   not easy at all very easy

5. **Universal Domain Use**

   How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

   1 2 3 4 5

   not realistic at all very realistic

Heuristic #4: Incorporate lecture-type teaching sessions to teach why and how specific non-verbal cues are associated with specific situations.

- Provide the specific non-verbal cue(s)
- Place the non-verbal cue in context
- When a visual stimulus of the non-verbal cue is presented it will strengthen what was learned in the lecture.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #5: Show visual representations or scenarios more than once.

- Some new recruits will need to see visual representations more than once.
- Presenting the visual scenarios a number of times will aid new recruits in practicing how to establish "normal" baseline behaviors.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #6: Require new personnel to include reasons for decisions made…why that decision?

- Answers will reveal information about the new recruit's decision-making process.
- The training instructor will have some idea of how to help the recruit change, correct, and reorganize visual and cue-related information to correct situational awareness errors.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #7: Refresh threat detection skills and knowledge for new recruits as often as permitted.

- Refresher training will reinforce knowledge that has been previously learned and acquired through experience.
- Permits new recruits to modify and update their knowledge base to maintain a high-level of situational awareness.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #8: Identify and keep cumulative training records for above-average performing personnel.

- Recruit this group of personnel to help design and update training modules and materials.
- Excellent personnel choice to facilitate training sessions.
- Difficult-to-explain domain concepts may emerge in real-world examples during training sessions.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Heuristic #9: Continuously improve the content of visual scenarios.

- As new tactics are developed by the enemy, visual scenarios should be updated to include these tactics.
- Exposure to examples of the visual tactics will allow new recruits to transfer this training to real-world situations and immediately identify the new tactical behaviors and events as they begin to unfold.
- Helps in maintaining a high-level of situational awareness.

==========

1. **Relevance**

How relevant do you think this heuristic is for teaching entry-level recruits to detect a threat?

1 2 3 4 5

not relevant at all very relevant

2. **Importance**

How important do you think this heuristic is to follow as a "rule-of-thumb" when designing a training program to help entry-level recruits successfully acquire the skill of threat detection?

1 2 3 4 5

not important at all very important

3. **Violation**

How often do you think this heuristic is violated in current threat detection training programs for entry-level recruits?

1 2 3 4 5

never very often

4. **Integration**

How easy do you think this heuristic is to integrate into an existing threat detection training program for entry-level recruits?

1 2 3 4 5

not easy at all very easy

5. **Universal Domain Use**

How realistic do you think this heuristic is for use by most law enforcement agencies in designing a threat detection training program for entry-level recruits?

1 2 3 4 5

not realistic at all very realistic

Below is a list of the heuristics you just rated. If there are any additional "rules-of-thumb" you think are important for training entry-level recruits to be successful in the identification of threat please list them in the empty numbered spaces provided. Also include why you feel the "rule" is important.

1. Clearly define the situation.

2. Visual versus (Written or Oral) scenarios are best for portraying non-verbal threat.

3. Incorporate visual scenarios that contain no threat.

4. Incorporate lecture-type teaching sessions to teach why and how specific non-verbal cues are associated with specific situations.

5. Show visual representations or scenarios more than once.

6. Require new personnel to include reasons for decisions made…why that decision?

7. Refresh threat detection skills and knowledge for new recruits as often as permitted.

8. Identify and keep cumulative training records for above-average performing personnel.

9. Continuously improve the content of visual scenarios.

10.

11.

12.

13.

APPENDIX F: Consent Form for Phase 3

Informed Consent for Participant's in Research Projects Involving Human Subjects

Title of Project: Activity-Based Target Acquisition Methods for Use in Urban Environments
Investigator(s): Tonya L. Smith-Jackson, Kimberly Myles

Purpose of the Research

The purpose of the research is to help provide the novice in the threat detection domain with the skill to identify and categorize persons as friend or foe. Such skills will allow novices to identify threatening people who are not otherwise identifiable by any other method in urban environments.

Procedures

This study will require that you read and sign a consent form. You will be given a heuristic and an evaluation form and will be asked to evaluate the contents of the heuristic. The evaluation form will require you to answer questions about the heuristic, as well as, provide your opinions about how to improve the tool via comments and suggestions. You may comment about any aspect of the heuristic. Your total time commitment will be 40 minutes – 30 minutes for the evaluation and 10 minutes for administrative concerns.

Risks

This study may present minimal risk associated with engaging in everyday activities.

Benefits

There is no immediate benefit to you for participating in this study other than the assurance you may feel that this research may improve how soldiers conduct missions in urban environments.

Confidentiality

The information gained in this research project will be kept strictly confidential. At no time will the researcher release the results of the study to anyone other than individuals working on the project without your written consent.

Data will be stored securely and will be made available only in the context of research publications and discussion. No reference will be made in oral or written reports which could link you to the data nor will you ever be identified as a participant in the project.

Compensation

You will be paid $60 for participation in the entire study. However, you are free to withdraw from this study at any time without penalty. If you choose to discontinue your participation at any time, you will be paid at a rate of $10.00 per hour for the time you have expended. Compensation will be paid at the end of the study.

Freedom to Withdraw

You are free to withdraw from this study at any time without penalty. You are also free not to answer any questions or respond to experimental situations that you choose without penalty.

Contacts for Additional Assistance

If you have questions at any time about the project or the procedures, you may contact the principal investigator, Tonya Smith-Jackson at 540-231-4119 or smithjack@vt.edu (519-H Whittemore).

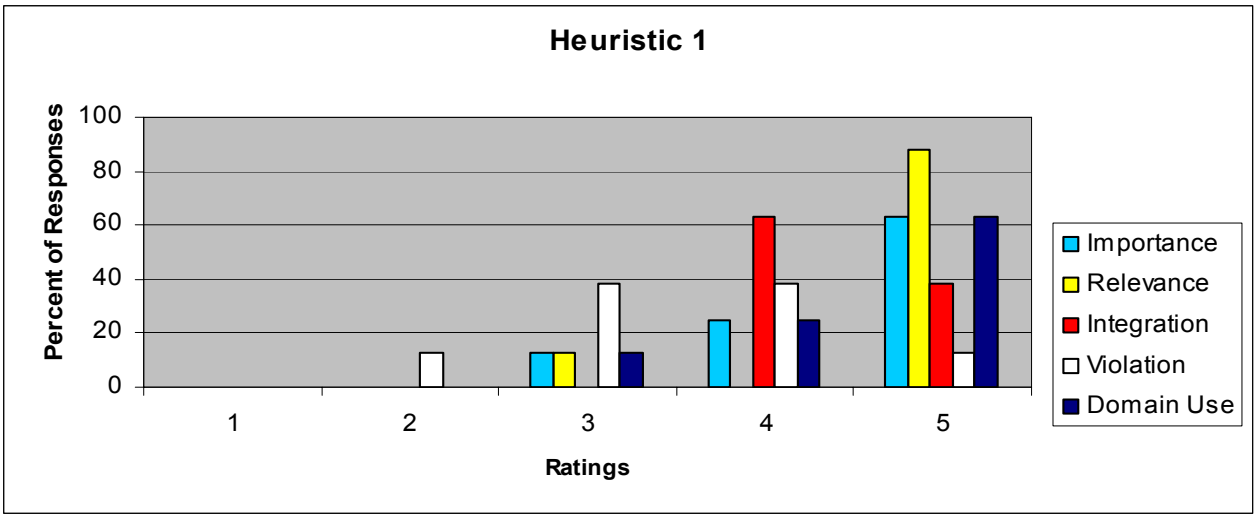
If you feel you have not been treated according to the descriptions in this form, or your rights as a participant have been violated during the course of this project, you may contact David Moore, Chair of the Institutional Review Board Research Division at 540-231-4991.

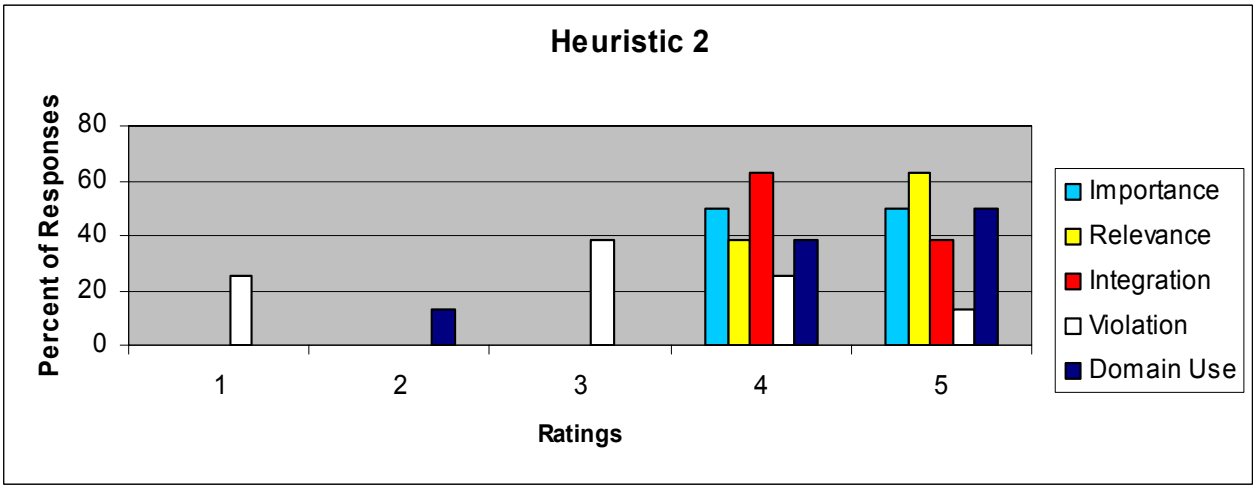
Participant's Permission

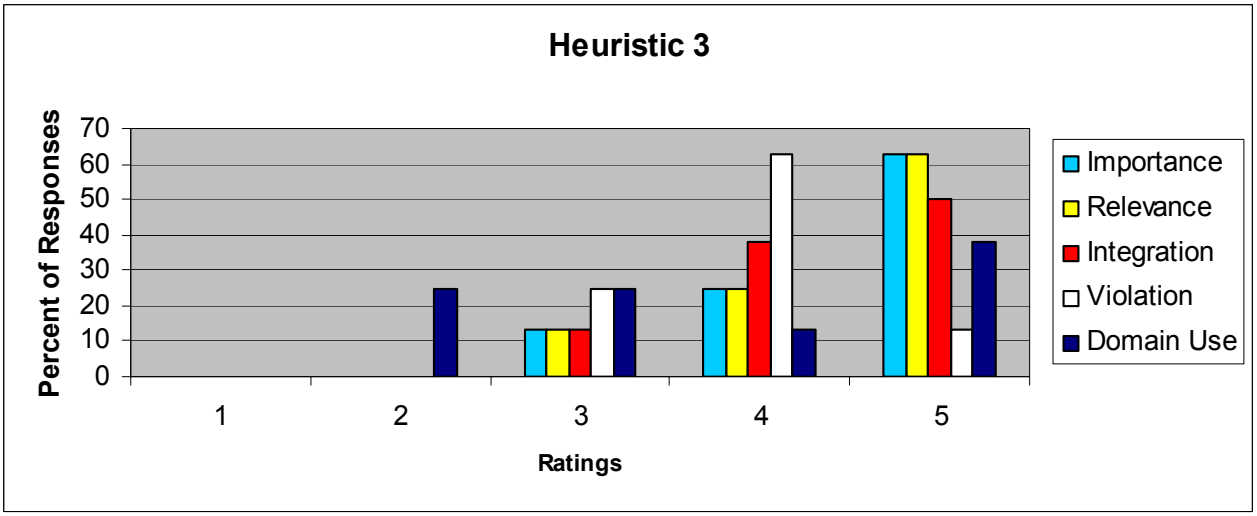
I do hereby volunteer to participate in the research project described in this document. The implications of my voluntary participation, duration, and purpose of the research project, the methods and means by which it is to be conducted, and the inconveniences and hazards that may reasonably be expected have been explained to me. I have been given an opportunity to ask questions concerning this research project. Any such questions were answered to my full and complete satisfaction. I understand that any published data will not reveal my identity. If I choose not to participate, or later wish to withdraw from any portion of it, I may do so without penalty.

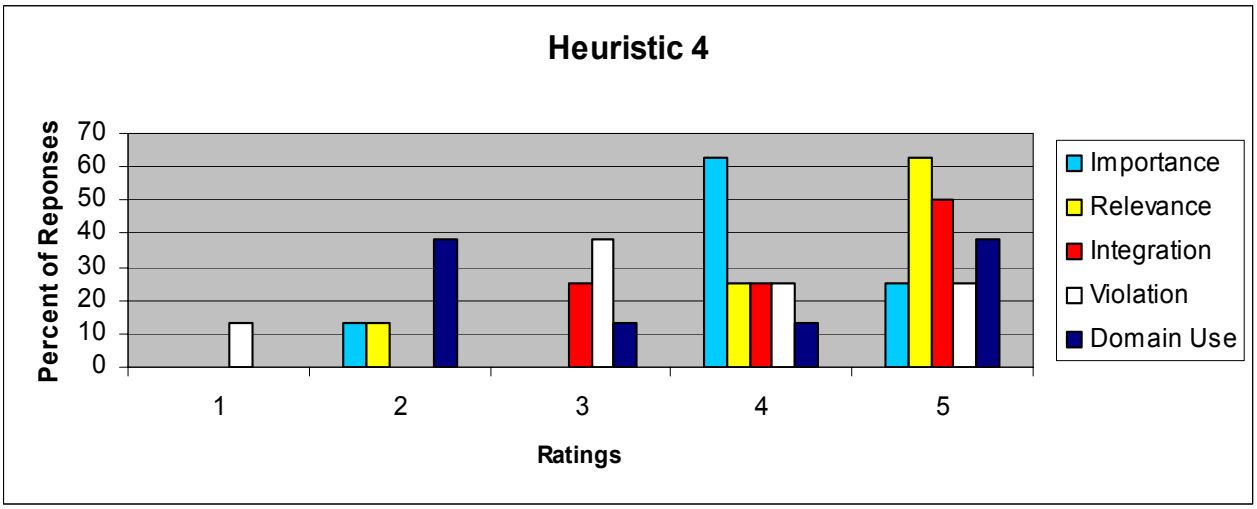
Printed Name Of Volunteer (First, MI., Last)	
Today's Date (Month, Day, Year)	*Signature Of Volunteer*

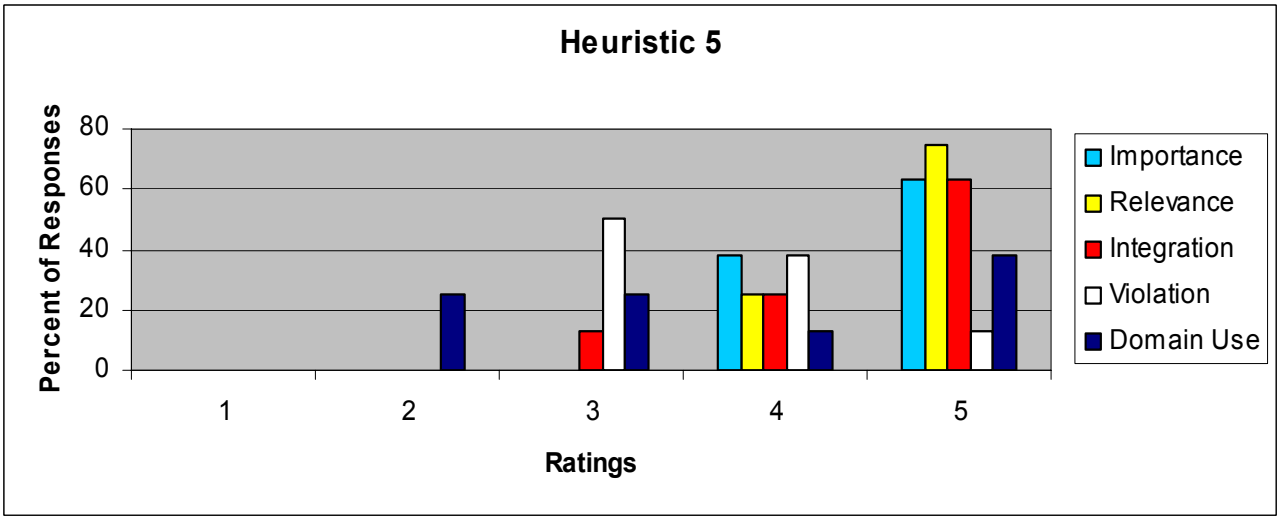
APPENDIX G: The Percentage of Expert Responses for Each Construct by Rating Level for Each Individual Heuristic

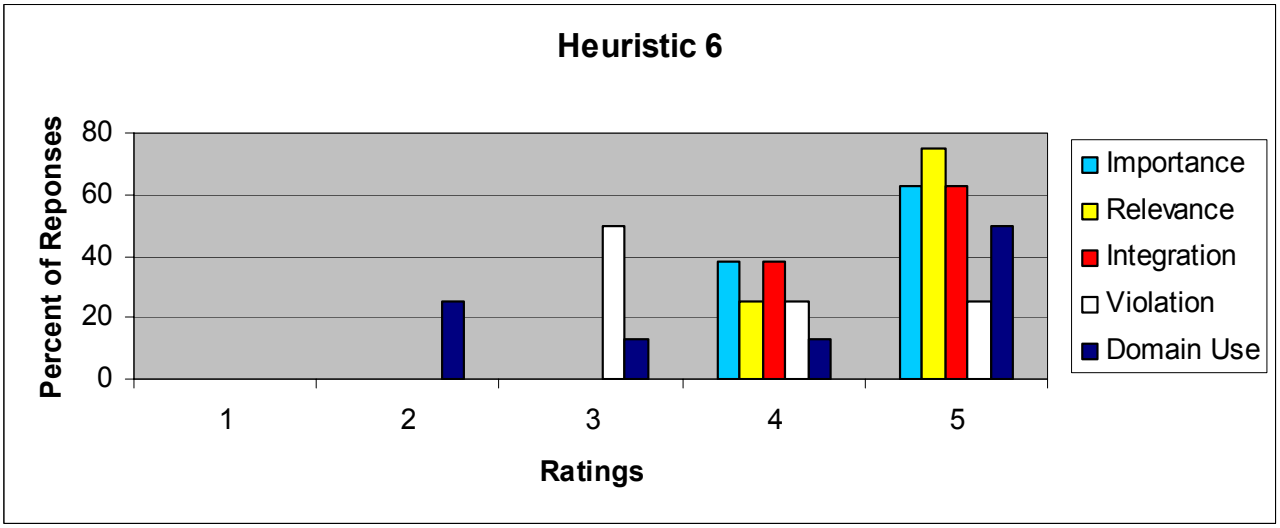

Heuristic 1
Percent of Responses
100
80
60
40
20
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use

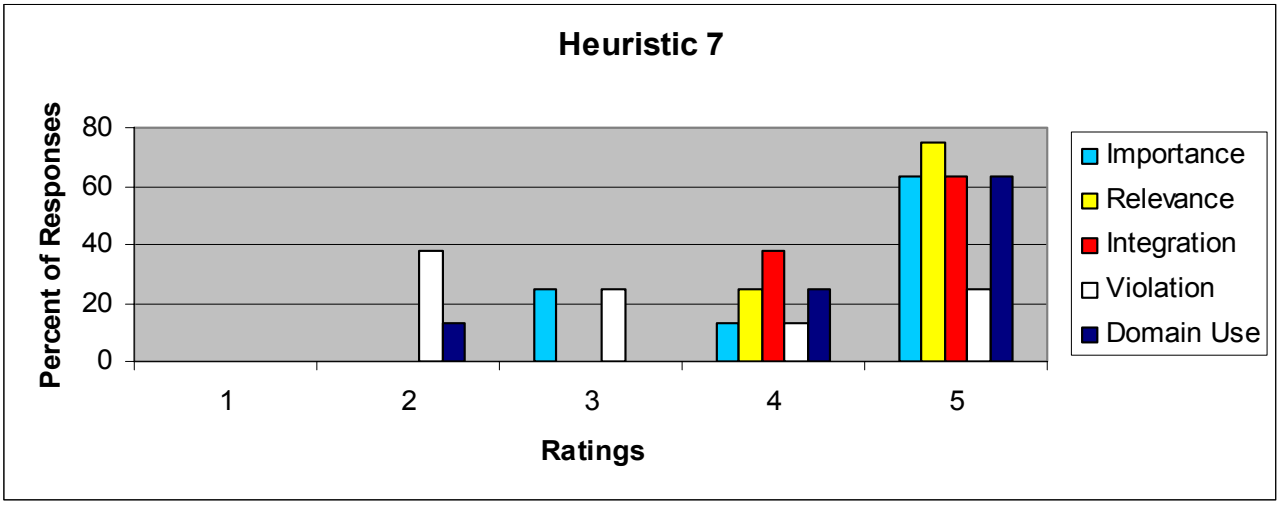

Heuristic 2
Percent of Responses
80
60
40
20
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use

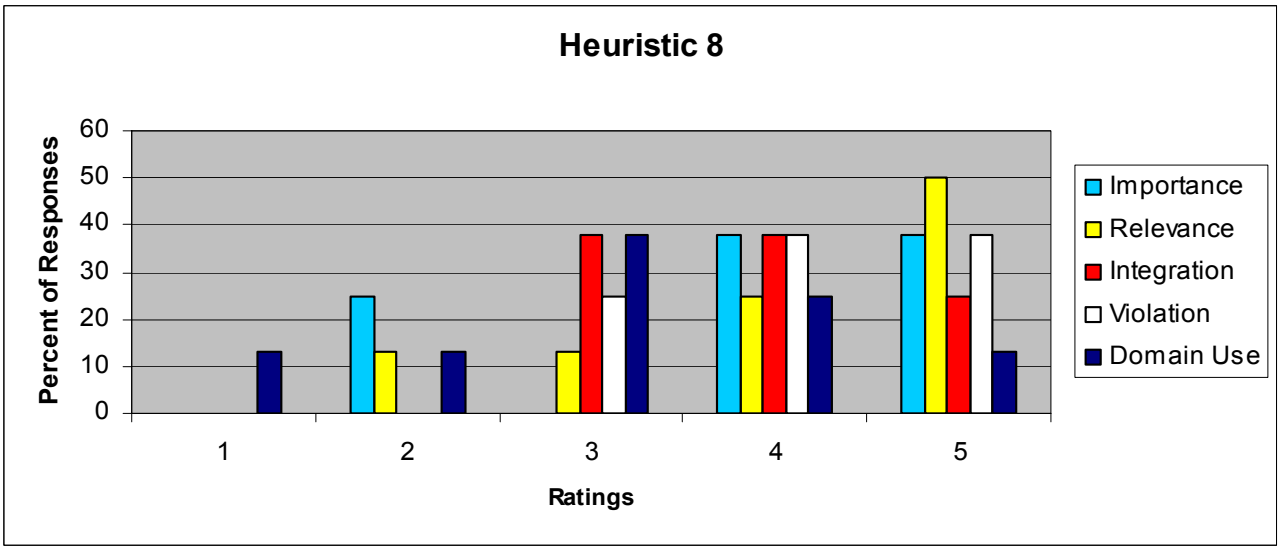

Heuristic 3
Percent of Responses
70
60
50
40
30
20
10
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use

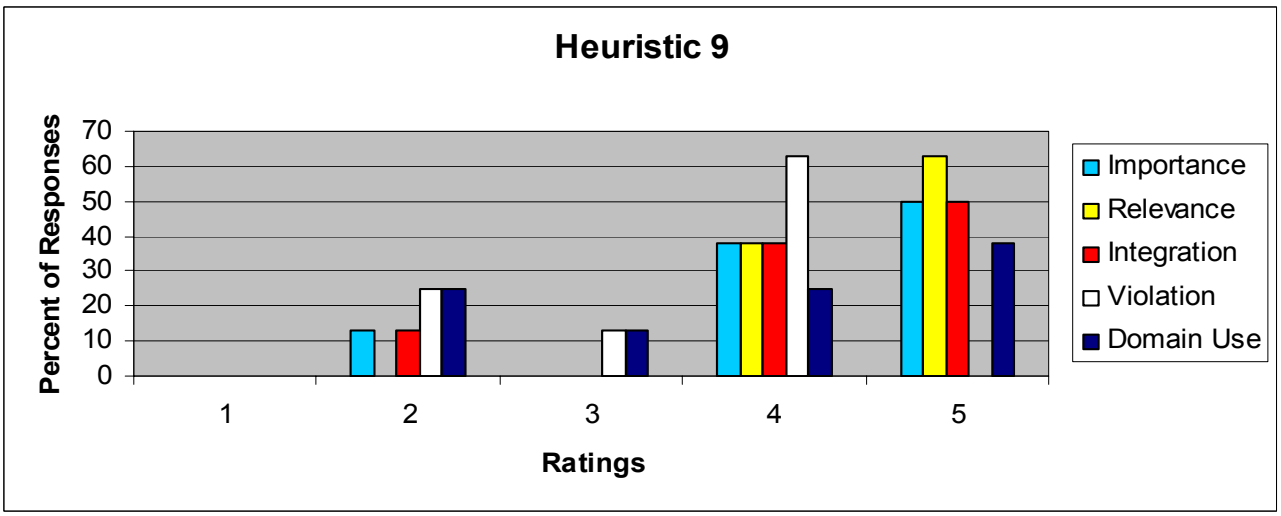

Heuristic 4
Percent of Reponses
70
60
50
40
30
20
10
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use


Heuristic 5
Percent of Responses
80
60
40
20
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use


Heuristic 6
Percent of Reponses
80
60
40
20
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use


Heuristic 7
Percent of Responses
80
60
40
20
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use


Heuristic 8
Percent of Responses
60
50
40
30
20
10
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use


Heuristic 9
Percent of Responses
70
60
50
40
30
20
10
0
1
2
3
4
5
Ratings
Importance
Relevance
Integration
Violation
Domain Use