ARMY RESEARCH LABORATORY

Remote Detection of Covert Tactical Adversarial Intent of Individuals in Asymmetric Operations

by Ann Bornstein, Thyagaraju Damarla, John Lavery, Frank Morelli, and Elmar Schmeisser

ARL-SR-197 **April 2010**

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

ARL-SR-197 **April 2010**

Remote Detection of Covert Tactical Adversarial Intent of Individuals in Asymmetric Operations

Ann Bornstein
Computational and Information Sciences Directorate, ARL

Thyagaraju Damarla
Sensors and Electron Devices Directorate, ARL

John Lavery
Elmar Schmeisser
U.S. Army Research Office

Frank Morelli
Human Research and Engineering Directorate, ARL

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
April 2010	Final	7–8 December 2009

4. TITLE AND SUBTITLE
Remote Detection of Covert Tactical Adversarial Intent of Individuals in Asymmetric Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Ann Bornstein, Thyagaraju Damarla, John Lavery,* Frank Morelli, and Elmar Schmeisser*

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: RDRL-CII-C
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-SR-197

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
U.S. Army Research Office, U.S. Army Research Laboratory, P.O. Box 12211, Research Triangle Park, NC 27709-2211

14. ABSTRACT

The goal of this report is to design a first-order road map for modeling research to bridge the scientific gap between observations from physical sensor networks at 3–50 m on the one hand and determination of covert tactical adversarial intent of individuals with deception and in extensive clutter on the other. The research needs to integrate components from kinesiology, neurophysiology, psychology, cognitive science, sociocultural anthropology, and information science. Research and development (R&D) issues that need to be considered include metrics for cognitive phenomena and how well detection systems work, data sets, determining whether actors can provide sufficient verisimilitude to create data sets, and relevant sensing technologies and information fusion techniques. Successful procedures may need to include actively (but unobtrusively) perturbing the situation in order to elicit specific responses. Comprehensive Department of Defense, Department of Homeland Security, Intelligence Advanced Research Projects Activity, and Federal R&D programs are required to promote rapid progress. The Federal Government should fund R&D programs with the objective of producing a theoretically founded design of a prototype system for remote detection of covert tactical adversarial intent of individuals in asymmetric operations within 5 years and a working operational system within 10 years.

15. SUBJECT TERMS
adversarial, asymmetric, covert, detection, intent, remote

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Ann Bornstein
Unclassified	Unclassified	Unclassified	UU	46	19b. TELEPHONE NUMBER (*Include area code*) 410-278-8947

Contents

Preface

On December 7 and 8, 2009, the U.S. Army Research Laboratory (ARL) held a Strategic Directions Workshop "Remote Detection of Covert Tactical Adversarial Intent of Individuals in Asymmetric Operations" at its laboratory in Adelphi, MD. Collaborating in this workshop were ARL's U.S. Army Research Office (ARO), Computational and Information Sciences Directorate (CISD), Human Research and Engineering Directorate (HRED), and Sensors and Electron Devices Directorate (SEDD); the U.S. Army's Communications and Electronics Command's (CECOM's) Night Vision and Electronic Sensors Directorate (NVESD) and Intelligence and Information Warfare Directorate (I2WD); the U.S. Air Force Research Laboratory's (AFRL's) Human Effectiveness Directorate; and the Defense Academy for Credibility Assessment (DACA). The participants in the workshop are listed in appendix A of this report. The goal of the workshop was to design a first-order road map for research to bridge the scientific gap between observations from physical sensor networks at 3–50 m on the one hand and determination of covert tactical adversarial intent of individuals on the other.

The first day of the workshop consisted mainly of short (5–10 min) presentations of relevant material coupled with extensive, in-depth discussion. At the end of the first day, information on paths to the future in many of the technical themes of the workshop was available. The information was sketchy, not well organized, and partially conflicting. At the end of the first day, the workshop participants set up three working groups (cognitive/perceptual phenomena, sensors, and information fusion) for the second day. The second day of the workshop consisted of working sessions to write and organize the technical information and resolve conflicts. Based on the material written at the workshop and material subsequently written by the workshop participants, the present unified report was collated and written by the workshop steering committee with the input and advice of the workshop's participants. The workshop and the report are unclassified with unlimited distribution. The main audience for this report is U.S. Department of Defense and Federal management, and the scientific and engineering research and development community interested in remote detection of adversarial intent.

It is because of the participants in the workshop, who generously shared their time, experience, and advice, that this report could be written. The workshop steering committee expresses its gratitude to them. This report affirms that remote detection of covert tactical adversarial intent of individuals in asymmetric operations is an area that is feasible and holds great promise for the future. It is our hope and expectation that this document will contribute to harnessing interdisciplinary science and technology in this area for the benefit of the United States and its allies.

Ann Bornstein, CISD, ARL; Thyagaraju Damarla, SEDD, ARL; John Lavery and Elmar Schmeisser ARO, ARL; Frank Morelli, HRED, ARL

INTENTIONALLY LEFT BLANK.

Executive Summary

The ability to identify covert intent of individuals who may be hostile would significantly improve asymmetric counter-insurgency and peace-keeping operations. Such individuals are generally embedded in extensive "clutter" of neutral and friendly human beings and various physical objects. At present, covert adversarial intent is identified through judgment of Soldiers and close-range sensing and searching, which often entail significant danger and possibly high false-positive and false-negative rates. Approaches to checkpoints (before a person gets close enough to blow up the checkpoint) and remote screening of people on patrol missions are defense scenarios where remote determination of adversarial intent is needed. Determining covert adversarial intent will help shift the balance in operations, mission planning, training, and simulation from more costly and dangerous sweeping operations toward much safer pinpoint operations based on refined estimates of people from which danger may come. Dual-use civilian benefits will be in crowd control and antidrug, anticrime, and border security.

The fundamental principles that allow remote (i.e., at 3–50 m) identification of covert adversarial intent based on externally observable physical information are not known. The goal of this report is to design a first-order road map for modeling research to bridge the scientific gap between observations from physical sensor networks at 3–50 m on the one hand and determination of covert tactical adversarial intent of individuals with deception and in extensive clutter on the other. Although empirical observations and experiments will play large supporting roles in this research, the main emphasis is on discovery of theoretically justified quantitative predictive principles (models) and their implementation in tractable analytical and computational procedures. To be successful, the research needs to integrate components from kinesiology, neurophysiology, psychology, cognitive science, sociocultural anthropology, and information science.

An important and often overlooked concept is measuring the problem. Metrics for cognitive phenomena and for how well detection systems work are needed. In addition to being practically useful, the metrics need to be computationally feasible (not combinatorially expensive) and mathematically justified. In cases where the computational cost of the desired metric(s) is too large, approximate ersatz metrics need to be developed. Whatever metrics or ersatz metrics are proposed should be justified not based on traditional use of the metrics in other areas, successful as that use may be, but rather on the basis of human goals in the remote detection of covert tactical adversarial intent.

One major issue is the development of data sets. Can "method acting" (or any other school of acting) provide sufficient verisimilitude on all scales, including emotive/biochemical (sweat, breath, body habitus, kinesiology) to permit its use as a surrogate for "real" data? If so, the

creation of data sets, while still expensive, will be less expensive. One methodology for developing valid empirical data sets is to design experimental scenarios so that behaviors of interest are likely to be expressed. If enacted experiments cannot provide data that matches data of "real" situations, the expense and uncertainty will be larger.

Sensing will require utilizing as many different measureable indicators of intent as possible and, thus, integration of multiple sensor modalities. Potential indicators of adversarial intent include posture, posture rigidity, heartbeat waveform, heart rate, breath rate (volume approximation, patterns, anomalies), wheezing, coughing, gasping, blood pressure trends (waveform shape and transit time), pulse-wave velocity (beat-by-beat approximation of blood pressure), movement (fidgeting, remaining still, shaking, shivering, having spasms), body stiffness, muscle tension, resonant frequency of body movement, voice stress analysis, voice onset timing, gastrointestinal distress, bowel sounds, reluctance to engage socially (distance from others, response to attempts to engage verbally), observation tendencies of subject (eye-glancing, head turning, situational awareness), people whose actions are coordinated or who are actively avoiding each other, exposure to bomb-making materials/chemicals, hyperthermia from stress (generally expressed in the face, palms of the hands, and soles of the feet), gait as indicators of stiffness (stress) or carrying a load or wearing protective clothing, breath biochemistry, and microbiology. Sensing technologies that may be able to measure relevant data include visible bandwidth imagers, thermal imagers, hyperspectral imagers, laser Doppler vibrometry, E-field, radar, ladar, gas chromatography, interrogators of the genetic signatures of prokaryotic microorganisms, chemical sensors (laser-induced fluorescence, laser-induced breakdown spectroscopy, Raman spectroscopy), photoacoustic sensors, retroreflection sensors, seismic sensors, and magnetic sensors.

Fusion of the information from multiple sensors will be required to achieve accuracy. The Joint Directors of Laboratories (JDL) Data Fusion Model is the most widely used method for categorizing data-fusion-related functions. The JDL model is composed of levels of abstraction, with level 0 being the lowest or the minimally processed information level and with level of abstraction increasing in levels 1–4. Although there are many criticisms of the JDL model and many competing models, the JDL model has, in general, withstood the test of time, and most of the fusion community has accepted the JDL fusion levels. The JDL fusion framework is a suitable (but not the only) framework in which fusion of the output of many different sensors could take place.

Successful identification procedures may need to include actively (but unobtrusively) perturbing the situation in which the sensing takes place in order to elicit specific responses (an abstract analogue of putting speed bumps in approaches to checkpoints so that the oscillation of cars can be observed and one can infer whether the car is carrying a heavy load).

Comprehensive U.S. Department of Defense, Department of Homeland Security, Intelligence Advanced Research Projects Activity, and Federal research and development (R&D) programs are required to promote rapid progress. Specific recommendations are as follows:

- The Federal Government should fund R&D with the objective of producing a theoretically founded prototype system for remote detection of covert tactical adversarial intent of individuals in asymmetric operations within 5 years and a working operational system within 10 years.
- The Federal Government should continue to provide broad support for academic and industrial efforts both in remote detection of adversarial intent and in areas (such as linkage of these systems with databases, media, and human input) that are useful for larger systems of systems.
- The strong interdisciplinary nature of remote detection of adversarial intent should be reflected in all efforts supported by the Federal Government.

INTENTIONALLY LEFT BLANK.

1. Introduction

Today's operations are being conducted in congested urban and remote mountainous terrains against an asymmetric threat. The targets that they encounter consist of (1) humans trained to maximize their disguise and conceal their intentions, (2) commercial vehicles, compact cars, sedans, station wagons and trucks optimized for quiet and smooth driving, and (3) explosives in the form of IEDs (improvised explosive devices) and UBEs (unknown bulk explosives) well hidden and camouflaged to minimize detection. These targets are hard to locate. Efforts are made by foes to plan these operations and conduct repeated rehearsals to provide the appearance of normal day-to-day events. The threat targets blend in the crowd, hide behind objects, and purposely occlude their appearance. Our foes spend many hours training and rehearsing every step of the operation to make the preparation and deployment up until the time of the actual attack or detonation appear as normal as possible.

The ability to identify covert intent of individuals who may be hostile would significantly improve asymmetric counter-insurgency and peace-keeping operations. Such individuals are generally embedded in extensive "clutter" of neutral and friendly human beings and various physical objects. At present, covert adversarial intent is identified through judgment of Soldiers and close-range sensing and searching, which often entail significant danger and possibly high false-positive and false-negative rates. Approaches to checkpoints (before a person gets close enough to blow up the checkpoint) and remote screening of people on patrol missions are defense scenarios where remote determination of adversarial intent is needed. Determining covert adversarial intent will help shift the balance in operations, mission planning, training, and simulation from more costly and dangerous sweeping operations toward much safer pinpoint operations based on refined estimates of people from which danger may come. Dual-use civilian benefits will be in crowd control and in antidrug, anticrime, and immigration enforcement.

It has been known since the Facial Action Coding System (FACS) created by Ekman and Friesen (1978) that the expression and microexpression of certain emotions related to adversarial intent take place partially involuntarily through facial muscles. Other physiological actions such as speech, heart rate, respiration rate, skin temperature, and perspiration can also carry information about emotions related to intent, although they are more subject to environmental influence than facial expressions. Laser methods can detect muscle movement, heart, and respiration rate and skin temperature. Visual sensors provide information about facial and body dynamics. Computer vision techniques can now automatically track facial expressions, eye movement and gestures. The ability to fuse information, for example, laser information with visual information, and to identify seemingly hidden patterns is increasing rapidly. Many of these techniques require close-range sensing/observation, often in a controlled environment and at the 0–2 m

range. This is suitable for airport screening but not appropriate for asymmetric defense scenarios, where threats need to be detected at distances at 3 m and, preferably, up to 50 m. To what extent close-range sensing techniques can be extended to larger ranges is not yet known. Moreover, modeling of the connection between emotions and intent is quite incomplete. Detecting that a person is afraid, for example, does not provide significant evidence for or against a hypothesis that the person has adversarial intent, since both friendly and adversarial people often have fear in commonly encountered scenarios. Conversely, a person with adversarial intent may show little or no fear. While there is some understanding about how to detect emotions, there is much less understanding about how to go further into the cognitive realm and determine intent.

The fundamental principles that allow remote (i.e., at 3–50 m) identification of covert adversarial intent based on externally observable physical information are not known. Indeed, the step from recognizing physical objects, events, and patterns to recognizing intent is fairly described as a scientific chasm. Recent basic research related to bridging this chasm includes, but is not limited to, "Future Attribute Screening Technology (FAST)" (Department of Homeland Security—DHS), "Violent Intent Modeling and Simulation (VIMS)" (DHS), "Detection of Intent through Perception of Biomotion Signatures" and "Visualization of Belief Systems" (U.S. Army Research Laboratory Human Research and Engineering Directorate—ARL/HRED), "Remote and Passive ID of Electrodermal Response" (Night Vision and Electron Sensors Directorate—NVESD), "Behavioral Signatures" and "Human MASINT" (U.S. Air Force Research Laboratory—AFRL), "Hostile Intent" (U.S. Naval Research Laboratory—NRL), "Computational Modeling of Adversary Attitudes and Behaviors" (U.S. Air Force Office of Scientific Research—AFOSR, George Mason University), "Dynamic, Adaptive Techniques for Adversary Behavior Modeling" (AFOSR, University of Maryland—U MD), "Human, Social, Cultural, and Behavioral Modeling" (U.S. Army Research Office—ARO, Carnegie Mellon University, U MD), and "Tools for Recognizing Unconscious Signals of Trustworthiness Program (TRUST)" (Intelligence Advanced Research Projects Activity—IARPA).

The goal of this report is to design a first-order road map for modeling research to bridge the scientific gap between observations from physical sensor networks at 3–50 m on the one hand and determination of covert tactical adversarial intent of individuals with deception and in extensive clutter on the other. Although empirical observations and experiments will play large supporting roles in this research, the main emphasis is on discovery of theoretically justified quantitative predictive principles (models) and their implementation in tractable analytical and computational procedures. To be successful, the research needs to integrate components from kinesiology, neurophysiology, psychology, cognitive science, sociocultural anthropology, and information science.

Throughout this report, the phrase "remote detection of adversarial intent" will mean "remote (at 3–50 m) detection of covert tactical adversarial intent of individuals in asymmetric operations."

1.1 Technical Themes

The technical themes of the workshop were as follows:

- The strong interdisciplinary nature of remote detection of adversarial intent should be reflected in all efforts supported by the Federal Government.
- Definition and quantification of types and/or classes of covert adversarial intent of individuals that generate terrorist/insurgent activities.
- Principles from kinesiology, neurophysiology, psychology, cognitive science, sociocultural anthropology, and information science that link covert adversarial intent with data/information that can be observed noncooperatively through physical sensor networks at 3–50 m. The principles must take extensive clutter and deception by the targets into account.
- Research on identifying emotions. However, emotions do not uniquely map (or, at least, it is not yet known that a collection of emotions can be uniquely mapped) to intent. For approaches involving emotions, the models that link the emotions to intent need to be considered.
- Both passive and active sensing modes need to be considered.
- Metrics for measuring adversarial intent. All metrics need to be based on cognitive, psychological, neurophysiological, and/or kinesiological principles. *Ad hoc* or heuristic metrics are not preferred. Most classical metrics (such as the root-mean-square or "rms" metric, L_p metrics, etc.) are of doubtful applicability. The metrics need to be capable of distinguishing "normal" and "anomalous."
- Identification of relevant data sources, determination of what data are relevant, and determination of new types/forms of information, sensors, and exploitation that may be needed.
- Quantitative procedures that can, in extensive clutter, automatically infer from remotely observed data/information (shape, color/spectrum, movement, temperature, etc., on scales from micro to macro) covert adversarial intent of individuals. These procedures will involve fusion of parallel, unreliable, asynchronous data and information from "orthogonal" sensing modes.
- "Data tractability" of the quantitative procedures (i.e., the ability to produce accurate results with data no more than is realistically likely to be available).
- Scalability and overall computational feasibility of the quantitative procedures.
- Limitations of the procedures, including whether the procedures do not work under various circumstances and/or cannot identify some types of covert adversarial intent. Estimation of the extent to which the procedures produce false positives and false negatives.

- Creation of empirical data sets to aid in creating new theory and quantitative procedures and for verification and validation. How can the data sets be collected to emphasize U.S. Department of Defense (DOD) needs?
- Verification and validation of the quantitative procedures on empirical data sets.

1.2 Delineation vs. Neighboring Areas

The topic of this report is to detect individual intent and deception at distances (3–50 m) at which the damage that an individual can do is limited. There are many important related topics that are not focal topics of this report. We describe these topics here.

1. Information operations and deciphering enemy strategic and tactical intent in predicting what actions the enemy force will undertake when and where are highly important but not the focus of this report.
2. Although close-range techniques for airport security checking are generally not included, the extent to which the ranges of these techniques can be extended and whether they can work in noncooperative scenarios is included. Skin conditions that can be remotely detected—even though they may usually be detected at short range—do fit the focus of the report. Very close-range cooperative techniques such as EEG (electroencephalography), fMRI (functional magnetic resonance imaging), polygraph, etc., are not included.
3. Research on physical pattern recognition (physical appearance and action) is likely to form a significant portion of the basis for the research envisioned in this report. However, research on physical pattern recognition is not, per se, a focus of the report. Research on physical pattern recognition is widely labeled research about determining intent, but such labeling is often inaccurate. For example, detecting a person with a gun running across a field toward a high-value target in video images is not equivalent to detecting adversarial intent. That person may well be a local security officer (whose job requires him to carry a gun) who wishes to urgently communicate that the real threat is a suicide duo disguised as fruit merchants poised to strike within a short time. Physical pattern recognition needs to be accompanied by science-based modeling that links the physical and cognitive.
4. In future operations, the physical sensor networks will certainly be supported by human reporting, media, databases, data mining, learning, World Wide Web, game theory, etc. These topics are not foci of this report. However, the report does recognize that models that bridge the gap between remote physical sensing and cognitive phenomena will be embedded into larger frameworks that use these additional sources of information.
5. Behavior modeling is the basis and context for this report but not the theme.
6. Predictive modeling (What specifically will that person do next?) is a potential next step but not the focus of this report.

2. Remote Detection of Intent: The Current Situation and the Future

In the early part of the 21st century, we are in the middle of "asymmetric warfare." Asymmetric warfare, i.e., armed conflict between a nation and often faceless, nameless people, and organizations not affiliated with any government, has occurred throughout human history but has recently become more prevalent.

2.1 The Current Situation

Over the past two decades, warfare has shifted from traditional warfare (i.e., wars of fire and maneuver) to asymmetric warfare (i.e., wars of insurgency) due to many factors, including, but not limited to, terrorist actions in the U.S. homeland and operations in Afghanistan and Iraq.

2.1.1 Traditional Warfare

This type of warfare is characterized by large force-on-force actions. Traditional armies face each other over an invisible line of control. In this situation, individuals are not as important as collectives, and leaders are well known or easily identifiable. Furthermore, there are definable start and end points of these conflicts. This type of conflict predominated until the collapse of the Soviet Union in 1991. While still important, traditional warfare is now less common than asymmetric warfare.

2.1.2 Rise of Terrorism

Individuals or groups of individuals rebelling against a large county have been known throughout human history. Over the past few decades, terrorism has been increasing. While there is no widely agreed definition of terrorism, terrorism commonly refers to violent acts by civilians intended to create fear (terror), are carried out based on ideological goals, and deliberately target or disregard the safety of noncombatants.

2.1.3 Asymmetric Warfare

During the 1990s, with the Intifada in Palestine, the rise of al Qaeda in Afghanistan, and the coalition operations in Afghanistan and Iraq, asymmetric warfare has become prevalent. Terrorist groups unable to directly confront traditional armies resort to covert operations. The leaders are typically in hiding, and the terrorists are dispersed. Defeating such a faceless, nameless enemy embedding itself within a peaceful civilian population is a major military problem that confronts the United States and its coalition partners.

Given the current situation, the United States has the need to find individuals who are hiding in civilian populations and remove them without causing collateral damage. In order to find these individuals, it is necessary to determine their intent—hence, the need for remote detection of covert, tactical adversarial intent of individuals. Since determining intent of adversaries is

extremely important to the DOD, the urgency to date has resulted in widespread adoption of ad hoc solutions. Discovering solutions that will work in a wide variety of situations and are based on sound scientific principles is greatly needed. This report attempts to shine light on this significant problem important to the DOD.

2.2 The Future

The concept "intent" is widely used in the signal processing literature for "a physical pattern that (in a layman's view) allows a conclusion of intent." However, the number of false positives and false negatives produced when intent is interpreted as "a physical pattern" is large. Physical states such as sweating are also poor indicators of intent. In this report, intent is a concept with cognitive content that does not need to coincide with the seemingly obvious physical patterns or states that are often connected by nonspecialists with intent. The step from fused physics-based information to a conclusion of cognitive intent is huge. In this process, physical patterns and states may not individually indicate intent. However, by proceeding from the physical patterns and states through a fusion process that will put "orthogonal" signals together based on cognitive principles, intent can be determined.

Humans who are intending to carry out preplanned violence have usually been coached and prepared in a manner not common to daily life. Historical data on World War II kamikaze pilots may be relevant to these considerations. Differentiable commonalities may exist in schooling and kinship. Just knowing one's task and fate can have consequences in biological motion, especially if the violence is technologically enabled (e.g., triggered bomb vest). There is evidence that observers watching video clips on closed-circuit television can reliably detect individuals carrying weapons by judging that these individuals appear to have higher levels of malaise and restlessness (Blechko et al., 2009).

This report focuses on remote detection of covert tactical adversarial intent of individuals in asymmetric operations. In future operations, this topic will, of course be embedded in a larger framework that will include use of information from databases, media, human sources, and other nonphysics-based sources, which can operate at long distances (greater than 50 m) and long time scales (hours, days, months). The lower arrow in figure 1, which is meant to be an analogy of the stages of defense from launch to landing of a missile, indicates the time scale for processing information. The apex is where the transition from intent to planned action occurs. After this point, the action will generally take place unless it is thwarted. The time scale gets shorter as one gets closer to the event. The "months-minute-second" arrow highlights that the time to successfully respond is progressively shorter.

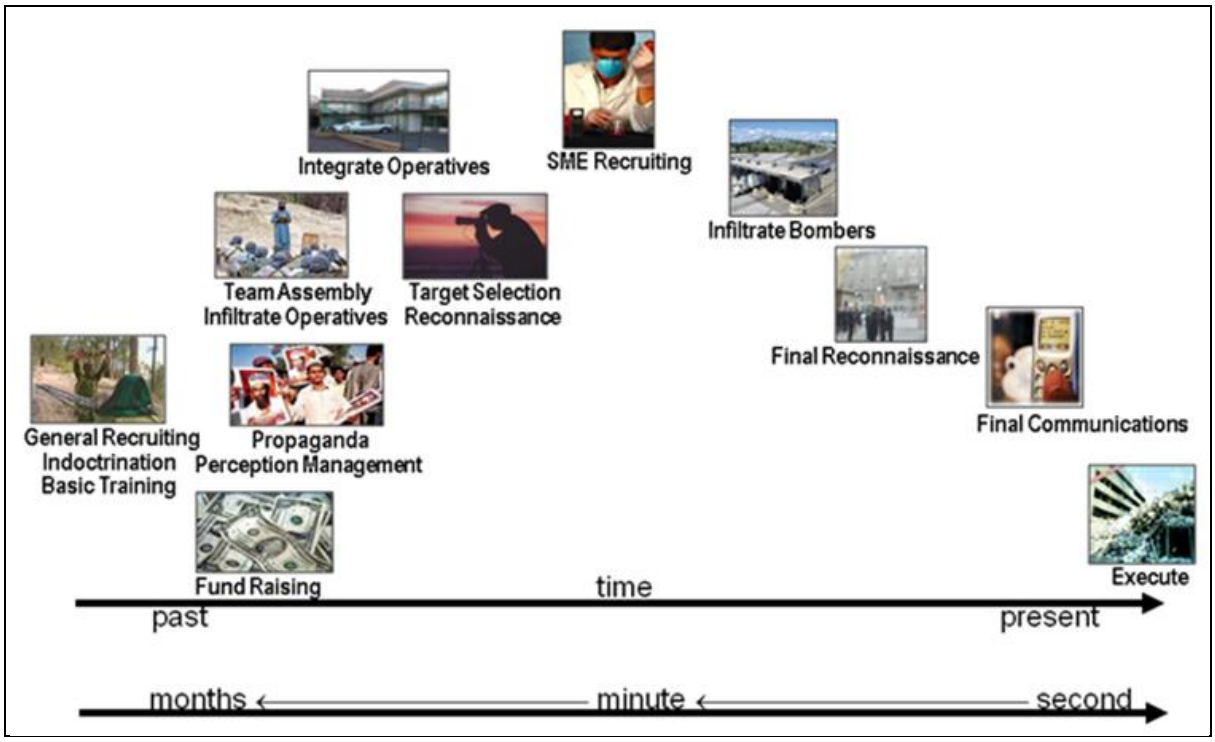

Figure 1. Processing times (lower arrow) for defense against adversarial asymmetric operations (represented by pictures and upper arrow).

There are many different approaches to understanding adversarial intent. They are organized by their relative time to the event as follows:

- Postevent: Persistent and pervasive sensing offers the ability to do detailed forensics of the events that led up to an event. This can be used to follow clues to determine where the adversaries came from and where they went and can also be useful for developing a deep understanding of the local components of an adversarial group.
- Imminent event: *This is the focus of the present report*. Thwarting an imminent event will most likely rely on very local information. Context or other indications that something is coming would help. However, this part focuses on and assumes that those indicators haven't come or are insufficient. In this case, local fusion is necessary to bring together, with sufficient time for prevention, the pieces of information that add up to a threat warning.
- Developing event: Most significant events do not take place without significant planning and preparation. Major components include fundraising, recruiting, indoctrination, training, team assembly, reconnaissance, infiltration, integration, recruiting of subject-matter experts, infiltration of materials, final reconnaissance, final communications, and execution. Each of these stages can be interrupted, but the timeline is progressively more compressed.

A wealth of potentially fruitful research directions is discussed in the next section. These directions indicate that it is fair to estimate that remote detection of adversarial intent is indeed feasible. Success, however, will depend on the details of how the already-existing building blocks plus new nonexistent building blocks can be put together to carry it out.

3. Research and Development (R&D) Directions

In this section, we estimate potentially fruitful R&D directions for remote detection of covert tactical adversarial intent of individuals in asymmetric operations. The objective here is to describe R&D directions that will eventually bridge the gap between physical phenomena and cognitive intent using principles, known or hypothesized, that provide a scientifically based (rather than a layman's experience-based) bridge from physical phenomena to the cognitive issue.

3.1 Cognitive/Perceptual Phenomena

In research on sensing adversarial intent, a basic assumption is that every brain action or state has a corresponding effect or state, however diminutive or hidden, in the body and that the effect or state in the body is amenable to some sort of sensing, even if not remote. What is sought is twofold: (1) an anomalous individual – a person who should not be in that place at that time and (2) a person acutely intending local violence after having planned and rehearsed the action. The first, considered for physics-based sensing, is a signal/noise problem. The second, a cognitive issue, implies a difference between "hot" anger (acutely triggered rage) and "cold" anger (similar to vengeance motivation), both of which can be physiologically differentiated from normal cognitive states. Can this be related to "state" vs. "trait" consideration in psychological profiling? One should note that superficial "profiling" seems to fail. The Transportation Security Agency (TSA) has noted that random screening produces more valid "hits" than superficial profiling. However, this experience may not be applicable without caveats to combat or quasi-combat situations. Can cognitive state be quantified in order to be related to detectable signals, or is this even needed? Is physiological state enough to determine that a person is "anomalous" and has an adversarial "plan"?

Specific questions to be answered include the following: What are the effects of people who are actually innocent bystanders but have knowledge that can potentially jeopardize them and their family? Can research be done on bystanders? What are the cues that a bystander gives off if he or she knows something about a plan? Are these cues detected by "expert human detectors"? Can these cues be automatically detected by sensors?

Exploration of enemy tactics, techniques, and procedures (TTPs), which often predictably vary relative to weather conditions, as contextual factors for determining intent should be considered. Most individuals intending to do harm have gone through at least some type of training and

practice. There is often a need to actively induce or ramp-up a response from individuals so that it can be sensed. By actively inducing a response, the flow of a plan will be altered and perhaps more easily observable. Those who have a plan may be affected more by even normal delays than others. The TSA Screening Passengers by Observation Technique (SPOT) program has noted that people with a plan can get increasingly angry with delays, whereas others may just have ordinary annoyance but not anger.

It is impossible to have a thought without some physical manifestation of the thought. Detecting such a manifestation may present a challenge when actively suppressed. It is in these instances that perturbing the individual's decision process may be effective for revealing covert adversarial planning. It may be worthwhile to explore the introduction of cognitive "speed bumps" (perturbations) into the decision process for individuals of interest, where real-time analysis of behavioral or physiological reactions is oriented toward a decision either to break contact and move on to checking other individuals or to retain contact and press further (i.e., take action with the present individual). "Active elicitation" of information may be a fruitful research area. Active elicitation processes should be minimally intrusive so that they are not easily detected as probing countermeasures by the subject of interest. The cognitive load of such an individual is likely to be at some times greater and at other times less than that of a normal individual—greater if they are attempting to appear "normal" and the planned event is still some time in the future, less if the event is imminent.

After the beginning of a stimulus, physiological cues in some/many processes can peak in 5–10 s. The human body tends to have many nonspecific responses (i.e., physiological responses that are part of the homeostatic or other internal state of the body unrelated to external cognitive stimuli). In order to understand which physiological cues relate to which stimulus, it is necessary to know the timing of the stimulus. Can a person's cognitive load be probed in time? If so, these probes need to be both culturally appropriate and relatively inconspicuous. How and when can previously rehearsed patterns be perturbed? It will be important to develop good stimuli for evoking a response that might be an idealized, adversarial intent, cognitive state, emotion, or arousal level. There may be differences due to different situations. Those carrying bomb vests implying self-immolation can have a different cognitive set (with associated biomarkers) than those controlling remotely triggered explosive devices. Research about how one actively (and unobtrusively) controls the situation so that threat indicators are likely to be expressed and thereby achieves subject engagement and behavioral authenticity is needed. Given the enormity of the topic and its currently amorphous state, perhaps an iterative approach to experimentation, in which scenarios are initially kept relatively simplistic and then experimental complexity is increased as knowledge is gained, is best.

Research on states of mind related to the timing of the event can be beneficial. For example, if an act and the associated verbiage to use if interrogated have been well rehearsed, then there might still be some variability in responses up until very close to the act. At that point, there could be a reduction in normal physiological responsiveness but more of a response to an

unexpected event delaying the plan. Research related to planning and disruption of plans might be helpful to distinguish the effect of the type of plan on the response to disruption or delay.

Much of what may have to be done, without the benefit of an interview/interrogation, is to induce a response. This response may be cognitive or behavioral and will be biased by cultural constructs. Stimulus-response, operational design in a complete theoretical framework is likely to be advantageous. However, the likely difficulty in constructing a suitable theoretical framework suggests that beginning with an empirical and observational approach may be advisable.

The physiological state of the observer should be considered as well as that of the target individual, specifically with respect to sleep deprivation, dehydration, and associated cognitive decrements such as decreased attention and hallucination. A related research direction could explore the impact of stimulant use (e.g., caffeine delivered via energy drink consumption), which is widespread among Soldiers. If a physics-based sensor system is created that focuses on the Soldier who is doing "human-based" sensing, it can act as an amplifier of perhaps ignored hunches and take advantage of the experience just cited.

Biomarkers can mark internal or external events. Animals can sense internal human states (e.g., fear). They are sensing (perhaps smelling) a characteristic of a person's state. People who have been around explosives may have explosives on their skin or clothes and can ingest them in some way into their bodies and may then emit them as biomarkers for very sensitive chemical signature detection.

Differentiation needs to be made between psychological issues (ideologues, disaffected, etc.) and psychopathological issues (not sociopathic or psychopathic). Clinical data may not be applicable as physiological indicators. For example, sociopaths may be emotionally numb. Further, there could be possible links to religious fanaticism and the associated training involved (Alamut, The Secret Doctrines of the Assassins, 1998). Can we identify the different types of terrorist psychologies? Are there significant differences between the person who totally believes he or she is carrying out an important duty vs. the person who has been forced into compliance with the plan through threats and intimidation?

Another important and often overlooked concept is measuring the problem. Metrics for cognitive phenomena and for how well detection systems work are needed. It helps to know what problem we are really trying to solve and define how well the processes are working. So often, current practices assume a certain level of competence; however, there are currently no good metrics in place to assess the effectiveness of current practices. It is important that these be developed. More than likely, most operational processes are working worse than assumed. What is the deterrence effect? The metrics themselves may be computationally intensive but should run seamlessly in the background, invisible to the user. Results should be easily interpretable and not lend themselves to a "so what" response by the user. Often, new metrics are developed in conjunction with user communities, which usually ensures that such metrics are

practically useful. In addition to being practically useful, however, the metrics need to be computationally feasible (not combinatorially expensive) and mathematically justified. In cases where the computational cost of the desired metric(s) is too large, approximate ersatz metrics need to be developed. Whatever metrics or ersatz metrics are proposed should be justified not based on traditional use of the metrics in other areas, successful as that may be, but rather on the basis of human goals in the remote detection of covert tactical adversarial intent. In the past, metrics based on information theory have been recommended for use in the fusion process. However, these metrics are designed for nonbiological physical processes. Evidence that they are applicable to the physiological, psychological, and cognitive processes of interest here is not available.

Good metrics to determine behavioral authenticity in experimental scenarios do not currently exist. This should be a focus for efforts in this domain. At the 6.1 level, the theory needs to be the driver in developing valid metrics of intent detection. Associated research questions include the following: What is the relation between emotion and adversarial intent? What are the emotions that a person would be experiencing as he/she goes through the plan from planning to execution? What are the effects of seeing an authority figure while carrying out the plan? What are the effects of changes in planned timing? Statistical interpretation of results will need to address the operational world (rather than the academic world). Group differences and associated parametric statistics often used in the academic world are only rarely useful in the operational world where we need to know how to react to an individual's behavior.

One major issue is the development of data sets. Can "method acting" (or any other school of acting) provide sufficient verisimilitude on all scales, including emotive/biochemical (sweat, breath, body habitus, kinesiology), to permit its use as a surrogate for "real" data. If so, the creation of data sets, while still expensive, will be less expensive. One methodology for developing valid empirical data sets is to design experimental scenarios so that behaviors of interest (e.g., facial expressions, specific human kinematics) are highly likely to be expressed. These behaviors of interest, while seemingly artificial within the framework of a contrived scenario, may be close to the behaviors in "real" scenarios. If enacted experiments cannot provide data that matches data of "real" situations, the expense and uncertainty will be larger. It is often expensive and difficult to get large amounts of data on "real" situations. The ground truth, i.e., the true intent of the subject, is often difficult to determine because of deception or disappearance of the subject. One notable exception is the vast store of video footage within the defense community depicting actual battlefield hostility, often including the behavioral precursors to a hostile event. The clear validity of such data is at least partially offset, however, by issues related to data format variability, resolution, and classification. Also, the sheer volume of these data sets, which often do not include sufficient event tagging or categorical organization, makes them less tractable for scientists attempting to exploit the content for empirical use.

The virtual reality community has a well-established database for determining participant engagement. This should be explored for its applicability to the current effort. The applicability

of virtual reality research to adversarial intent detection should be explored. Again, a primary concern is authenticity of the data gathered when the input is simulated. Time commitment does not seem to be a factor for subjective engagement levels. Good engagement can apparently be achieved over a few hours. Data from the virtual reality immersion literature is, however, mainly in the realm of psychological treatment (e.g., phobias) and may be contaminated from being in a patient population. An alternative might be to examine the principles of immersive game system design.

Automatic detection of adversarial intent can benefit from using methods that human experts use, including, but not limited to, criminological strategies of presenting photos of a crime scene, presenting mug shot albums, exposing subject to news clips or headline news, filling out surveys or forms, and delaying forward movement. There is, however, an open question about whether such expertise is transferable without extensive personal immersion within a conflict environment. Also, whether these can be adapted for the desired scenario (3–50-m distance) will need to be examined. Finally, without clear metrics for how experts detect intent, there is no theoretical basis for transferring such expertise.

The difficulty in obtaining ground truth for adversarial intent detection is an issue. The occurrence of adversarial intent, less than 1/1000, is also an issue. This fact makes a nonnormative approach to statistics important. Each individual may have unique responses relevant to his or her adversarial intent. Since we don't know what a "real bad guy" with adversarial intent may be like, perhaps we need to know in exquisite depth what a good guy looks like. Are there special populations that can be ethically tapped to provide appropriate cognitive or psychological constructs, i.e., can incentives provide the amount of "buy-in" needed for a valid proxy of a "bad guy"? These issues in basic research attempting to quantify the cognitive mechanisms that underlie threat detection skill are a primary concern. Are results valid when the actions observed are conducted by individuals who aren't actually hostile in the course of their normal existence? It should be noted that, among actual attackers, many are not actually hostile in the course of their normal existence and have varied motivations for conducting attacks.

3.2 Sensing

Individuals with adversarial intent will experience physiological changes and possibly display altered motions and behaviors that may be detected. In this section, we discuss physics-based sensors that may be able to remotely detect indicators for subsequent fusion to determine intent. Physics-based sensors will provide the input for a cognitive approach to sensing adversarial intent and offer the advantage of a quantitative assessment.

Sensing will require utilizing as many different measureable indicators of intent as possible and, thus, integration of multiple sensor modalities. The indicators relevant to adversarial intent must still be experimentally identified, underscoring the importance of developing experimental and simulated systems that reliably reflect intent. Sensing of indicators of intent will require data

collection on time scales of seconds to minutes. The fusion of this data from many sensors could enable monitoring of an individual over several hours, reinforcing the determination of intent. Moreover, indications of intent will ideally be sensed using passive observation as well as active perturbation of the individual. Determining the most effective means of active perturbation is an area needing exploration.

Efforts in this area should encompass fundamental research as well as application of sensing systems in testable environments, i.e., basic research ("6.1 research"), applied research ("6.2"), and advanced development ("6.3"). R&D may include the discovery and development of novel sensing capabilities for identifying indicators of adversarial intent within relevant experimental and simulated environments and detecting these identified indicators in relevant field situations. Individual sensors will need to be integrated into comprehensive systems to increase the overall sensitivity of the measurements, and sensor systems will need to be tested with increasingly larger sample sizes. It is anticipated that many of these sensors will flag significant numbers of false positives and false negatives. However, even though the measured parameters may individually have unacceptable error rates, they may still significantly improve the value of the system as a whole. It is important not to prematurely discard sensing technologies merely because false positives or false negatives will be generated.

3.2.1 Detectable Indicators of Adversarial Intent

The goal is to identify measureable physiological, biochemical, genetic, or other types of indicators that are correlated with an underlying elevated level of stress; a determination to carry out a plan with adversarial consequences as well as other less temporal predictors of violent activity including, but not limited to, social disconnectedness; and an embracing or acceptance of violence and death. Psychological, physiological, genetic, and biochemical factors that can correlate with social disconnectivity and a willingness to commit violence include aggression, impulsivity, autism, post-traumatic stress disorder (PTSD), unattractiveness, chromosomal copy number variants, and mutations in specific genes.

The first level of defense is to determine whether or not people are present. Technologies have been developed to detect the presence of human skin, heat from living organisms, etc. Once the presence of humans has been identified, analysis needs to move onto a deeper level to identify adversarial intent. Informative biological parameters that can be measured include the following:

- Posture
- Posture rigidity
- Heartbeat waveform
- Heart rate
- Breath rate, volume approximation, patterns, anomalies

- Wheezing, coughing, gasping
- Blood pressure trends: waveform shape and transit time
- Pulse-wave velocity giving a beat-by-beat approximation of blood pressure
- Movement: fidgeting, remaining still, shaking, shivering, having spasms
- Body stiffness, muscle tension, resonant frequency of body movement
- Voice stress analysis and voice onset timing
- Gastrointestinal distress, bowel sounds
- Reluctance to engage socially: distance from others, response to attempts to engage verbally
- Observation tendencies of subject, eye-glancing, head turning, situational awareness
- People whose actions are coordinated or who are actively avoiding each other
- Exposure to bomb-making materials/chemicals
- Hyperthermia from stress (generally expressed in the face, palms of the hands, and soles of the feet)
- Gait as indicators of stiffness (stress) or carrying a load or wearing protective clothing
- Breath biochemistry
- Microbiological organisms on skin or clothing

Attention should also be given to screening people in vehicles. Some potential informative and measureable signals include the following:

- Body and movement rigidity/stiffness as a measure of stress, probably more informative if measured in response to unexpected perturbation such as a unusual speed bump, unexpected timing of red light, provocative noise, or other stressor.
- Acoustic signals: If one can hear what is being said or happening in the vehicle, are the occupants making small talk, silent, listening to the radio, or praying?
- Lip and facial movements: Are the occupants talking, praying, silent, listening to the radio, or listening for outside cues?

3.2.2 Sensors of Detectable Indicators of Adversarial Intent

Body-contacting sensors that assess human physiology, such as those used for polygraphy, biometric identification, and medical diagnosis, are common. However, using these sensors at

stand-off distances presents both physics-based and operational hurdles. Many of the current sensors cannot operate at even modest distances (1 m) away from human bodies. Ongoing R&D is dramatically increasing sensor sensitivity, bandwidth, field of regard, and many other characteristics but still may not be able to overcome many of the technical barriers associated with remote intent assessment. Many of the sensors mentioned in this section may not be ready for immediate application but may offer significant benefits if sensor system maturity advances quickly.

We attempt to highlight sensing technologies that we believe can measure useful data for assessing adversarial intent. Passive and active sensors can be used to remotely characterize a human's physical features, clothing and equipment, and his or her interaction with the immediate surrounding environment. Passive sensors do not emit a signal and rely on a target's emission in some sensing domain. Active sensors emit a signal that interacts with the target in a known manner to produce a return that is quantifiable and related to the stimulus. Hybrid systems may use an active signal to produce a response observable in one or more domains. Sensor fusion can combine multiple inputs and domains to enhance features and remove noise or interferers. Redundancy of diverse sensor modalities will help corroborate physiological parameters in noise as well as alternative inputs for fusion algorithms. Some potential sensor domains and expected contributions are as follows:

- Imagers, in general: Imagers with related image-processing hardware and software can assess shape and contrast and change in single images and multiple frames. Change detection algorithms detect, track, and/or assess movements and establish "normal" traits, gait, movement tracking, surveillance activity, facial expression, emotion, phenotypic patterns, and body language. Imagers provide data for extracting behaviors and interactions among people in the field of view through pattern recognition. All of these capabilities can be implemented using thermal, hyperspectral, visible, and narrowband imagery.
- Thermal imagers: Passive thermal imagery can monitor overall surface temperature patterns, radiometric levels, facial thermal patterns, capillary dilation effects, bombs/weapons, clothing thickness, and specific body features.
- Hyperspectral imagers: Passive multiband imagers are optimized to select specific wavelengths of interest related to particular optical phenomena or material. Narrowband imagery can focus on sweat, subsurface blood flow, and particular types of clothing or equipment.
- Visible bandwidth imagers: These imagers establish "normal" visible appearance, identifiable traits for biometric ID, facial expressions, skin-tone changes, phenotypic patterns, and body language.

- Laser Doppler vibrometry: Active laser interrogation of skin or body surfaces reveals vibrational cues related to heartbeats, breaths, body resonances, muscle stiffness, voice, and voice stress.
- E-Field: Passive free-space electrodes (capacitively coupled) can detect electrical activity of the heart, brain, muscles, and hidden electronic devices.
- Radar: Active radar can detect and track human gait, heartbeats, breaths, radar cross section (RCS), and arm/leg movements.
- Ladar: Active laser radar produces three-dimensional (3-D) imagery related to "hostile" stance, 3-D posture, gait dynamics, facial recognition, carrying of backpacks, and unnatural frame proportions.
- Gas chromatography: Active collection of exhaled gas, such as through a suction tube near a microphone or portal, can provide a sample for trace gas analysis, chemical emission, odor, genetic material, and biochemistry assessment.
- Genetics of prokaryotic microorganisms: Genetic mutation of prokaryotic microorganisms on or in humans is environmentally influenced. DNA mutates in prokaryotes at a rate of approximately 1 in 300 nucleotides per generation; generations can be as short as 10 min. If the mutation patterns were untangled, the resulting information could reveal where the organism has been and what it has been exposed to. Mutation and mutation rates of prokaryotic organisms on or in humans might thus help determine where humans have recently been, what they have been eating, whether they have had unusual exposures to man-made or other toxins or mutagens and, in general, whether the patterns in their microorganisms' DNA is consistent with their purported history, identity, and activities. In addition, the relative fitness of different species of prokaryotes depends on the environment; the environment of prokaryotes growing in or on humans is influenced by that human's activity. The relative abundance of different species of prokaryotes on humans is also reflective of that human's environment and could be exploited to reveal information about that person's activities.
- Chemical sensors: Laser-induced fluorescence, i.e., active laser illumination with passive response monitoring (either fluorescent imaging or nonimaging amplitude of a particular wavelength), can be used to inspect a portion of the body for sweat or other compounds (salivary amylase or cortisol in the mouth or in the breath). Laser-induced fluorescence, laser-induced breakdown spectroscopy, and Raman spectroscopy can be used to inspect body and clothing for traces of explosive chemicals.
- Photoacoustics: Active laser stimulation of a test area and acoustic analysis of induced resonance can give indications of trace gas from the mouth, biological markers, and chemical residue on skin.

- Retroreflection: Active laser illumination and passive imaging of the collimated returns can be used for detecting optics/video cameras used by a target and can also detect naked eyes in close proximity for staring or eye tracking.
- Seismic: Passive sensing of ground or floor vibrations can be used to assess gait anomalies from concealed objects and weight anomalies for motion tracking. Active stimulation can induce movement of hidden objects.
- Magnetics: Passive magnetic sensing can detect hidden objects that might indicate intent, such as a pistol, knife, or explosive initiator component.

On a slightly higher level, one could measure the following:

- Physical evidence of psychological traits: Physical evidence of psychological traits of interest (PTSD, autism, antisocial behavior, embracing violence, indifference to human death, etc.) could be measured. One would have to develop an enabling database for phenotypic-to-psychological correlation.

These are just a few technologies that can potentially provide useful results. New sensors with enhanced capabilities as well as new data analysis techniques and information interpretation techniques are continually emerging.

All systems must undergo thorough evaluation to quantify efficacy. Since detection of intent by noncontact sensors is a new area, performance metrics have not yet been established. Individual sensor developers need to provide a full physics-based description of expected sensor capabilities as well as important parameters. Residual capabilities of a sensor may also have beneficial "artifacts" or add capabilities to other sensor modalities. The more diverse-modality information available, the better the fusion opportunities. The ability to individually update the algorithms for each sensor modality will accelerate the creation of new parameters or fusion results.

Signal processing methodology must provide a robust and automated ability to reduce high-bandwidth data to a few useful parameters and the ability to relate these measures to adversarial intent, stress, behavior, or other cognitive quantity. Obviously, robustness will also depend on each sensor's specific detection range, sensitivity, field of regard, dwell time, autonomy, and other characteristics.

Operational considerations include covertness of stand-off sensing, amount of clothing that might mask measureable parameters, interfering signals from motion artifacts, environmental considerations, ambient noise, speech, and the dynamic movement of the subject or sensor system. If a particular assessment of an individual requires a comparison with some preexisting "baseline," a plan needs to be established to access the baseline in the operational environments being discussed. An obvious objective is to process the data in real time to show states and changes in measured parameters. However, there may be a requirement to log raw data for post-processing for complex analysis of high-bandwidth imagery or multichannel fusion.

The scope of sensor system development for human intent prediction may range from initial proof of concept for novel sensing technologies to the evaluation and validation of sensing modalities for the new application of remote intent evaluation. Projects that involve the development of new remote sensing technologies should, at the very least, incorporate some element of validation using established "ground truth" sensors. For example, a novel sensor intended to evaluate heart rate at a distance should be validated with standard on-contact electrocardiogram (EKG) sensors to establish the accuracy of the system. This approach should also involve some consideration for potentially confounding factors.

Contact sensors may provide a level of measurement fidelity that permits a system to distinguish between an aggressive individual and someone who is merely distraught; however, the potential loss of sensitivity and incorporation of movement artifact with a novel remote sensor may obviate that distinction. Also, although it is not expected that a development project will involve validation with a complete human subject dataset, there should be some consideration of the sample size necessary for performance estimation. The sensor development approach should incorporate more than a demonstration of feasibility.

Mature sensor technologies originally developed for other applications will require testing and validation in this new setting. Testing should address elements of measurement paradigm (passive or stimulus/response), performance limitations and potential confounding factors, possibility of fusion with additional sensing modalities, and substantive testing with a dataset of human subjects for performance evaluation. One should identify and quantify sensor limitations related to environmental conditions such as ambient temperature, daytime vs. nighttime, visibility conditions (fog/rain vs. clear), and requirements related to sensor positioning and regarded field. The validation of remote sensors should also include fusion with alternate sensing modalities.

3.3 Information Fusion

Information fusion is a process that correlates, combines, modifies, and enhances the interpretation of a set of information from a state of lower generalization to one of higher generalization. The fusion process starts from data from sensors or sources. There are many existing sensing modalities and associated signal processing techniques that have matured over the years and that can extract target features for detection, classification (human, vehicle, animal), identification (e.g., man, woman vs. child; car vs. truck; dog vs. horse), recognition (e.g., John vs. Richard; Toyota vs. Honda), localization (x, y, and z) and tracking (as a function of time). Each sensing modality may be individually robust, but no one sensor can accurately produce the information needed to defeat the current asymmetric threat. Imaging sensors are needed for confirming the presence of a target and (by human judgment of the images) the intent of the target. However, remote and unattended imagers have a limited field of view, consume a lot of power, and are hard to camouflage and expensive (especially in night operation). Their performance is susceptible to weather changes. Acoustic sensors are passive, inexpensive,

provide accurate bearing, have a 360° field of view and non-line-of-sight capabilities but are susceptible to wind. Their detection range varies widely with diurnal and weather changes, and their performance degrades rapidly in the presence of multiple targets. Although radars provide accurate range, good target classification, and multiple target detection and tracking capabilities, they are active, have limited field of view, and consume a lot of power when emplaced in a remote, unattended scenario. Other sensors such as magnetic (detection of metal content on a target), seismic (ground vibration), and passive infrared (IR) (motion detection) are affordable and used in today's unattended ground sensors configurations as triggers for the more power-consuming sensors such as imagers and radars. Due to the limitations of each sensing modality, fusion of the output of many sensors will be needed to enable accurate determination of the detected threat. However, there is a challenge in designing fusion processes that achieve the higher confidence and lower false alarm rate expected when the output of different sensors is combined.

Remote human detection with high classification and determination of intent over ranges up to 50 m is a challenging task. Once detection is made, extracting the intent to determine a pending threat is desirable. There are new sensing modalities and signal-processing techniques that are being researched to extract this information. Humans engaged in planning a threat carefully plan their mission, rehearse, and take every precautionary measure to hide and disguise their intention as a normal event. Passive measurement of observable physical items (gait, arm swings, and posture—carrying a heavy load might alter the way a human walks) or a vehicle (determining the weight it is carrying—abnormal RPMs) can be accomplished. In addition, one can introduce a stimulus that generates an element of surprise that alters the rehearsed plan of action. A human might, in response, conduct unrehearsed sudden irregular motion. Such behaviors may help differentiate threats from nonthreats.

If time permits, the sensors can monitor the pending threat and extract additional information over longer intervals. With networked sensors and fusion of information from all available sources, accuracy may increase. Robust communication networks and compression are key, with only small bites of information exchanged to continuously monitor and pass forward information to sensors that can anticipate the arrival of a threat for efficient processing (detection, recognition, and tracking).

The Joint Directors of Laboratories (JDL) Data Fusion Model is the most widely used method for categorizing data-fusion-related functions (Steinberg et al., 1998, 1999). The data fusion process involves combining information—in the broadest sense—to estimate or predict the state of some aspect of the universe. These processes may be represented in attributive and relational states. It can be useful to include consideration of *informational* and *perceptual* states in addition to the *physical* state that was the main focus of the original JDL model. The JDL model is composed of levels of abstraction, with level 0 being the lowest or minimally processed information level and levels 1–4 having increasing levels of abstraction. Typically, hard information (information from physical sensors) is operated on at levels 0 and 1. Soft

information (information from human-based sources and/or related to human decision making) can be at any level. The JDL data fusion model was the first fusion model to capture the multiple levels-of-abstraction character of the situation-understanding process. Although there are many criticisms of the JDL model and many competing models, the JDL model has, in general, withstood the test of time. Most of the fusion community has accepted the JDL fusion levels. There are frameworks that extend and more practically functionalize the JDL fusion model. An example is the Contextual Fusion Model (Antony and Karakowski, 2008, 2009), which includes context and handles input derived from hard and soft sensors in addition to producing a more specific functionalization of the desired fusion process for implementation.

There is a question about whether and to what extent classical probability theory (typically, Bayesian theory) is meaningful for fusion processes involving cognitive phenomena. There is wide agreement that information from physical sensors can be assessed and fused using classical probability measures. When cognitive phenomena are considered, however, other representations of uncertainty, ones less dependent on statistical assumptions and more able to handle data of varying types and sparse data, may be needed. Consider the information processing at the cognitive level as a system of subsystems (i.e., local processing in physical devices, information fusion in the network, etc.). Uncertainty is propagated upwards. Uncertainty may be in the form of the pedigree of information, degraded sensing, digital communications degradation/collisions, etc. As these uncertainties are propagated upwards, the performance of the higher-level system is adversely affected. It is possible that the higher-level uncertainties will not be described appropriately by probabilities (which may have been inappropriately "summed" in prior efforts). There are many alternatives to classical probabilistic (often Bayesian) methods. Dezert-Smarandache Theory (DSmT) has had success in robotics. Dempster-Shafer Theory has been applied in many areas and has been useful for "real-life" problems. The Transferable-Belief Model (TBM) has been successfully used in marketing, and Analysis of Competing Hypotheses (ACH) has been used in human intelligence. All of these methods have had success in additional areas. Possibility theory is also a candidate for assessment of propagated uncertainties. Bossé et al. (2007) discuss various methods for representing uncertainty in fusion processes.

It is known that in some cases, humans can sense context very rapidly. This often requires experience within the local context as well as an openness to hunches. The process may work in a fractal fashion, with sensory and memory inputs ranging across a large set of scales (e.g., local smells, ambient noise, arrangement and density of visual detail at many scales, and building arrangements). It can also include dynamic human traffic flow fields, which invoke other humans as sensing elements around anomalous individuals or items. Complicating this issue are cultural components and sensitivity, which form strong structural elements of the cognitive landscape and include social interaction norms. Individuals who display these talents may have traits linked to those displayed by ADHD (attention deficit hyperactivity disorder)-type individuals (New Hope Media LLC, 2010; About.com, 2010).

Obvious adversarial action at the tactical level may take place over short time periods on about 3 s or less. However, remote detection of covert intent need not and preferably should not occur mainly at this time scale. Indicators of adversarial intent can be gathered over longer time intervals using human intelligence and social network analysis. These indicators are typically seen best by trained Soldiers and intelligence experts. Much bang for the buck may be gained by understanding how the Soldier-user observes and reacts. How do we train? How are quick decisions made? What makes an expert? What are best practices?

The emphasis here has been on the fusion of hard information from physics-based sensors because such fusion is currently not yet feasible and designing it is a huge task in itself. In future operations, all-source fusion ("hard/soft fusion"), where the input comes from all available sources (physical sensors, informational resources, human reports, etc.), will certainly be required.

Assessing one person by another is actually the analysis of information associated with people and their actions and surroundings. The analysis of a person's "intent" is problematic because some individuals may be performing deeds without full knowledge of their intent or actions; others may be highly engaged in their belief systems; and finally, individuals may be acting with limited knowledge of the full scale of the results of their actions. So, it appears that rather than determining intent, it may be better to assess whether someone's planned actions (thoughts) resulting in an outcome that should be acted upon is counter to our mission goals and objectives. Accordingly, from a cognitive science point of view, knowledge of the plan and overt indicators of the plan should be a main focus for detection. Intent is not always something that is attributable to the individual at the end stage of an attack plan (e.g., "bait" children locked in a hot car and a scenario designed to attract sympathetic Soldiers as triggers for a vehicle-borne improvised explosive device [VBIED]). The scenario itself may be the critical element, and the individuals that initiate an attack may exhibit no overt indicators of hostility if they are not in the loop. To reiterate, it may be necessary to explicitly address the separation of intent vs. plan to deal with bait individuals who may have no intent but are elements of a detectable plan. The cognitive issues may be better focused by considering the difference between individuals with or without situations reflecting a plan vs. individuals with or without intent. Detecting anomalous situations, per se, may be beyond the scope of this document, although it forms a context for detecting "intent."

The concept of adversarial intent needs to be well defined. The covert tactical adversarial intent is not just a generalized "I hate the American soldiers." Certainly, we cannot detain people until they decide to agree with us or like us. It will be important to always put cultural context into interpretation of results. All research should be aware of the cultural context in which behavioral responses can be properly interpreted. Contextually (at the very least), a sociocultural and anthropological framework for detecting intent must be well understood for the research in this domain to have any degree of efficacy. It would be appropriate to conduct cultural

anthropological studies to create the proper context. Most importantly, one must define what is "normal" for a particular operational environment.

Consideration of the local population as an indirect sensor (e.g., when normally populated areas become sparsely populated without explanation and when normally friendly locals suddenly give Soldiers a clearly hostile stare) may be worthwhile. Using a population as an indirect sensor net works only when a priori knowledge exists and the population adjusts its behavior to what may be considered anomalous for a particular venue, neighborhood, or district. Otherwise, there is no implied action (other than self-preservation) for that population. If the population detects an imminent threat soon, that places the population in essentially the same position that the Soldier is in—a naïve (relative to a hostile plan) observer who may detect such a change and, in turn, indirectly detect an imminent event even though detailed information about a perpetrator or detonation location is not evident. It should be noted that a critical difference between the population and the Soldier observer is that the Soldier is primed to act. This arguably makes the Soldier a better "sensor" if one subscribes to the proposition that environmental cues can lead to action and that without the potential for action, perception is degraded. A consequence may be that the detection of and behavioral response to someone "who does not belong here" can be partially triggered by the difference in observable biomarkers (personal smell, gait, facial expression, dress, self-isolation/reticence) and highlight the need to consider the context for any such detection system or approach.

V. S. Subramahnian and his colleagues at the University of Maryland have produced a portal called SOMA (Subramahnian, 2010) that catalogues information about terrors groups in the Middle East. In particular, Subrahmanian and his colleagues have been able to derive patterns and rules underlying the operation of these groups by analyzing news blogs, AP wire reports, and other online information. Having access to such information would greatly help the fusion process. Based on contextual information, it could help the group manning a checkpoint to change the normal flow of people or vehicles queuing up at a checkpoint to thwart a terrorist. A proactive approach of dealing with the enemy entails playing a cat-and-mouse game with an unknown, or only partially known, enemy. Furthermore, the unknown enemy has a chance to observe how a checkpoint is managed without being noticed. Recent events, such as the use of a U.S. citizen for surveillance of the sites in Mumbai (including the Jewish Center) for a later terrorist attack, clearly point to an enemy that adapts to any adopted security procedure. The availability of software agents or tools that make contextual information available during the fusion process would enhance the research.

3.4 System Design, Testing, and Execution

Developing and evaluating sensor systems for remote characterization of human intent should incorporate considerations of operational execution. Although the expectation is that an intent recognition system could be employed in a variety of operational settings, the problem can be simplified to address two measurement paradigms. First, a system may be employed in a passive

manner so humans are merely observed and their intent is inferred from their current state. As an example, if a subject is approaching a checkpoint, it may be feasible to employ sensors to estimate that individual's physiological state, the physics of their motion, or even the types of materials on their person. This type of system implementation involves no interaction with the person of interest. Along with passive observation and evaluation, there may be planned perturbation of either the human or the environment to elicit a stimulus/response effect that may amplify the relevant intent metrics. Perturbations can involve a variety of physical and psychological stimuli. One example of a physical perturbation might be the placement of an obstacle for which a subject must modify his or her walking path. Such a perturbation might augment changes in motion due to hidden loads or cognitive stress. Psychological stimuli could be used to evoke a physical response or change in behavior that might amplify indicators of human intent. Examples of this are a television screen with the subject's image on it to let them know that they are being watched or some modification to a checkpoint procedure to affect someone's plans. The objective of these and other stimuli is to disrupt the plans of potential human threats and elicit an observable response. Whether the ultimate implementation of a system is projected for a passive manner or in a stimulus/response application, this element of a system's execution should be addressed in the development and validation process.

Many different kinds of hierarchical architectures for information processing may be considered. All of these networks will most likely be semiautonomous at the lowest levels near the devices and cooperative at higher levels. As one proceeds up the hierarchy, the information should increase in quality, i.e., have an increasing detection rate and a decreasing false alarm rate. The hierarchies should exploit redundancy among the devices.

It is not expected that any one sensor will provide the complete solution but instead a combination of sensors and sensor metrics will be required for remote intent prediction. The performance of a given system should be validated with a human subject dataset sufficiently large enough to address issues related to a subject's variability and confounding factors. For example, if we consider the possibility of estimating intent from human physiology, it is possible that a person with no malicious intent will present physiological indicators that overlap with a malicious subject. Also, it is possible that alternative emotional states (e.g., fear and sadness) may produce physiological responses that mirror aggression or malicious intent. A large set of human subjects and experimental conditions should help sort out these factors.

4. Coordination

The infrastructure for R&D for remote detection of adversarial intent is already in place in academia, government laboratories, and industry. The way in which researchers and developers in various disciplines and organizations collaborate to pursue larger goals will be a large factor in determining the rapidity with which R&D is accomplished. Research in this area involves

kinesiology, neurophysiology, psychology, cognitive science, sociocultural anthropology, and information science. Relevant areas include clinical psychology, cognitive neuroscience, communications, computer science, criminal science, decision science, developmental psychology, ethics, geography, human cognition, industrial organization psychology, linguistics and computational linguistics, perception psychology, physical and cultural anthropology, psychophysiological psychology, risk and risk management, social psychology, and sociology.

4.1 Balance Between Near-Term Development and Long-Term Research

Today, R&D must be achieved with budgets significantly smaller than those of 10 years ago. Devices and systems must be cheaper, more robust in performance, and higher in efficiency. It is a dual challenge to satisfy these requirements, which are often near and medium term, and, at the same time, position the research so that maximum long-term benefits can also be achieved. In any long-term research project, there is a multitude of near-term issues that impact the conduct of research. On occasion, these near-term issues may hinder progress toward long-term solutions. At other times, the near-term issues aid progress toward long-term solutions by drawing attention to unforeseen problems that, if recognized and investigated early, significantly shorten the path to the long-term goal. The options of focusing exclusively on long-term research without recognizing the importance of near-term issues and focusing only on near-term issues without cognizance of the need for long-term research are both less than optimal. The DOD's needs require that near-term benefits and long-term goals be balanced against each other.

The traditional technology transfer paradigm of scientists, engineers, and mathematicians making basic discoveries in their research and passing them on to development personnel for implementation is no longer the only or best option for R&D. Increasingly, researchers are being called upon to interact and collaborate with development personnel to reduce the time necessary to build operational systems. It is in a framework of two-way technical collaboration between basic researchers and development personnel that issues impacting the long-term development of a system can be identified earliest and solved most efficiently. A successful basic research program on remote detection of covert tactical adversarial intent of individuals in asymmetric operations will be a set of interdependent projects linked interactively with development programs. The urgency of the need strongly suggests that 6.2 applied research and 6.3 development need to begin before 6.1 basic research is complete. In addition, 6.1 basic research, which currently has very little access to "real data," can benefit from 6.2 and 6.3 efforts that will, on the way to developing specific systems, likely generate "real data" that can help guide the 6.1 research. Traditionally, basic research is carried out either by chance or because of a demonstrated need over a long period of time. There is currently a great need to carry out basic research and applied development hand-in-hand so that the entire problem is solved and the time taken to produce a deployable solution is shortened. The current situation of asymmetrical warfare demands that we get the basic theoretical framework right the first time.

4.2 Collaboration Among Government, Academia, and Industry

Currently, there are many efforts in and bordering on the areas discussed in section 3. These efforts are supported by many different agencies and coordinated through formal and informal meetings of investigators at working groups, conferences, and other events. Some of these efforts by DHS, ARL/HRED, ARL/ARO, NVESD, AFRL, NRL, AFOSR, and IARPA are mentioned in the Introduction. Given the current constraints on federal, academic, and industrial budgets, coordinating future efforts at a deep level and thereby ensuring quicker and greater payoff are given high priority. The DOD, DHS, IARPA, the entire Federal Government, state and local governments, academia, and industry all have considerable interest in remote detection of adversarial intent. Consistent with the approach mentioned in section 4.1, DOD's effort should contain 6.1, 6.2, and 6.3 components. Small, newly emerging companies often connected with academic research groups constitute one dynamic factor in this R&D. These companies should be supported through programs such as Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR). Three-way collaboration between government, academia, and industrial organizations should be maintained through these programs and other channels.

5. A Path to the Future

In this report, we have summarized the state of the art in remote detection of adversarial intent and have pointed out the need for coordinating R&D in many dimensions, including cognitive/perceptual phenomena, sensing and information fusion, near-term development, long-term research, and different types of organizations (government, academia, and industry). The scientific and administrative factors to support rapid progress in R&D of remote detection of adversarial intent are all in place.

5.1 Recommendations

Comprehensive DOD, DHS, IARPA, and Federal R&D programs are required to promote rapid progress. Specific recommendations are as follows:

- The Federal Government should fund R&D programs with the objective of producing a theoretically founded a prototype system for remote detection of covert tactical adversarial intent of individuals in asymmetric operations within 5 years and a working operational system within 10 years.
- The Federal Government should continue to provide broad support for academic and industrial efforts both in remote detection of adversarial intent and in areas (such as linkage of these systems with databases, media, and human input) that are useful for larger systems of systems.

- The strong interdisciplinary nature of remote detection of adversarial intent should be reflected in all efforts supported by the Federal Government.

5.2 Conclusion

To stop a missile from hitting its intended target, we need to track/influence the missile throughout its whole trajectory, starting as soon as it is fired. It is even better to prevent the missile from being produced in the first place. In much the same way, to stop terrorists before they reach a target, we should track them through the planning and rehearsal stages and discourage them from even entering these stages. Research about this is not the research described in this report, which handles the "end stage" of the adversarial intent phenomenon. However, it is important research at "the initiation" of the adversarial intent phenomenon. Such research on winning the hearts and minds of populations may work well in reducing the occurrence of adversarial intent (Atran, 2008a, 2008b). The reduction will, however, never be to zero, and the research described here will always be needed.

As the need for more comprehensive security in asymmetric situations grows, so does the need for prioritizing remote detection of adversarial intent. Uses of remote detection of adversarial intent in the civilian economy include crowd control, antidrug and anticrime operations, border security, and ensuring the security of government and private personnel and property. The many different directions of R&D in remote detection of adversarial intent are evidence of the richness of this field. While all of these directions are important and interesting in their own right, the task is now to coordinate and focus basic R&D efforts in areas that will quickly lead to creating a class of detection techniques with acceptable or better false-positive and false-negative rates. The bottom line in security 5–20 years from now will depend on the vigor with which this R&D is pursued today.

6. References

About.com. http://add.about.com/sitesearch.htm?terms=hyperfocus&SUName=add &TopNode =2852 &type=1,2010) (accessed 3 March 2010).

Alamut, The Secret Doctrines of the Assassins. http://www.alamut.com/subj/ideologies/alamut /secDoctrines.html (accessed 3 March 2010).

Antony, R. T.; Karakowski, J. A. First-Principle Approach to Functionally Decomposing the JDL Fusion Model: Emphasis on Soft Target Data. *Proceedings of the 11th International Conference on Information Fusion*, IEEE, 2008.

Antony, R. T.; Karakowski, J. A. Private note, 2009.

Atran, S. Who Becomes a Terrorist Today. *Perspectives on Terrorism* **2008a**, *2* (5).

Atran, S. The Making of a Terrorist: A Need for Understanding from the Field. Testimony before the House Appropriations Subcommittee on Homeland Security, Washington, DC, 12 March 2008b.

Blechko, A.; Darker, I. T.; Gale, A. G. The Role of Emotion Recognition from Non-Verbal Behaviour in Detection of Concealed Firearm Carrying. *Proc. Human Factors and Ergonomics Soc. 53rd Annual Meeting*, 2009; pp 1363–1367.

Bossé, E.; Roy, J.; Wark, S. *Concepts, Models, and Tools for Information Fusion*; ARTech House: Boston, 2007.

Ekman, P.; Friesen, W. *Facial Action Coding System: A Technique for the Measurement of Facial Movement*; Consulting Psychologists Press: Palo Alto, CA, 1978. (See also http://en.wikipedia.org/wiki/Facial_Action_Coding_System, accessed 3 March 2010.)

New Hope Media LLC. http://www.additudemag.com/additude /article/612.html,2007 (accessed 3 March 2010).

Steinberg, A. N.; Bowman, C. L.; White, F. E. Revisions to the JDL Model. *Joint NATO/IRIS Conference Proceedings*, Quebec, October 1998.

Steinberg, A. N.; Bowman, C. L.; White, F. E. *Sensor Fusion: Architectures, Algorithms, and Applications*. *Proceedings of the SPIE* **1999**, *3719*.

Subramahnian, V. S. SOMA Terror Organization Portal. http://www.umiacs.umd.edu /research/LCCD/projects/stop.jsp,2009 (accessed 3 March 2010).

INTENTIONALLY LEFT BLANK.

Appendix A. Workshop Participants

Gregory Arnold and Adam M. Fullenkamp
Human Effectiveness Directorate
U.S. Air Force Research Laboratory

Ann Bornstein
Computational and Information Sciences Directorate
U.S. Army Research Laboratory (ARL)

Troy Brown
Research Branch
Defense Academy for Credibility Assessment

Purush Iyer, John Lavery, Elmar Schmeisser, Stephanie McElhinny, and Mimi Strand
U.S. Army Research Office, ARL

Joseph Karakowski
I2WD
U.S. Army Communications and Electronics Command (CECOM)

Frank Morelli
Human Research and Engineering Directorate, ARL

Barbara L. O'Kane
Night Vision and Electronic Sensors Directorate, CECOM

Michael Scanlon and Nino Srour
Sensors and Electronic Devices Directorate, ARL

INTENTIONALLY LEFT BLANK.

Appendix B. Workshop Steering Committee Contact Information

Ann Bornstein
Computational and Information Sciences Directorate
U.S. Army Research Laboratory
Aberdeen Proving Ground, MD 21005
Tel: 410-278-8947 (DSN 298-8947)
annb@arl.army.mil

Thyagaraju Damarla
Sensors and Electron Devices Directorate
U.S. Army Research Laboratory
2800 Powder Mill Road
Adelphi, MD 20783-1197
Tel: 301-394-1266 (DSN 290-1266)
rdamarla@arl.army.mil

John Lavery
Mathematical Sciences Division
U.S. Army Research Office
U.S. Army Research Laboratory
P.O. Box 12211
Research Triangle Park, NC 27709-2211
Tel: 919-549-4253 (DSN 832-4253)
john.lavery2@us.army.mil

Frank Morelli
Human Research and Engineering Directorate
U.S. Army Research Laboratory
Aberdeen Proving Ground, MD 21005
Tel: 410-278-8824 (DSN 298-8824)
frank.morelli@us.army.mil

Elmar Schmeisser
Life Sciences Division
U.S. Army Research Office
U.S. Army Research Laboratory
P.O. Box 12211
Research Triangle Park, NC 27709-2211
Tel: 919-549-4318 (DSN 832-4318)
elmar.schmeisser@us.army.mil

NO. OF
COPIES ORGANIZATION

1 (PDF only) DEFENSE TECHNICAL INFORMATION CTR
DTIC OCA
8725 JOHN J KINGMAN RD
STE 0944
FORT BELVOIR VA 22060-6218

1 DIRECTOR
US ARMY RESEARCH LAB
IMNE ALC HRR
2800 POWDER MILL RD
ADELPHI MD 20783-1197

1 DIRECTOR
US ARMY RESEARCH LAB
RDRL CIM L
2800 POWDER MILL RD
ADELPHI MD 20783-1197

1 DIRECTOR
US ARMY RESEARCH LAB
RDRL CIM P
2800 POWDER MILL RD
ADELPHI MD 20783-1197

1 DIRECTOR
US ARMY RESEARCH LAB
RDRL D
2800 POWDER MILL RD
ADELPHI MD 20783-1197

ABERDEEN PROVING GROUND

1 DIR USARL
RDRL CIM G (BLDG 4600)

NO. OF
COPIES ORGANIZATION

ABERDEEN PROVING GROUND

1 DIRECTOR
US ARMY RESEARCH LAB
RDRL CII
B BROOME
2800 POWDER MILL RD
ADELPHI MD 20783-1197

9 DIR USARL
RDRL CII C
A BORNSTEIN (5 CPS)
E BOWMAN
T HANRATTY
M THOMAS
D WELSH

INTENTIONALLY LEFT BLANK.