

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

LIAR! LIAR! DECEPTION DETECTION IN 2035

by

Kevin L. Lockett, Chaplain, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Zoe M. Hale, Ph.D.

Maxwell Air Force Base, Alabama

April 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States government of the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Disclaimer	ii
Abstract	iv
Introduction.....	1
1969	1
1983	2
The Problem.....	2
The Question.....	6
The Method.....	7
Current State of the Art.....	9
2010	9
The Challenge	11
Looking to the Near Future.....	15
2020	15
Exploring Future Technologies and Processes	16
Thoughts from the Delphi.....	19
Hindrances	20
Looking to the Distant Future	22
Exploring Future Technologies and Processes	25
Thoughts from the Delphi.....	28
Conclusion	34
Notes	39
Bibliography	42

Abstract

Since the dawn of time, humans have quested to know the truth and to detect deception. Over the years technological breakthroughs have assisted that endeavor. This Blue Horizons paper looks at the current state of the art for deception detection, the polygraph, and briefly examines its history, function, strengths, and weaknesses. Then, utilizing environmental scanning, backcasting, and a conversational Delphi technique, it looks to the near and distant future to answer the question, “How can today’s best practices be combined with tomorrow’s promising technologies and discoveries to enhance the fields of investigation, human intelligence gathering (HUMINT), and deception detection for other purposes?” Through futurist case studies in the year 2020 and 2035, the paper looks to technologies such as brain fingerprinting, P300 scanning, thermal imaging of facial physiology, facial micro-expressions, and “Silent Talker.” In the end, research seems to point to technology as the enabler for the critical human element in criminal investigation and deception detection.

“Then you will know the truth, and the truth will set you free.”

~ Jesus of Nazareth

Introduction

1969

“Kevin LeRoy Lockett! Get back over here this minute!” There it was: *the tone*. When mom combined *the tone* with my full name, I knew nothing good could come from it. But I also knew the consequences of disobedience, so I hurried back to the front porch of our simple white frame home. Moments before, a gust of wind had blown over a potted plant on a flimsy plastic stand mom had placed on the porch some days before. My friends and I, playing in the front yard, felt the gust, heard the crash, saw the debris, and following our most base instinct, ran like criminals with the law in hot pursuit.

“Kevin LeRoy, why did you knock this plant over?”

“I didn’t, mom, it was the wind.” I knew she wouldn’t believe me, especially because she saw us running, but still I protested, “It wasn’t us, honest!”

“Look me in the eyes and tell me that.” Oh, no. There it was, mom’s never-fail, portable deception detector: *the eyes thing*. “You’re lying,” she would tell me, “I can see your eyes twinkling.” (Interestingly, years later, my sister’s twinkling eyes meant she was pregnant.) Mom’s *eyes thing* was very versatile and amazingly reliable. Somehow, she always knew when I was stretching the truth or telling an outright lie. (And with all three of my sister’s pregnancies, mom knew before Peggy Jo ever breathed a word of the good news.) But this time, I was telling the absolute truth. I was innocent, and mom’s *eyes thing* was obviously malfunctioning. I was doomed to take the fall and do hard time, grounded for a week for a crime I didn’t commit. There had to be a better way of getting at the truth!

1983

I spent three of my high school years working as a stock clerk for a major retailer. I loved my job and I was good at it. Mr. Schmidt, my general manager, liked me and, more importantly, he trusted me. He gave me a lot of interesting assignments beyond the standard stocking the end cap with sale merchandise, helping load a new television into a customer's too-small car, or crushing a pallet of boxes in the compactor we called "Jaws." He let me stay on when I moved away to college. I was able to work as many hours as I wanted when I came home for a weekend.

Then came the rash of thefts. Small stuff began to disappear in huge numbers. At first, security assumed it was roving shoplifters, but the other regional stores hadn't suffered any similar losses. Finally Mr. Schmidt and the management team decided it must come from company personnel. All employees, full or part-time, were given a polygraph test to determine if they had ever stolen merchandise from the store. Those who "failed" the polygraph were fired on the spot, or so I was told. I was away at school at the time. Mom warned me when I came home for the weekend I might have to take a test. She said my best friend from high school had been dismissed because he didn't pass the test. She didn't ask, but the implied question was there. Could I pass it? It was a good question. I knew I was innocent, but I flashed back to that windy day in 1969. I was innocent then too, but still convicted. There had to be a better way at getting at the truth!

The Problem

These are simple, somewhat humorous, accounts of the human quest for truth. One author observes, "Although people have been communicating with one another for tens of thousands of years, more than three decades of psychological research have found that most

individuals are abysmally poor lie detectors.”¹ Even most mental health specialists and criminal justice professionals, including customs officers, federal law enforcement officers, and police officers, demonstrate no better success at accurately detecting deception than laymen.² Generally, they perform no better than chance, largely because most people hold incorrect assumptions about behaviors associated with lying. For example, like my mother, most people believe liars always avert their gaze. According to Dr. Charles F. Bond, Jr., professor of psychology at Texas Christian University, this is the most prevalent stereotype about deception, and it simply is not true.³ Despite my mother’s belief to the contrary, to say nothing of childhood legends, neither twinkling eyes nor a growing nose nor even “pants on fire” indicate deception. Similar theories of determining deception have abounded across cultures and generations. The ancient Chinese believed liars had dry mouths and required suspects to chew rice powder and spit it out to determine their guilt or innocence.⁴ In India, curled toes betrayed a liar to judges.⁵ Until recently, Arabian Bedouins telling conflicting stories were both required to lick a glowing hot iron; the one whose tongue blistered was declared the liar.⁶ During the Inquisition, one suspected of bearing false witness was given a “trial slice” of bread and cheese to swallow; if it stuck or the suspect choked, guilt was assumed. A blush, an eye movement, a peculiar hand gesture – all have been interpreted to suggest one may be a teller of untruths.

These theories are based on the assumption that a measurable, physical reaction accompanies internal, hidden cognitive processes. As described by one of the inventors of the first polygraph device, such reactions are natural and irresistible responses within the human body when a conscious decision to deceive conflicts with the subliminal base instinct for truth. He writes, “When the conscious self deviates from the truth, and denies it, the subconscious self and the body demand to be adapted to reality, to be truthful. We come to the paradoxical

formulation that human beings lie with their consciousness, but are truthful with their unconscious, and when they do not confess with their mouths, then they confess with their body.”⁷

The inventors of the first polygraph machine sought to find a way to detect and measure these physical “confessions.” The two men behind the “Cardio-Pneumo Psychogram,” the first polygraph machine later known as the “breadboard polygraph” (because in order to make the unit more portable, its parts were each attached to a large breadboard), were both police detectives in Berkley, California, serving under Chief of Police August Vollmer, considered one of the nation’s earliest promoters of forensic sciences.⁸ One of those police officers, John Larson, was a medical student and the nation’s first criminal investigator with a doctorate. He was meticulous to describe his research as an endeavor to create methodology for deception detection rather than a quest to invent a lie detector “apparatus.”⁹ He was a dedicated professional deeply respected for his work ethic and unrelenting integrity. His partner Leonarde Keeler was a high school teen with more perceived charisma than veracity.¹⁰ Ironically, though they began as partners on a quest for truth, they parted as enemies, each accusing the other of being a liar.¹¹

The idea Larson and Keeler eventually developed and marketed as the polygraph was originally the creative imagining of Harvard psychologist and lawyer, Dr. William Moulton Marston.* Theorizing that a telltale symptom of verbal deceit was measurably increased systolic

* Dr. Marston is likely better remembered by his nom de plume Charles Moulton as the creator of DC Comics’ Amazon super heroine, Wonder Woman, making her debut in issue #8 of All American’s *All Star Comics*, in December 1941 (Daniels, *Wonder Woman*, 25). Along with amazing cunning and strength, Wonder Woman used fantastic devices like a silent, invisible airplane, indestructible bullet-defying bracelets, and the “Lasso of Truth” to stop super villains in their tracks. When bound with her lasso, criminals were mystically forced to tell the truth. Wonder Woman’s lasso was given to her by Hephaestatus who forged it from the Magic Girdle of Aphrodite (National Research Council, *The Polygraph and Lie Detection*, 295). In real life, Dr. Marston may have based the binding lasso on a sphygmomanometer cuff he theorized could detect deception through blood pressure fluctuations.

blood pressure, in 1915, Dr. Marston used a common medical device, a sphygmomanometer or blood pressure cuff, during interrogations to predict sincerity.¹² Similarly, he later theorized the stress of intentional deceit would cause changes in breathing and used a pneumograph to record respiration rate.¹³ Yet despite his promotion in academic literature (as well as comics) of gadgets, instruments, lassos, and truth serums, it was the quest for truth, not merely advancing technology, that drove Dr. Marston. One researcher notes, “Marston was practically insulted by the idea that his attempts at lie detection were simply an application of technology. He believed that it was the interrogation techniques used in conjunction with the technology rather than technology itself that was responsible for the ability to detect lies.”¹⁴

The skill of interrogation still plays a central role in the effectiveness of modern deception detection, as do fear and belief in the polygraph, both the process and the paraphernalia. As one researcher not convinced of the effectiveness of existing technology notes cynically, “Tests of deception, ironically, must themselves include a deceptive element. ... Validity [of polygraph tests] depends on an examiner’s ability to convince (deceive) a subject that he or she must respond truthfully because deception will be detected.”¹⁵ Another researcher concludes there is “strong evidence that the lie detector test is indeed highly fallible and that this fallibility translates into a strong bias against the innocent respondent.”¹⁶ Another, while serving on a panel of five expert witnesses before a 1984 Senate hearing testified if the polygraph is useful, it is because

[t]he mechanism by which polygraph tests gain information is fear. As long as individuals are both afraid of polygraph tests and believe that the test can detect lies, they may show highly aroused reactions to questions on which they lie.

If these conditions are not met, the test may have little validity.¹⁷

Another expert witness, Gen Richard G. Stilwell, USA (Ret.), admitted under testimony the breadth of research conducted on the validity of polygraphs has produced a startlingly wide range of results from “no better than toss of a coin – to upwards of 97 percent accuracy,” though he immediately added, “[O]ur assessment shows it to fall in the higher range.”¹⁸ He assured the Senate Committee that despite the controversy over its scientific legitimacy, the empirical evidence of its effectiveness in the hands of highly skilled, stringently selected and trained technicians has proven valuable at solving criminal cases, obtaining confessions from criminals, identifying agents of hostile intelligence agencies applying for sensitive defense or intelligence jobs, and deterring current intelligence agents from mishandling classified materials.¹⁹ Perhaps this is so, but is there a better tool, one which can go mobile and be employed undetected?

The Question

When ensuring national security, protecting lives, or promoting justice is on the line, detecting deception is critical. How can today’s best practices be combined with tomorrow’s promising technologies and discoveries to enhance the fields of investigation, human intelligence gathering (HUMINT), and deception detection for other purposes? Can the current intimidating, sterile investigation room be made more inviting, comfortable, and, in the process, more effective? Can the equipment itself be made small enough to be carried, or perhaps even worn unnoticeably into the field for on-the-spot interviews? These are the questions this paper will explore. It will discuss current trends in deception detection and how future technological breakthroughs in fields such as artificial intelligence, pervasive computing, and distributed sensors might enable operators to move from current bulky polygraph machines, which must be tethered to the interviewee and directly monitored throughout the interrogation, to a more welcoming conference room in which the same functions and more are discretely and remotely

monitored and evaluated by human and machine, guiding the conversation as it flows to a mobile system which the agent can wear unsuspected while conducting field interviews and investigations.

The Method

I began research utilizing environmental scanning to broaden my limited knowledge of the subject of deception detection, reviewing past and current tactics, techniques, procedures and technology utilized in deception detection as it is recorded in peer-reviewed professional and academic journals and like media. Next, I utilized limited backcasting to establish reasonable timelines for the near future (2020) and far future (2035) scenarios I present in the text. I concluded my research with a modified Delphi study method described by Futurist Joseph Coates as a “conversational Delphi technique,”²⁰ in order to further explore current trends and future possibilities by hearing from the experts in the field.

Two Special Agents from the Air Force Office of Special Investigations shared their knowledge of the current state-of-the-art of investigations, interrogations, and the polygraph. While they presented much higher confidence in the polygraph technology itself than many researchers, their personal stories of its effectiveness were typically grounded in how the interrogation techniques and personal interaction, supported by the technology, produced a remarkably high number of admissions or confessions in real-world application.

Three nearby university professors, experts in systems management, knowledge management, information technology, and network security, also provided helpful insights through face-to-face and telephone conversations. I shared with them my research findings and proposed scenarios for the near and far future. I asked them open-ended questions about their general knowledge of the subject area and how their particular areas of expertise might

contribute to the field in the near and distant future. In particular, the comments of the expert in knowledge and data management aligned precisely with the forecasts of futurists Dr. Marvin J. Cetron and Owen Davies, who predict the necessity of greater progress in data compression and storage capacity as well as expansion of bandwidth to support the enormous increase in data as computer processing speeds continue to grow and virtually all communications go digital.²¹ I also asked four targeted questions regarding the future scenarios I present in this paper, namely: “Is it reasonable to believe these events could occur by 2020 and 2035?” “What factors would enable these new technologies?” “What factors would hinder them?” and “Should we pursue these technologies?” Their responses are incorporated into the “Responses from the Delphi.” In keeping with Coates’ ethical guidance regarding Delphi participant responses, and Air University policy regarding academic non-attribution, all interviews were conducted in confidentiality and the names of interviewees withheld by mutual agreement.

Finally, it was originally my intent to investigate the broader application of tactics and technology from the 2035 case study in the realm of caregivers, to discuss how they might improve detection of stress levels or suicidality among clients for chaplains, physicians, or mental health providers. Two subject matter experts provided feedback on that issue. A chaplain and a judge advocate general, both Air Force field grade officers, insisted on “pulling the plug on that idea”²² before discussion continued simply because it would present major ethical issues for caregivers which may negatively impact trust relationships with those whom they serve. While this seemed at first a setback to my initial research intent and earliest hypothesis of how advances in technology might be used among caregivers, it upheld the initial feedback I received from my Delphi members regarding the critical role of human interaction in the process now and in the future. What Dr. Cetron predicts about intelligence collection holds

true for deception detection as well: “the traditional superiority of U.S. SIGINT is rapidly falling by the wayside. Without corresponding HUMINT to point the way, giving at least the opportunity to penetrate communications systems, we will still be oblivious to many of the messages streaming back and forth under our noses.”²³

Current State of the Art

2010

Agents have been investigating John for weeks. Something just doesn’t make sense about his story. His daughter Kelly told one version, his estranged wife Janet another, and John continues to deny both. Interviews with her daughter’s friends last week corroborated at least part of the events Kelly described to the first agent about the first time she says he struck her. Her friends claim they heard the stories, too, and saw the bruises on her face. But John claims the bruises were from her getting hit with a softball while playing catch with him after work that day. He says the stories of abuse were concocted by Janet as a way to get even with him and to punish him for breaking his marriage vows during his deployment last summer. Certainly, if the tales are true, Kelly must be protected from more abuse, and John must be held accountable. But John has always been an exemplary Airman, one of the group’s most promising young noncommissioned officers. If he is innocent, he deserves the chance to clear his name.

At last John has consented to come into the office for a polygraph. Probably because he knows the results can’t be used against him in court and only the answers he gives to the questions asked are admissible as evidence, his lawyer has consented to this interview.

John and his attorney arrive about ten minutes early. They have had an opportunity to review the questions John will be asked and John’s attorney will be present in the observation

room during the entire interview. Special Agent Jackson offers John a can of soda. (In some cases, the can might be secretly retrieved from the trash following the interview to obtain DNA samples, but that will not be required for this investigation.) Jackson then escorts John to the interview room, a small, tidy, rather formal place sparsely furnished with a small table and a few rigid, uncomfortable chairs. A small camera mounted on the wall juts obtrusively into the room just above a large mirror. John is sure it is a one-way viewing mirror and wonders who besides his attorney will be monitoring this interview from the observation room. A laptop computer spewing wires and electrodes blinks to life and glows obtrusively on the table beside the chair where John is offered a seat. He can feel his face reddening. "Is it getting warm in here?" he wonders. He glances at the machine and the operator again and can feel his palms sweating and his pulse beginning to increase. "This isn't good," he thinks. "We haven't even begun, and I'm failing already." Jackson explains the procedures one more time as he places the heart monitor around John's chest. With it, they will measure his pulse and respiration. A blood pressure cuff is placed on John's arm to take readings throughout the interview. "Great," John thinks, "I can't even get my pressure taken at the clinic without it going up a few notches!" Electrodes are attached to his fingers and arms to detect muscle tension and perspiration and pneumatic tubes are placed around his chest and abdomen to measure his respiration.

Today's interview will be a controlled question test. Jackson explains it is "very reliable, and will detect immediately if you lie, so don't bother. He reads aloud through the list of questions John and his lawyer have already seen and assures John he will ask only questions from this list.. As he does so, he emphasizes the most relevant question of the interview, "Did you strike Kelly and cause her bruises?" He pauses, giving John a few moments for silent reflection before launching into the interview. Then it begins.

The Challenge

The effectiveness of today's technological deception detectors depends largely on the skill of the administrator to ask appropriate questions, observe a wide range of behaviors, and correctly interpret responses and machine outputs. Interviews typically follow similar, structured approaches. As explained by General Stillwell, a polygraph examination consists of three phases, although only one phase requires the individual to be connected to the machine.²⁴

The pre-test phase is a period of preparation for the examiner and the examinee alike. The examiner uses this time to review information about the individual to be interrogated and the specific details of the case and to prepare a series of question charts, usually three, that ask strategic questions about the individual and the case. The examiner will base questions on specific types of prescribed interrogation templates depending on the circumstances and type of test to be conducted. The examiner will remind examinees of their legal rights, including their right to have an attorney present, their Fifth Amendment right against self-incrimination, and in most cases, their right to refuse to submit to the polygraph examination.

The interview begins during this pre-test phase to establish a subjective impression or baseline for the examiner and to determine the examinee's mental and physical fitness to participate in the polygraph test. Once assured both are prepared to continue, the examiner begins the explanation (and some cynics suggest hard-sell) of the equipment and how it works. The examinee is reminded repeatedly that it is absolutely imperative to tell the truth throughout the entire interview because the machine will be able to detect the slightest hint of indecision or deception. Finally, the examiner will share with the subject all of the questions to be asked during the interview with the reminder that any attempt to obfuscate the truth will be caught by the machine. That nearly 10 percent of criminal suspects offer a full confession at this point

before being connected to the equipment speaks to the effectiveness of the interrogation method, the skill of polygraphists, and the fear of being caught more than the reliability of the polygraph machine itself.²⁵ Even if it is simply a placebo, the polygraph has a powerful emotional effect on some individuals.

Phase two, the in-test phase, begins with connecting the subject to the machine – usually two finger clips to measure galvanic skin response (GSR), a measurement of electrodermal response associated with perspiration; a sphygmomanometer cuff to measure pulse rate and blood pressure; and pneumatic tubes around the chest and abdomen to measure breathing rate and depth.²⁶ Other sensors may be attached directly to the skin or hidden in the chair arms and seat to record movement or muscle tension in the arms or legs. As each item is connected, the subject is reminded again of the purpose and effectiveness of each item to detect deception. Then the questioning begins.

As suggested in the scenario above, the most common form of polygraph testing is the control question test (CQT).²⁷ Investigators ask insignificant control questions such as “Have you ever taken anything without permission?” They compare responses with those to more specific questions about the incident under investigation, such as “Did you steal the” The other most common test, called the Relevant-Irrelevant Test (RI), also compares responses to two types of questions, some pertaining directly to details of the case, and others more open ended, such as “ “Is your name ... ?” “Is today Tuesday?” or “Are the lights on in this room?” The series of yes or no questions will be repeated in various ways multiple times during phase two. Between the first and second round of questions, the examiner may insert a test of the equipment purportedly to make necessary adjustments and test the machine, but more likely its

true purpose is to further impress on the subject the effectiveness of the machine at detecting deception.²⁸

During the final post-test phase, the examinee is disconnected from the machine, but the test is not over. The examiner will go over the results hoping to engage the subject in further discussion and give one last chance for a guilty individual to “come clean.” The examiner may ask if any question particularly troubled the subject or may point out recorded or observed agitation about a specific question and ask for more clarification. The examinee may be asked if there is anything he would like to get off his chest. General Stillwell notes, “Significant admissions or confessions are also frequently obtained during this phase of the examination.”²⁹ He reports elsewhere 40 percent of all cases where deception is indicated will result in confessions.³⁰

Throughout the interview, the polygraphist is not seeking so much to identify outright truth or a lie as he is to identify differences in tone, expression, behavior, and voluntary and involuntary biological responses to the questions. While existing technology does add a level of objectivity to the process, ultimately, as Dr. Margaret Gibson notes, “The machine is translating the body, and the polygraph expert is translating a graph”³¹ which still makes successful detection of deception largely dependent on the skill of the interviewer.

Successful detection throughout the three phases requires well-prepared questions and skillful guiding and observation by the examiner; it also depends on the ability of the equipment to accurately measure and record “microscopic, subvisual fields of emotional and cognitive activity.”³² Dr. Gibson calls the polygraph “a psychophysiological biotechnology operating within a different logic of identification and detection.”³³

Still, even with years of experience, well-trained and talented investigation professionals, with the best technology currently available, can mistake natural behaviors reflecting stress, fear, or discomfort for guilt. As observed in the episode with my mother, stress can sometimes cause truth tellers to appear to be liars, and obviously the converse can also be true – liars can sometimes lie so convincingly they are perceived to be truth tellers. Indeed, some of the best controlled studies produce no better than 25 to 75 percent accuracy rates.³⁴ Dr. John Allen notes, “Traditional polygraphs, which measure anxiety and emotional arousal, are notorious for falsely incriminating innocent (and anxious) individuals.”³⁵ Although polygraph examiners rightfully boast their interrogations frequently result in confessions, aggressive interrogations might also encourage false confessions. In one lab test, for example, polygraphists were able to pull false confessions of guilt from 17 percent of test subjects who had not participated in the mock crime. They were told certain parts of their polygraph test were suspicious and were pushed aggressively for a response.³⁶

While the psychological theory behind the polygraph remains more theory than irrefutable science, as there is no conclusive evidence for a universally consistent reaction to duplicity,³⁷ there may be some measurable responses to the stress of guilt or fear caused by conscious deception, at least among some people. Yet, as one author suggests, those same physical behaviors frequently associated with deception may also be the result of other stressors “such as being suspected of a crime or being hooked up to a machine and asked a lot of questions.”³⁸ Perhaps that is why the National Research Council determined the theoretical basis of the polygraph is “quite weak,” that research has stagnated over the years showing no likely improvement for the future, and then concluded, “Almost a century of research in scientific

psychology and physiology provides little basis for the expectation that a polygraph test could have extremely high accuracy.”³⁹

Looking to the Near Future

2020

Imagine Bob’s surprise when the police came knocking on his door a few weeks ago. It was late in the evening and he couldn’t imagine who it could possibly be. He was further shocked when he opened the door to discover two large police officers with weapons drawn standing in the doorway shouting instructions for him to put his hands in the air, then handcuffing him and leading him off to be booked into jail for a crime Bob claims he didn’t commit. Since then, Bob’s lawyer has informed him he is charged with armed robbery of a local bank. Although bank cameras didn’t get a look at the robber’s stocking-clad face, Bob otherwise matched his physical features perfectly, down to preferring his left hand to his right, and the getaway vehicle matched a car Bob drove until he sold it just a week ago.

Bob claims it is a case of mistaken identity. The cops have only limited evidence; while sufficient to obtain an arrest warrant and indictment, it is not likely enough for a conviction, but something’s just not right. So they’re not yet ready to dismiss the charges or drop the case. Bob’s lawyer makes other arrangements with the district attorney. If Bob can pass a lie detector test, he will be released. If he cannot, he will be offered a second chance with a private examiner. If he fails both, Bob will agree to plead guilty and face a reduced sentence or take his chances of a maximum sentence in court.

Bob’s never been through a lie detector test before, but he’s seen them on television, so he’s caught off-guard by the comfortable, welcoming office he is invited into. Bob looks around

the room but sees no special equipment, just a few comfortable looking chairs and a large flat-screen LCD television on one wall.

The interview begins. The examiner thanks Bob for his cooperation and promises the interview won't take too long, reminds Bob of his rights, and goes through the kinds of questions he will be asking. First are general questions about where Bob was on the day of the robbery, what if anything he knows about the crime, if anyone can verify his alibi during the crime, and why he decided to sell his car, to whom, and for how much. Then the television is turned on, and Bob is asked to look at pictures that pop up on the screen two or three at a time to see if he recognizes anything in the photos. They contain a series of picture of the community, people who were present in the bank, stores in the area, pictures of weapons including one that matches the weapon used in the holdup, and numbers – some random, some addresses, and some dollar amounts, one that matches the amount of money stolen. Several of the pictures capture information about the robbery that until now only the investigators and the robber would know.

When the slide show and questions are complete, the interviewer asks Bob if he wants to change his story about the bank robbery. When he again insists on his innocence, the examiner tells Bob to work with his lawyer to schedule another examination. What they don't tell him outright is they are convinced of his guilt based on this one.

Exploring Future Technologies and Processes

Perhaps the most obvious difference between this scenario and the present is the absence of the polygraph machine. Instead, Bob has been observed through distributed sensors hidden in the comfortable chair in which he sat throughout the interview. Computers in another room have monitored his body temperature, heart rate, and respiration remotely. Gone are the simple yes or no answers. Instead, Bob is given the chance to answer other directed questions and his

responses are recorded by microphones, cameras, and an eye scanner. Sensors in the ceiling have recorded bursts of brain activity when Bob responded to certain questions or photos on the screen. Not simply one test, but multiple tests found several points during the interview where Bob appeared to be experiencing specific stress, memories, or knowledge that only the police and robber should have had. It was enough to convince the police they got their guy.

Probably the easiest part of this scenario to imagine is the distributed sensors. Already, as noted earlier, some polygraph equipment uses hidden sensors to analyze muscle tension or movement. When I was a child, getting one's temperature taken meant an unpleasant experience with a thermometer being placed uncomfortably in one end or the other. When my children were born, the pediatrician simply stuck an electronic thermometer in the child's ear. Today, a device is waved across the forehead and body temperature is digitally displayed. When Grandma made peanut brittle, she made sure the candy was at the right temperature with a special thermometer hanging on the edge of the pan. It was just one more thing to wash. When Alton Brown⁴⁰ makes peanut brittle, he points a gun-like device at the bowl, pulls the trigger, and has an instant reading. By 2025, such devices will measure body temperature and perspiration from a distance and report them via wireless network to a central data collection point that will analyze data in real time. As is true today, changes in normal patterns will be evaluated to determine possible deception.

As the television flashes pictures and facts, sensors will also measure brainwaves. Called Brain Fingerprinting and invented by neurologist Dr. Lawrence A. Farwell, this new technique does not predict deception but simply detects memories present in the brain. The images are part of a new test procedure resembling a multiple choice quiz called the Guilty Knowledge Test (GKT).⁴¹ GKT, also known as concealed information test (CST) has been around since the late

1950s, but not in the way in which it will be utilized in the near future. Bob might be shown various types of handguns. If the weapon used was a Beretta M9 Special, when Bob sees that picture, it will trigger a memory and evoke a measurable brainwave. Other pictures might include a photo of the bank teller held up during the burglary or a photo of a large, brass name plate on the bank entrance. One researcher says this new method may sound like science fiction, but it is well documented; he explains, “Also known as event-related potentials or ERPs, [the brainwaves] measure the electrical activity of myriad neurons in response to a stimulus, such as a word or an image.”⁴² One portion of the ERP wave, a bump called the P300, is especially important to research. It derives its name because it is observable about 300 milliseconds after a trigger event and typically notes a significant memory has been prompted.⁴³

Another method used in conjunction with the television in this new interview room is an eye tracker that, like P300 scanning, searches for signs of stored memories. The theory behind this advance currently being investigated by the Department of Defense Polygraph Institute (DoDPI) is that the eyes will spend more time gathering new information than scanning familiar images.⁴⁴ While the difference is measured in milliseconds, computers receiving the eye-scan data can determine Bob spent less time looking at the familiar Beretta than the other weapons flashed on the screen. Likewise, he merely glanced at the dollar amount that matched his take from the bank while spending more time looking at other numbers. By themselves, these clues may not be as conclusive, but when several triggers point at deception, odds are greater they should be taken seriously.

Thoughts from the Delphi

Feasibility

The initial comment regarding feasibility comes from multiple sources on the Delphi. It is already painfully difficult to get suspects to consent to a polygraph, even rarer in criminal settings where defense attorneys will not allow a polygraph to be administered to a client. Advances in technology alone will not change the legal or civil rights limitations or current pushback to its use in the civilian realm. The technology itself captured the interest of the Delphi members, but sparked the thought that increased ability to detect deception may begin to shorten investigator's time to employ technology, particularly in domestic law enforcement settings where protection from self-incrimination is a celebrated Constitutional right.

Brain Fingerprinting is interesting and holds some promise for deception detection in the future, but right now, says Dr. J. Peter Rosenfeld, a Northwestern University Psychologist researching EPR, a field study published in 2004 "reported approximately chance accuracy."⁴⁵ Dr. William G. Iacono of the University of Minnesota, however, believes that finding is pessimistic. He admits research is yet to be done but argues, "[T]he GKT and its brain fingerprinting offshoots are based on sound science" and suggests it meets legal standards for admissible evidence in a courtroom today.⁴⁶ Tests by Dr. Farwell in 1991 demonstrated P300 combined with GKT are at least as accurate as the polygraph. Results showed the method correctly identified 88 percent of test participants who had knowledge of a mock crime. The remaining 12 percent were classified "undetermined," which would obviously call for more investigation in the real world. The best news is that there were no false-positives and no false-negatives.⁴⁷ Subsequent studies revealed countermeasures can impact the device's accuracy, and field testing was not as impressive as initial lab tests. Only 27 to 47 percent of participants in a

highly realistic mock crime scenario were accurately categorized.⁴⁸ Nevertheless, if further study can overcome these factors, the hope that this new technology can help identify liars without falsely incriminating innocents is worth pursuing.

Delphi members agreed, overall as presented, the technology seems feasible, limited only by the level of interest federal agencies that would benefit from these advances demonstrate through appropriate funding of ongoing research and development.

Catalysts

One catalyst is the American passion for technology and innovation. However, that can create a new set of challenges. *Nature* journalist Jonathan Knight reports statistician, Dr. Stephen E. Fienberg of Carnegie Mellon University, warns against moving too quickly from research to real world in deploying modern deception detection technology.⁴⁹ He argues people are hungry to believe in the value of new technology to solve great security or defense problems. Dr. Fienberg fears that putting new tools into use too quickly can create the risk of false incrimination of the innocent and a false sense of security from real terrorists or criminals. He explains when technology falsely categorizes the innocent as deceptive, their character is besmirched and their future well-being is threatened. Likewise, when those who wish to do harm slide through sensors and interrogations undetected, the public blindly believes technology has done its job and all is well.

Hindrances

For the time being, there are too many questions that must be answered before one can evaluate the real potential for Brain Fingerprinting: how does the lapse of time, onset of disease or mental illness affect memories? How does substance abuse or even limited use of drugs affect one's P300 response? In addition, Dr. Rosenfeld has already discovered some potential

countermeasures that can be used to manipulate the P300 response. In a lab test, Dr. Rosenfeld exposed some student subjects to a mock crime and then tested them for Brain Fingerprinting. Some participants in the test received instructions to imagine being slapped in the face by their professor each time they saw a new image. In the end, two-thirds of Dr. Rosenfeld's students generated P300 waves even when they should not have. His report concludes such results may not clear a suspect, but they would certainly ruin the validity of the test.⁵⁰

Certainly, there will be ethical and legal implications to consider with the proposed technologies. In Bob's scenario, his lawyer arranged the interrogation. This is not likely, says the Delphi lawyer, especially on a case with weak evidence, and certainly not with Bob knowing the tools being used would not only be measuring his truthful responses but would also be "virtually mind reading" for signs of guilt as images and text triggered memory points possibly associated with the crime.

A final drawback to the success of even the best in breakthrough technology as presented in this scenario is the ongoing demand for and shortage of trained investigators, field agents, and technicians who can employ the technology. As Remotely Piloted Vehicles took to the air over Iraq and Afghanistan, each signal sent back to earth created even greater demand for another aircraft, more information, and increased bandwidth. As accuracy of these technologies increases, so will the demand for the equipment and operators as close to the point of origin as possible whether that may be in the local police precinct, a walk-in source at a military base, or in the battlespace in a deployed location. Already there is a shortage of qualified civilian and military polygraphists. As demand for improved equipment increases it must be accompanied by an increase in technicians. Perhaps the best way to overcome this shortage, especially during a time of drawdown in personnel and funding, is through development of Artificial Intelligence to

accompany the technologies, to analyze data and provide immediate feedback to investigators to enable questioning and decision making as it occurs.

Value

Dr. Farwell suggests Brain Fingerprinting and P300 tests could be used to identify terrorists. He claims to have used the tests to distinguish between FBI agents and civilians by tracking P300 waves that followed terms related to FBI training.⁵¹ Perhaps similar images or terms known only to al Qaeda members could be used to trigger P300 waves in suspects in the same way as a screening tool when attempting to identify an individual or smaller pool of individuals from a larger pool. Since the National Research Council has declared polygraph research has reached a point where little more can be expected to be gained, any avenue that shows a reasonable hope of detecting deception should be welcomed and pursued.

Looking to the Distant Future

2035

As they approach the counter, the two thirty-something women look just like the other customers standing in lines to purchase tickets, check bags, or wait their turn to run the security check gauntlet before boarding their flight.

“Things sure have changed since 9/11,” says Arianna.

“How would you know?” retorts her companion Nova. “You were barely out of diapers yourself when that event happened. That’s ancient history!”

“I know,” says Arianna with a smile and a wink that tells Nova it’s all meant in fun, “but that’s what my parents say every time we fly. And I guess it’s true. I mean, there have been long lines at the airport as long as I can remember. I think I took my first flight when I was in

third or fourth grade. We flew to the U.S. and had to be at King Fahd at least two hours before the flight. It felt like forever back then.”

“Yeah, two hours! What a joke compared to the half-day we have to spend waiting at the spaceport now.”

“I know. But it’s gotten better since AM&M opened their new gates here.⁵² You can get through twice as fast. And it’s nice to see all the security lines move a lot faster now, too. But somehow, it doesn’t make me feel any safer, you know?” She adds another wink and a smirk.

“Stop messing around. We’re next,” instructs Nova, suddenly sounding like the adult of the two.

“I know, I know,” breathes Arianna. “O.K., here we go.”

“Good morning, welcome to AM&M,” says the man behind the counter. His name tag says Kirk, he speaks rather matter-of-factly, and looks as if he has done this too many times already today as he collects their ID cards. He waves them before the computer screen, pauses just a moment, and then continues, “You’re on the 4:00 p.m. to Lunar Port Scipio, is that right?” Seeing them nod, he continues, “That will be on board our new DH-3. How lucky for you, traveling to our newest spaceport aboard our newest craft. Did you know the port is named for a Catholic Priest—

“—Who was one of the pioneers of tourist space travel because he took a bunch of monks there about fifteen years ago,” Arianna interrupts. “Yeah, we know,” she murmurs under her breath.

Nova nudges her, then smiles nervously at Kirk who continues, “Well, will this trip be business or pleasure?”

“Trust me,” says Nova smiling, “our business is a pleasure.” Arianna nearly chokes with laughter. “I mean, we’ll be checking into the new Forsyth Manor Inn when we get there. It’s not like we’ll be at that Saint Senility Monastery or anything.” She receives another nudge from Nova.

“I see,” says Kirk, a bit puzzled. “I see you bought passes for four bags. Did you pack these bags yourselves?”

“Yes,” say both women.

“Good, and have these bags been in your possession since you packed them?”

“Again, yes,” says Arianna, growing more annoyed with the questions. “Just let us get on with this,” she thinks.

“O.K., and have you read the instructions for prohibited items?”

“Yes,” says Nova.

“So there aren’t any explosives, no weapons, nothing dangerous, none of the items on the list, right?” Kirk drones on as he glances at his screen with a puzzled look.

“Nope, none of those things, can we just check our bags now? I mean, does anyone really think someone is going to answer yes to any of those questions anyway?” Arianna asks with a smile.

“I’m afraid you just did,” says Special Investigator Scotty Duncan, suddenly standing behind the two women as he shows them his badge and a drawn taser. They look from Officer Duncan to four other agents in dark suits surrounding them. “Please come with us, and no sudden moves. Leave the bags where they are,” he instructs both the women and Kirk. “The EOD bots are right behind us to take care of them.”

Agent Duncan and his partners lead the two women away, two would-be terrorists, both fundamentalist supporters of a radical new religious group ironically protesting against organized religion. The group has been under close scrutiny for some time because of their calls for violent action against churches, religious institutions, and holy sites around the world. Most recently, there were rumblings about an attempt to bring down the first Christian institution in space. When the EOD robots inspect the bags in a safe, controlled environment, they will determine the hidden lie detector equipment worked and those crazy questions TSA has been requiring for decades now finally really mean we can catch criminals!

Exploring Future Technologies and Processes

You may find yourself asking, “What just happened? Can we really get from ‘Did you pack these bags yourself?’ to nabbing radical religious terrorists that quickly?” The real answer is, probably not. But the technology behind the story is clearly more science than science fiction even if it seems a bit of a stretch. So how did the Special Agents catch the terrorists in their tracks? It began the moment they pulled their rental vehicle into the spaceport parking bay. Video surveillance cameras captured their license plate number and ran a check against local, state, and national databases to ensure the vehicle’s owners were not on special watch lists. That’s how Arianna’s name first came up as the vehicle renter, and a quick cross-check found her name and a couple aliases she had used in recent years on a federal watch list. As the two women made their way from the parking bay to the concourse to check their bags and enter the security area, dozens of hidden digital video cameras followed them. Facial-recognition programs once again cross-checked the two women against digital data bases of individuals on wanted, watch, or no-travel lists. The software is so sophisticated even the dark glasses Nova wore did not prevent her being identified, and a software program called NORA made the

connections between Nova, Arianna, and about twelve other members of their radical religious terrorist cell.

This scenario is not far-fetched. According to *Baseline Magazine*'s Larry Barrett and Sean Gallagher, whose information technology case study, "What Sin City Can Teach Tom Ridge" claims Las Vegas casinos began implementing these same security precautions and more as early as 1999.⁵³ Facial recognition software used in the Stratosphere Casino Hotel & Tower, for example, measures key points on the face such as distance between the eyes or cheekbone structure and compares images to stored databases.⁵⁴ Already that technology has improved, claims Dr. Yi Hua Ma, University of Illinois at Urbana-Champaign professor of electrical and computer engineering. His development of an algorithm based on "sparse representation and compressed sensing" allows even partial facial images or images corrupted up to 80 percent to be used in successfully identifying individuals in real time.⁵⁵

NORA, an acronym for "non-obvious relationship awareness," is software already in use to probe databases in multiple languages to seek ambiguous associations between germane pieces of information.⁵⁶ It can make connections between people up to 30 degrees of separation in a way TV Land, the cable network, used to broadcast brief filler spots called "Six Degrees to ..." which connected two celebrities through six steps such as Adam Sandler to Rosanne Barr.⁵⁷ In a real-world example, had NORA been available in 2001, it could have detected that Mohammed Atta checked into an Econo Lodge Motel on Las Vegas Boulevard South on 13 August, and within moments, could have gleaned through data bases that Atta once shared a home address with Khalid-Al-Midhar and Salem Alhazmi, both also 9/11 terrorists.⁵⁸

High speed networks, data compression, sophisticated tracking software, and facial recognition are remarkable breakthroughs in security technology that helped to apprehend Nova

and Arianna, but where did deception detection play a part? What did Agent Duncan mean when he said, “I’m afraid you just did”? Facial recognition is the first remarkable step to this technology, but the next step is even more remarkable.

According to Dr. Ken Alder, Northwestern University Professor of Science in Human Culture, the ancient Greeks may have had the answer long ago. He writes, “The Greeks developed a science of physiognomy to assess people’s character from their facial features and gestures.”⁵⁹ Dr. Ioannis Pavlidis, professor of computer science at the University of Houston, and Dr. Norman L. Eberhardt and Dr. James A. Levin, both of Mayo Clinic, have developed a new approach to deception detection based on observations that capillary blood flow in the face is affected by fight-or-flight triggers such as a sudden start. Dr. Richard Davidson of the University of Wisconsin, Madison, claims an abundance of brain research rather than psychological theories allows new technologies like thermal imaging to detect the “fear of detection” in the amygdale region of the brain.⁶⁰ The fight or flight response to such fear triggers a unique “facial ‘thermal signature,’ in which there is instantaneous warming around their eyes.”⁶¹ This sudden thermal response can be observed with high definition infrared imaging scanners and give instantaneous feedback with at least as much accuracy as current polygraph machines.

Dr. Pavlidis and his team conducted a DoDPI sponsored test of the system in which 20 volunteers were assigned to simulate murder by stabbing a mannequin, rob it of 20 dollars, and then claim innocence of the mock crime.⁶² Thermal imaging correctly identified 83 percent of the participants; 6 of 8 were correctly identified as guilty and 11 of 12 were rightly categorized as innocent. Traditional polygraph tests on the same volunteers resulted in only 70 percent accuracy, with only 8 of 12 innocent participants being correctly identified. While not

significantly better than the polygraph in accuracy, the technology is still new and interests DoDPI and TSA because it can be used in high throughput areas like airport terminals and does not depend on the analysis of highly trained polygraphists.

Drs. Janet Rothwell, Zuhair Bandar, James O'Shea, and David McLean, all of Manchester Metropolitan University in the UK, also offer a new method of deception detection based not only on facial analysis but on examining multiple factors for non-verbal clues to stress, arousal, felt emotion, or cognitive processing indicating lying.⁶³ They suggest the polygraph examines certain "channels" – heart rate, respiration, and perspiration, for example. Thermal imaging of the face as described above is another. Drs. Paul Ekman and Maureen O'Sullivan of the University of California, San Francisco and the University of San Francisco, respectively, describe facial microexpressions (facial expressions that last no longer than 1/25 of a second) and "masking smiles" (false, nervous smiles that do not involve the eyes) as yet another such channel.⁶⁴ Dr. Rothwell and her team have created an Artificial Neural Network-based system they call "Silent Talker" that digitally records and analyzes these channels to detect deception. Their research has determined that multichannel analysis is superior to consideration of a single channel, producing positive identification of deception in over 80 percent of test trials.⁶⁵

Combined with technologies from the 2020 scenario about Bob, these technologies will serve to assist human agents in detecting deception and apprehending criminals and terrorists before they can act.

Thoughts from the Delphi

Feasibility

Dr. Ekman says it is possible to train people over time how to become better lie detectors without the need for other technology by teaching them the signals to look for. That success

level, he admits, will never reach 100 percent.⁶⁶ Still, as evidence that some people can indeed catch a liar, he points to the success level of highly trained human lie detectors such as Secret Service agents, whom he claims scored accurately 64 percent of the time on exercises during workshops he conducted.⁶⁷ During the workshops, Dr. Eckman attempted to determine how effectively professionals could detect deception and what means they used. Participants including Secret Service agents, Federal polygraphists, police investigators, judges, psychiatrists, and a control group of students were shown 10 one-minute video samples of previously recorded interviews. The test group viewed the 10 videos of women all claiming to be watching a nature film during the interview; however, about half of the women were really watching a visually disturbing, graphically violent film. Dr. Eckman reports Secret Service agents scored highest followed by psychiatrists at 58 percent; polygraphists and investigators who tied at 56 percent.⁶⁸ According to Dr. Eckman, those who scored best reported “using nonverbal as well as verbal clues to deceit” and “are better able to interpret subtle facial expressions.”⁶⁹

Dr. Cetron predicts by 2035 we will see greatly increased processing speed, data storage and compression, and advances in artificial intelligence and conversational computers, “mind machines,” that respond instantly as humans simply think questions.⁷⁰ If humans can learn to detect behaviors that signal deception unassisted with accuracy nearing that of the polygraph, imagine how much greater will be their ability to scan and analyze multiple “channels” of signals, verbal and nonverbal, with real time feedback. From that perspective, the advances described here seem very feasible indeed.

However, not everyone agrees people can be trained or technologies developed quite so easily. Dr. Bond is a critic of Dr. Ekman’s research and reports that what Dr. Ekman chose not to report in his studies was the high scoring Secret Service agents scored their own tests, and

concludes sarcastically, “Who can catch a liar? It would appear to be Secret Service agents who get to score their own tests.”⁷¹ Dr. Kenneth R. Foster of the University of Pennsylvania insists we must move slowly and carefully in adopting new technologies of deception detection. He cautions, “Polygraph testing came to be widely used and accepted in the United States and other countries without the careful evaluation that should be required of any investigational tool on which the future of the subject’s life depends. ... [N]eurotechnological methods should be subjected to a rigorous, independent, public assessment.”⁷² So, are the technologies feasible? Perhaps. Easy or swift? Certainly not.

Says one Delphi member, “I see no ‘holy grail’ of infallible detection deception as ‘lying’ is a personal experience which comes with many personal attributes and individual characteristics... technology will have to overcome the huge variances [in emotion, fear, or physical responses] brought on by the uniqueness of humans.” The consensus was, at least in the near future, due to such human differences, reaching 100 percent accuracy is unrealistic. However, increasing accuracy of deception detection even in small steps of percentage points and minimizing false positives would greatly enhance both civil and military cases.

Catalysts

An obvious catalyst is funding. Delphi members agree initiatives led and funded by the Departments of Defense, Justice, and Homeland Security would jump start technological breakthroughs. Grants, internships and Federal directed research at institutions like the Air Force Institute of Technology, National War College or service academies could enhance ongoing research or inspire new concepts. We must ensure the human agents who depend on deception detection tactics, techniques, and technologies are provided as quickly as reasonably

possible developing resources to improve their investigations and HUMINT collection and assessment.

Recent re-emphasis of HUMINT is itself a catalyst. One Delphi member returned to Dr Cetron's earlier comments on the critical role of HUMINT, especially as the U.S. dominance in SIGINT and IMINT diminish as technology becomes more affordable and accessible. Field agents need greater ability to gather and analyze information from multiple sources simultaneously, "thus maximizing our numbers and effectiveness of 'HUMINT platforms' from the ground level soldier, sailor, airman or marine interacting with lower level sources of information, to our most sensitive operations involving critically placed human sources managed by our most highly trained intelligence service agents."

Another catalyst is the development of other supporting technologies. A major drawback to Dr. Ma's program is the size limitation of the database. Although it is based on a scalable algorithm, "if the number of subjects becomes large, running the algorithm in real time on current hardware is challenging."⁷³ In 2009, the program was limited to around 1,000 records. Enter Dr. Dennis Bushnell and Moore's law. Dr. Gordon E. Moore, author of "Moore's Law" predicted computing power would double every two years, but only through 2020, by which time, he believes, transistors will have reached the limits of miniaturization. However, Dr. Bushnell of NASA's Langley Research Center predicts computing power will increase even faster than Dr. Moore envisaged through 2030 and beyond.⁷⁴ According to Dr. Deton, silicon chips will be replaced by higher speed optical or molecular computers, or possibly even biocomputers capable of "sustaining over 20 petaflops, 20 million billion floating point operations per second."⁷⁵ He explains that speed is roughly the equivalent of a human brain, and

he continues, “[B]y 2030, the personal computer will have computing power equal to a town full of human minds.”⁷⁶

So, computational power will not be a problem. Nor will pervasive sensors including “undetectable cameras and sophisticated networks,” and massive, searchable databases capable of storing detailed personal data, according to a 2006 RAND Report on technology which predicts by 2020 such technological breakthroughs are highly likely.⁷⁷ The study further suggests virtually ubiquitous use of radio frequency identification (RFID) tracking for both commercial goods and individuals—that rental vehicle is more likely to be identified by RFID than a license plate by 2035. Finally, both Dr. Cetron and the RAND study predict pervasive computing and ubiquitous internet will carry such data at lightning speeds virtually anywhere across “fiber optic networks and satellite-based Internet backbone services” by 2020.⁷⁸

Hindrances

Continued research on thermal imaging funded by DARPA has made improvements to Dr. Ma’s previous work. A team of six researchers from four different universities and academic fields were able to increase accuracy to above 87 percent in lab tests by using tandem tracking of scans to accurately record the region of interest on the face, and noise suppression to remove high frequency blurs from images.⁷⁹ Yet, despite these improvements, a simple pair of eyeglasses still blocks the thermal signal.

Silent Talker holds promise because it incorporates existing technologies with others as they develop, and utilizes artificial intelligence to assist in evaluating trigger behaviors and signals in real time. However, early studies demonstrated that ethnic and cultural differences affected the way Silent Talker interpreted data in much the same way they can confuse human observers. One Delphi member recalled observing a conversation between two Turkish men

standing chest to chest, talking loudly and excitedly, and gesturing wildly with their arms. The American observer assumed they were arguing. Another Turk later explained they were good friends simply talking about their families. Emotion is a complex issue made more complex by cultural sensitivities. Dr. Roberto Caldara at the University of Glasgow concludes, “[F]acial expressions that had been considered universally recognizable cannot be used to reliably convey emotion in cross-cultural situations.”⁸⁰ Perhaps over time Dr. Rothwell and her team can train the artificial neuron networks informing Silent Talker to recognize and consider one’s ethnicity based on language, dialect, or accents, but doing so adds another factor to the already complex system.

Another hindrance will be privacy. As information sharing increases both in speed and quantity of personal information carried over networks, personal privacy will be an ongoing concern. Futurist Joseph Coates even foresees a time when technology will provide drivers immediate feedback from their vehicles, (“You took that turn too fast,”) and may report such behaviors to parents of teen drivers or even law enforcement officials.⁸¹ How much privacy and freedom Americans are willing to trade for the sake of increased security has yet to be determined.

The Delphi also added a caution that constitutional civil rights will limit the application of much of the technology described. An increase in accuracy of deception detection technologies will likely correlate with a decrease in the ability to test suspects with criminal defense attorneys. More emphasis may need to be placed on moving deception detection closer to the initial interactions with suspects. Mobility would allow use of such technologies during the initial field investigation. As one member noted, “It may even re-define what we know as an interrogation.”

Value

Besides the obvious value of increasing national security by improving deception detection and perhaps reducing false-positives that can permanently impact the innocent who are accused of dishonesty, the technologies described in this section can be combined with anticipated nanotechnology solutions that by 2035 will be able to produce nearly invisible cameras and remote sensors, ubiquitous internet, and pervasive computers that are worn rather than carried.⁸² Such technologies could accompany field agents conducting crime investigations in public or interviewing foreign nationals in a war zone, and provide instantaneous analysis, feedback, and increased situational awareness alerting the agent to suspicious responses or threatening postures, and helping guide the conversation with follow-up questions or direction for clarification, shaping the interview as it transpires.

Of special interest to the Delphi were technologies aided by Artificial Intelligence and mobility which enable the broadest dissemination and application of viable technologies and enhance the ability of even novice agents to gather and assess the veracity of information as close to the original source of collections as possible. One member noted, “Detecting deception in human sources of information is a huge part of making leaps in HUMINT.”

Conclusion

According to at least one telling of Greek mythology, the Titan Prometheus created the first human to win a competition among the gods to prove who among them was the best artist. Momus, the god of satire, censure, and criticism mocked the creation, man, because Prometheus had failed to place “windows in his chest which could be opened to let everyone see his desires and thoughts and if he were lying or telling the truth.”⁸³ This is the quest of the modern investigator, special agent, intelligence officer, and even chaplain or other caregiver – to break

through the barriers of human kind, to hear beyond words and see beyond the surface to know the truth. Yet even the best methods in use today have a shaded reputation and hotly debated validity.

One polygraphist I interviewed took strong exception to comments I wrote earlier suggesting modern polygraph technology correctly identifies deception in laboratory settings correctly only 40-60 percent of the time, arguably the same percentage expected by sheer chance. He assured me the equipment works if the technician knows how to use it, and then persuasively argued he has gotten numerous individuals to confess to crimes during interrogations after connecting them to the polygraph equipment. It is understandable that some examiners were reluctant to speak openly about their processes, the equipment, or what lies ahead. As the National Research Council found, “Members of the polygraph examiner culture have a particular jargon and shared lore that are generally unknown to others. They also maintain secrets because to reveal too much of their knowledge would enable targets of investigations to ‘beat’ polygraph tests. The polygraph device or instrument is purported to have the power to discriminate lies from truths in the hands of a certified and experienced examiner.”⁸⁴ It seems Dr. Marston was right: the technique and the technician are as critical as the technology, perhaps more. Even J. Edgar Hoover testified the lie detector was just a “psychological aid” when he appeared in Congressional hearings.⁸⁵ If it produced results, he reasoned, it was not the equipment alone but the work of a skilled operator which made the difference.

Drs. Benjamin Kleinmuntz and Julian J. Szucko concluded their research with the same findings: “The fact is that lay persons and many law enforcement personnel believe that the lie detector works. This belief provides polygraphists with their necessary leverage and advantage to carry out their tasks even though the polygraph has no intrinsic scientific validity. In this

sense, lie detectors serve as a sort of gun-to-the-head threat to make people confess or, at very least, to behave themselves because Big Brother may interrogate them”⁸⁶ They compare the effectiveness of the technology to spurious video cameras mounted in some stores, equipped to periodically turn, and accompanied by highly visible warning signs that customers are being observed. If such equipment works, they reason, it is because of the would-be thief’s belief in the equipment and not its intrinsic value that makes the difference. As Dr. Alder notes, “...[P]ersuading Americans of the machine’s potency was itself a prerequisite for the machine’s success. As its proponents acknowledged, the lie detector would not distinguish honest Americans from deceptive ones unless those same Americans believed the instrument might catch them.”⁸⁷ The National Research Council cites an exemplary study called a “bogus pipeline” study in which student research subjects were given answers to a classroom test. When interviewed in two groups afterwards, one group without a lie detector and the other with students wired to a bogus machine, only 1 of 20 in the group with no machine admitted guilt whereas 13 of 20 in the other group admitted to the cheating scandal after being wired to a machine – even a machine that did absolutely nothing!⁸⁸ Dr. Alder observes, “In short, the lie detector depends on what medical science has dismissively termed, “the placebo effect.”⁸⁹

Perhaps that was the secret to Wonder Woman’s Lasso of Truth: not a mysterious power, but a placebo effect that promoted truth telling among not-so-super villains. And perhaps, if the skeptics are correct, the best we can hope for in deception detection is the state of the art today, and the more wires and the more whirring, clicking, and pulsating equipment, the more credibility the experience creates for layman and technician alike. Perhaps taking away the sensors and palpable technology will reduce that placebo effect and render other tests less reliable.

Perhaps, but another name for *placebo* is a *lie*. From 1912 to 1991 the Central Committee of the Soviet Union used a newspaper as a tool for promoting party propaganda. Although it originated as a voice for the people during the Bolshevik Revolution and was used to raise issues about labor parties and working conditions, it eventually devolved into an official organ of the Communist Party, a means to promote the official, carefully edited government view on news and world events. It promoted nationalism through militant slogans and smeared any who stood opposed to the party. Ironically, the name of the paper which so blatantly recreated reality as the party saw fit was *Pravda*, which means *Truth*. It is no less ironic that while the purpose of the polygraph, the so called *lie detector*, is to determine truth, it does so largely through deceptive practices designed to promote the validity of the instrument and induce fear in the interviewee for the purpose of scaring the truth out of would-be deceivers.

While it may be effective at persuading some to confess, the research behind the polygraph is dated and its psychological foundation is academically contested. *Science* medical health reporter Constance Holden cites the growing interest in alternative technologies among researchers and writes, “Even practitioners acknowledge that the validity of polygraph tests relies heavily on factors not related to the instrument, such as the training of polygraphers and the nature of the screened population.”⁹⁰ New research is necessary. Not research founded on the psychological inner struggles between good and evil, the *lying consciousness* and the *confessing body* of which Dr. John Larson spoke in 1969,⁹¹ but research based on sound science which seeks to increase deception detection rates while at the same time reducing false positives.

This research deserves the support and funding of DoDPI as well as the Departments of Justice and Homeland Defense. One Delphi member stated, “The return of emphasis to HUMINT must be accompanied by innovative technological approaches to capturing and

evaluating the veracity of human offered and gathered information.” National security and criminal justice demand a renewed emphasis on deception detection research that boldly and purposefully moves beyond the psychological fraud and dated technology of the polygraph. As one Delphi member stated

We lament commanders must often make decisions based on intelligence that is 65 percent complete. No intelligence or information is perfect, but wouldn't it help a commander make a better decision based on an intelligence report from a human source when it was accompanied by a trusted assessment of the level of deception noted during the information gathering? Wouldn't it help a lead detective or special agent making a critical decision about using resources to continue to pursue a suspect in a major crime based on an assessment of their responses to initial questions? Increasing our accuracy in detecting deception would be yet another way of improving operations and investigations in domestic and military settings thus paying huge benefits.

If we're going to make statements about the importance of HUMINT more than lip-service, we need to advance beyond the stubby-pencil and pad days and into how to make the intelligence collection method more reliable and timely, just as we do with other platforms today.⁹²

Dr. Alder reminds us, “Saint Augustine long ago defined a lie as the gulf between the public utterance of one's mouth and the secret knowledge of one's heart.”⁹³ We are still seeking to bridge that gulf and like Momus, we desire a window into the soul through which we can see another's heart and determine for ourselves the truth. An Arab proverb decrees, “He who foretells the future lies, even if he tells the truth.” So I am reluctant to declare what will be. But of this I am certain: the quest for truth will continue, and if this research has proven anything, I believe it is this: as Dr. Marston knew from the beginning, at the forefront of tomorrow's breakthroughs will be the human investigators enabled by modern technology and not the converse.

Notes

(All notes appear in shortened form. For full details, see appropriate entry in the bibliography.)

- ¹ Lock, "Deception Detection," 72.
- ² Klaver, et al., "Psychopahty and deception using indirect measures," 172.
- ³ Lock, "Deception Detection," 72.
- ⁴ Kleinmuntz and Szucko, "Lie Detection in Ancient and Modern Times," 766. As well as Alder, *The Lie Detectors* "xii.
- ⁵ Alder, *The Lie Detectors* "xii.
- ⁶ Kleinmuntz and Szucko, "Lie Detection in Ancient and Modern Times," 766.
- ⁷ John Larson quoted in Gibson, "The Truth Machine," 61.
- ⁸ Alder, *The Lie Detectors*, "xi.
- ⁹ The Polygraph Museum
- ¹⁰ Alder, *The Lie Detectors*, "xi.
- ¹¹ Ibid., "xiii.
- ¹² National Research Council, *The Polygraph and Lie Detection*, 291.
- ¹³ The Polygraph Museum
- ¹⁴ Singel "Origin of the Modern Polygraph."
- ¹⁵ Saxe, "Detection of Deception," 72.
- ¹⁶ Kleinmuntz and Szucko, "Lie Detection in Ancient and Modern Times, 773.
- ¹⁷ Statement of Leonarde Saxe, Ph.D., Boston University, in Senate, *Polygraphs for Counterintelligence Purposes in the Department of Defense*, 61.
- ¹⁸ Prepared Statement of Gen Richard G. Stillwell, USA (Ret.), Deputy Under Secretary of Defense for Policy, in Senate, *Polygraphs for Counterintelligence Purposes in the Department of Defense*, 20.
- ¹⁹ Ibid., 22-23,32.
- ²⁰ Coates, "An Overview of Futures Methods," 62.
- ²¹ Cetron and Davies, *Tech 2035*, 18-19.
- ²² Interview with a chaplain, 10 February 2009.
- ²³ Cetron and Davies, *Tech 2035*, 19.
- ²⁴ Prepared Statement of Gen Richard G. Stillwell, USA (Ret.), Deputy Under Secretary of Defense for Policy, in Senate, *Polygraphs for Counterintelligence Purposes in the Department of Defense*, 9-10.
- ²⁵ Ibid., 23.
- ²⁶ Kleinmuntz and Szucko, "Lie Detection in Ancient and Modern Times," 768.
- ²⁷ Saxe, "Detection of Deception," 70.
- ²⁸ Kleinmuntz and Szucko, "Lie Detection in Ancient and Modern Times," 768.
- ²⁹ Prepared Statement of Gen Richard G. Stillwell, USA (Ret.), Deputy Under Secretary of Defense for Policy, in Senate, *Polygraphs for Counterintelligence Purposes in the Department of Defense*, 9.
- ³⁰ Ibid., 23.
- ³¹ Gibson, "The Truth Machine," 69.
- ³² Ibid., 63.
- ³³ Ibid.
- ³⁴ Saxe, "Detection of Deception," 70.
- ³⁵ Allen, "Not Devoid of Forensic Potential, But...", 28.
- ³⁶ National Research Council, *The Polygraph and Lie Detection*, 56.
- ³⁷ Saxe, "Detection of Deception," 70.
- ³⁸ Knight, "The Truth about Lying,"692.
- ³⁹ National Research Council, *The Polygraph and Lie Detection*, 212.
- ⁴⁰ Alton Crawford Walter Brown is the part scientist-part chef who hosts Food Network's "Iron Chef America" and "Good Eats" programs. On the latter, Brown frequently demonstrates and utilizes smart new kitchen technology

that inspired the slogan, “Science, it’s what’s for dinner.” The object described here is an infrared food thermometer.

⁴¹ Iacono, “The Forensic Application of ‘Brain Fingerprinting,’” 30.

⁴² Knight, “The Truth about Lying,” 693.

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ Rosenfeld, et al., “Simple, effective countermeasures ...,” 205-6.

⁴⁶ Iacono, “The Forensic Application of ‘Brain Fingerprinting,’” 30.

⁴⁷ Allen, “Not Devoid of Forensic Potential, But...,” 27.

⁴⁸ Ibid.

⁴⁹ Knight, “The Truth about Lying,” 694.

⁵⁰ Rosenfeld, et al., “Simple, effective countermeasures ...,” 213.

⁵¹ Knight, “The Truth about Lying,” 693.

⁵² The inspiration for this scenario came from two sources. The first was Patrick J. G. Stiennon and David M. Hoerr’s book, *The Rocket Company*. Chapter 20 of the book tells the story of a Catholic priest, Fr. Scipio, who partners with John Forsyth and AM&M Rocket Company to plant a monastery on the moon sometime around 2015-2020 (Stiennon, *The Rocket Company*, 171-182). The second was a glancing comment by *Nature* reporter Jonathan Knight in his discussion of infrared scanning which he suggests may be useful in airports and other US ports of entry, specifically to monitor responses to questions like, “Did you pack that bag yourself?” (Knight, “The Truth about Lying,” 693)

⁵³ Barrett and Gallagher, “What Sin City Can Teach Tom Ridge,” 34-55.

⁵⁴ Ibid., 49.

⁵⁵ Kroeker, “Face Recognition Breakthrough,” 18-19.

⁵⁶ Barrett and Gallagher, “What Sin City Can Teach Tom Ridge,” 45.

⁵⁷ Adam Sandler was in *Click* with Henry Winkler, who was in *Happy Days* with Ron Howard, who was in *American Graffiti* with Suzanne Somers, who was in *Three’s Company* with Ann Wedgeworth, who played the mother of John Goodman’s character, Dan, the husband of Rosanne Bar on the sitcom *Roseanne*. “TV Forum: *Roseanne* - Six Degrees of *Roseanne* Conner,” *TV.com*, <http://www.tv.com/roseanne/six-degrees-of-roseanne-conner/topic/170-693061/messages.html> (accessed April 1, 2010).

⁵⁸ Barrett and Gallagher, “What Sin City Can Teach Tom Ridge,” 45.

⁵⁹ Alder, “The Lie Detectors” xii.

⁶⁰ Holden, “Panel Seeks Truth,” 967.

⁶¹ Pavlidis, et al., “Seeing through the face of deception,” 35.

⁶² Ibid.

⁶³ Rothwell, et al., “Silent Talker,” 757-777.

⁶⁴ Ekman and O’Sullivan, “Who Can Catch a Liar?”

⁶⁵ Rothwell, et al., “Silent Talker,” 775.

⁶⁶ Ekman, “Why Don’t We Catch Liars?” 815-816.

⁶⁷ Ibid., 919.

⁶⁸ Ibid., 916.

⁶⁹ Ekman and Sullivan, “Who Can Catch a Liar?” 920.

⁷⁰ Cetron and Davies, *Tech 2035*, 21-22.

⁷¹ Bond, “A Few Can Catch a Liar, Sometimes,” 1299.

⁷² Foster, “Building Better Lie Detectors with Neuroscience?” 8.

⁷³ Kroeker, “Face Recognition Breakthrough,” 19.

⁷⁴ Cetron and Davies, *Tech 2035*, 18.

⁷⁵ Ibid. Dr. Cetron explains a petaflop equals 10¹⁵ floating point operations per second.

⁷⁶ Cetron and Davies, *Tech 2035*, 18.

⁷⁷ Silbergliet, et al., *The Global Technology Revolution 2020, In-Depth Analysis*, xix.

⁷⁸ Cetron and Davies, *Tech 2035*, 19.

⁷⁹ Tsiamyrtzis, et al., “Imaging Facial Physiology for the Detection of Deception,” 213.

⁸⁰ “Facial Expressions,” 8.

- ⁸¹ Coates, "The Future of the Web," 2.
- ⁸² Krüger and Malaka, "Artificial Intelligence Goes Mobile," 469.
- ⁸³ Verne, *Philosophy and the Return to Self- Knowledge*, 80. (Also referred to in Alder, *The Lie Detectors*, " 12.)
- ⁸⁴ National Research Council, *The Polygraph and Lie Detection*, 19.
- ⁸⁵ Alder, *The Lie Detectors*, " 227.
- ⁸⁶ Kleinmuntz and Szucko, "Lie Detection in Ancient and Modern Times," 775.
- ⁸⁷ Alder, *The Lie Detectors*, " xiv.
- ⁸⁸ National Research Council, *The Polygraph and Lie Detection*, 55.
- ⁸⁹ Alder, *The Lie Detectors*, " xiv.
- ⁹⁰ Holden, "Panel Seeks Truth," 967.
- ⁹¹ Gibson, "The Truth Machine," 61
- ⁹² Interview with an AFOSI Special Agent, 3 April 2010.
- ⁹³ *Ibid.*, xii.

Bibliography

- Alder, Ken. *The Lie Detectors: The History of an American Obsession*. New York, NY: Free Press, 2007.
- Allen, John J. B. "Not Devoid of Forensic Potential, But..." *The American Journal of Bioethics*, vol. 8, no. 1 (2008): 27-28.
- Bond, Charles F., Jr. "A Few Can Catch a Liar, Sometimes: Comments on Ekman and O'Sullivan (1991), As Well As Ekman, O'Sullivan, and Frank (1999)." *Applied Cognitive Psychology*, vol. 22 (2008): 1298-1300.
- Barrett, Larry and Sean Gallagher. "Case 113 Las Vegas Casinos: What Sin City Can Teach Tom Ridge." *Baseline* (April 2004): 34-55
- Cetron, Dr. Marvin J., and Owen Davies. *The Proteus Monograph Series*. Vol 2, issue 2. Tech 2035: Future Technology, Future Power in Asia, and Future Intelligence Challenges. Carlisle, PA: Proteus USA, September 2008.
- Coates, Joseph. "The Future of the Web." *The World & I—The Magazine for Lifelong Learners*. (April 2002): 1-3.
- Coates, Joseph F. "An Overview of Futures Methods." In *The Knowledge Base of Future Studies*. Vol. 2, *Organizations, Practices, Products*, edited by Richard Slaughter, 57-75. Hawthorne, Australia: DDM Media Group, Futures Study Centre, 1996.
- Daniels, Les. *Wonder Woman, the Complete History*. San Francisco, CA: Chronicle Books LLC, 2000.
- Ekman, Paul. "Why Don't We Catch Liars?" *Social Research*, vol. 63, no. 3 (Fall 1996): 801-817.
- Ekman, Paul and Maureen O'Sullivan. "Who Can Catch a Liar?" *American Psychologist*, vol. 46, no. 9 (September 1991): 913-920.
- "Facial Expressions." *Science and Children*, (November 2009): 8-9.
- Foster, Kenneth R. "Building Better Lie Detectors with Neuroscience?" *IEEE Spectrum* (July 2005): 8.
- Gibson, Margaret. "The Truth Machine: Polygraphs, Popular Culture and the Confessing Body." *Social Semiotics*, vol. 11, no. 1 (2001): 61-73.
- Glenn, Jerome C. "Chapter 14: Participatory Methods. In *Futures Research Methodology – V2.0*, edited by Jerome C. Glenn and Theodore J. Gordon, 1-32. New York, NY: American Council for the UNU, 1 August 2003. CD-ROM

- Holden, Constance. "Panel Seeks Truth in Lie Detector Debate." *Science*, vol. 291, issue 5506 (9 February 2001): 967-972.
- Iacono, William G. "The Forensic Application of 'Brain Fingerprinting': Why Scientists Should Encourage the Use of P300 Memory Detection Methods." *The American Journal of Bioethics*, vol. 8, no. 1 (January 2008): 30-32.
- Klaver, Jessica R., Zina Lee, Alicia Spidel and Stephen D. Hart. "Psychopathy and deception using indirect measures." *Legal and Criminological Psychology*, no. 14 (2009): 171-182.
- Kleinmuntz, Benjamin and Julian J. Szucko. "Lie Detection in Ancient and Modern Times: A Call for Contemporary Scientific Study." *American Psychologist*, vol. 39, no. 7 (July 1984): 766-776.
- Knight, Jonathan. "The Truth about Lying." *Nature*, vol. 428, issue 6984 (15 April 2004): 692-694.
- Kroeker, Kirk L. "Face Recognition Breakthrough." *Communications of the ACM*, vol. 52, no. 8 (August 2009): 18-19.
- Krüger, Antonio and Rainer Malaka. "Artificial Intelligence Goes Mobile." *Applied Artificial Intelligence*, vol. 18, no. 469 (2004): 469-475.
- Lock, Carrie. "Deception Detection." *Science News*, vol. 66, no. 5 (July 31, 2004): 72-73.
- National Research Council. *The Polygraph and Lie Detection*. Washington, D.C.: The National Academies Press, 2003.
- Pavlidis, Ioannis, Norman L. Eberhardt, and James A. Levine. "Seeing through the face of deception." *Nature*, vol. 415 (3 January 2002): 35.
- The Polygraph Museum. "John Larson's Breadboard Polygraph." Ball & Gillespie Polygraph. <http://www.lie2me.net/the-polygraph-museum/id16.html> (accessed 26 March 2010).
- Rosenfeld, J. Peter, Matthew Soskins, Gregory Bosh, and Andrew Ryan. "Simple, effective countermeasures to P300-based tests of detection of concealed information." *Psychophysiology*, vol. 41 (2004): 205-219.
- Rothwell, Janet, Zuhair Bandar, James O'Shea, and David McLean. "Silent Talker: A New Computer-Based System for the Analysis of Facial Cues to Deception." *Applied Cognitive Psychology*, vol. 20 (2006): 757-777.
- Saxe, Leonard. "Detection of Deception: Polygraph and Integrity Tests." *Current Directions in Psychological Science*, vol. 3, no. 3 (June 1991): 69-73.
- Silberglitt, Richard, Philip S. Antón, David R. Howell, and Anny Wong, Natalie Gassman, Brian A. Jackson, Eric Landree, Shari Lawrence Pfleeger, Elaine M. Newton, and Felicia

Wu. *The Global Technology Revolution 2020, In-Depth Analysis: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*. Santa Monica, CA: Rand Corporation, 2006.

Singel, Kati. "Origin of the Modern Polygraph." University of Mary Washington.
http://www.umw.edu/hisa/resources/Student%20Projects/Singel/students.umw.edu/_ksing2os/polygraph/origin.html (accessed March 26, 2010).

Stiennon, Patrick J. G., and David M. Hoerr. *The Rocket Company*. Reston, VA: American Institute of Aeronautics and Astronautics, Inc., 2005.

Tsiamyrtzis, P., J. Dowdall, D. Shastri, I. T. Pavlidis, M. G. Frank, and P. Eckman. "Imaging Facial Physiology for the Detection of Deception." *International Journal of Computer Vision*, vol 71, no. 2 (2007): 197-214.

US Senate. *Polygraphs for Counterintelligence Purposes in the Department of Defense: Hearing before the Committee on Armed Services*. 98th Cong., 2d sess., 7 March 1984.

Verne, Donald Phillip. *Philosophy and the Return to Self-Knowledge*. New Haven, CT: Yale University, 1997.