NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DETECTING DECEPTION IN THE WILDERNESS: A PROPOSAL OF WARFARE INTEGRATED LIE DETECTION SYSTEM (WILDS)

by

Ayesha Ahmad

June 2021

Thesis Advisor: Shannon C. Houck
Second Reader: Edward L. Fisher

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
DETECTING DECEPTION IN THE WILDERNESS: A PROPOSAL OF WARFARE INTEGRATED LIE DETECTION SYSTEM (WILDS)

5. FUNDING NUMBERS

6. AUTHOR(S) Ayesha Ahmad

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Currently, the Marine Corps and the Department of Defense do not leverage human-machine team pairing during the collection of human intelligence. Consequently, they may miss or not exploit key information gained from human sources during times of both peace and war. This research aims to examine the viability of leveraging human-machine team pairing during intelligence gathering operations with particular focus on detecting human deception. It provides an in-depth overview of the current unclassified practices used to detect deception, evaluates the viability of incorporating emerging technologies, and proposes an operator function model and employment model for a human-machine team pair to improve deception detection performance during enemy prisoners of war interviews.

14. SUBJECT TERMS human-machine team pairing, human intelligence, counter-intelligence	**15. NUMBER OF PAGES** 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

DETECTING DECEPTION IN THE WILDERNESS: A PROPOSAL OF WARFARE INTEGRATED LIE DETECTION SYSTEM (WILDS)

Ayesha Ahmad
Captain, United States Marine Corps
BS, U.S. Naval Academy, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Shannon C. Houck
Advisor

Edward L. Fisher
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Currently, the Marine Corps and the Department of Defense do not leverage human-machine team pairing during the collection of human intelligence. Consequently, they may miss or not exploit key information gained from human sources during times of both peace and war. This research aims to examine the viability of leveraging human-machine team pairing during intelligence gathering operations with particular focus on detecting human deception. It provides an in-depth overview of the current unclassified practices used to detect deception, evaluates the viability of incorporating emerging technologies, and proposes an operator function model and employment model for a human-machine team pair to improve deception detection performance during enemy prisoners of war interviews.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AK-47	Avtomat Kalashnikov Model 1947
ANOVA	Analysis of Variance
BCI	Brain Computer Interface
CI	Counterintelligence
CSE	Cognitive Systems Engineering
DOD	Department of Defense
DoDD	Department of Defense Directive
EEG	Electroencephalogram
EPW	Enemy Prisoners of War
F-35	Fighter Aircraft 35
FM	Field Manual
FMRI	Functional Magnetic Resonance Imaging
FNIRS	Functional Near-Infrared Spectroscopy
HUMINT	Human Intelligence
HMT	Human Machine Team
IC	Intelligence Community
ICD	Intelligence Community Directive
JP	Joint Publication
LIWC	Linguistic Inquiry and Word Count
MCWP	Marine Corps Warfighting Publication
MP	Military Police
NLP	Natural Language Processing
OFM	Operator Function Model
POW	Prisoners of War
UAS	Unmanned Aerial System
UCMJ	Uniformed Code of Military Justice
US	United States
WILDS	Warfare Integrated Lie Detection System

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge my thesis advisor, Dr. Shannon Houck, for spending countless hours answering my questions and making sure that I was somewhere near the right path to accomplish this. Additionally, I want to extend a special thank you to my loving and encouraging family and friends who, without their patience and persistence, this thesis would still be a good idea in my head rather than a completed work. Finally, thank you to God for putting me on this path and letting me rise to the challenge.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

All warfare is based on deception.

—Sun Tzu, *Art of War*

War is deceit.

—Prophet Muhammad

A. PURPOSE

Detecting deception is a difficult task for a human to do accurately. Though there have been mixed results in studies, on average, people can only detect deception about 50% of the time.[1] This statistic does not change for intelligence operations conducted by military professionals. Currently, the techniques and procedures implemented by the military call for the utilization of the information gained or verified by enemy prisoners of war to conduct continuing operations. Due to the accuracy of current practices for detecting deception there is a certain level of risk associated with acting upon the knowledge gained through the interrogations or conversations with hostile combatants. Reducing this risk by improving deception detection accuracy could lead to more successful tactical engagements. To accomplish this, artificial intelligence (AI) and other technological advancements may provide an opportunity to leverage human-machine team pairing during intelligence gathering operations.[2] Currently, the Marine Corps and the Department of Defense (DOD) do not optimally employ human-machine team pairing during the collection of

[1] Shannon C. Houck et al., "When Beliefs Lead to (Im)Moral Action: How Believing in Torture's Effectiveness Shapes the Endorsement of Its Use," *Political Psychology* 40, no. 6 (2019): 1315–39, https://doi.org/10.1111/pops.12590; Aldert Vrij et al., "Psychological Perspectives on Interrogation," *Perspectives on Psychological Science* 12, no. 6 (November 2017): 927–55, https://doi.org/10.1177/1745691617706515; Verónica Pérez-Rosas et al., "Deception Detection Using Real-Life Trial Data," in *Proceedings of the 2015 ACM on International Conference on Multimodal Interaction,* Seattle, WA, USA: ACM, 2015, 59–66, https://doi.org/10.1145/2818346.2820758.

[2] Pérez-Rosas et al., "Deception Detection Using Real-Life Trial Data"; Judee Burgoon et al., "Detecting Deception in the Military Infosphere: Improving and Integrating Human Detection Capabilities with Automated Tools," Report Number AFRL-SR-AR-TR-07-0193 (Arlington, VA: AF Office of Scientific Research, April 25, 2007), https://www.researchgate.net/publication/235028335_Detecting_Deception_in_the_Military_Infosphere_Improving_and_Integrating_Human_Detection_Capabilities_with_Automated_Tools/link/0f31752e68cf733e76000000/download.

human intelligence (HUMINT).[3] Consequently, the Marine Corps and the DOD may miss and therefore not exploit key information gained from human sources during times of peace and war.

The purpose of this study is threefold. First, this thesis provides an in-depth overview of the current unclassified practices the intelligence communities (IC), the DOD, and the Marine Corps use to detect deception during operations. Second, this thesis will evaluate the potential benefits of leveraging human-machine team pairing to detect deception during intelligence gathering operations. Third, it will propose a method of integrating the current emerging technologies to aid human operators in human deception detection during interrogations and interviews.

B. RELEVANCE

Throughout history, deception has played a key role in gaining a strategic advantage on the battlefield, from the trojan horse used by the Greeks to Operation OVERLORD during World War II.[4] When militaries achieve deception, they gain an advantage over their enemies. For militaries to deny their enemies this advantage and prevent deception from contaminating intelligence, there is a requirement for accurate intelligence collection and assessments. One of the most informative lines of intelligence is HUMINT. However, humans that provide such intelligence often employ deception tactics such as lying and evasiveness. Therefore, to effectively inform intelligence operations it is critical to detect when a person is lying or being evasive. One potential way to detect deception accurately would be the employment of technological advances.[5]

The advent of the personal computer and other information technologies has caused a fundamental shift in warfare. From the integration of software in the F-35, to the use of unmanned aerial systems (UAS), to the use of computers as diagnostic gear for vehicles, technological advancements across battlespaces have worked to modernize and optimize the battlefield. These

---

[3] S. Keller-McNulty, "Quest for Truth: Deception and Intent Detection," (Ft. Belvoir, VA: The MITRE Corporation; JASON Program Office, October 29, 2008), https://fas.org/irp/agency/dod/jason/quest.pdf; Richard Potember, "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DOD" (Alexandria, VA: The MITRE Corporation; JASON Program Office, January 2017), https://fas.org/irp/agency/dod/jason/ai-dod.pdf.

[4] William B Breuer, *Hoodwinking Hitler: The Normandy Deception* (Westport: Praeger Publishers, 1993).

[5] Keller-McNulty, "Quest for Truth: Deception and Intent Detection."

technologies, when employed correctly, have mitigated risks for friendly forces and civilian personnel. The human counterintelligence (CI) field is one area within the warfighting domain that seems untouched by these new advances. The DOD, and the Marine Corps, should identify the requirements for private industry to design new technologies for integration into HUMINT operations, as they have the potential to give the force an asymmetric advantage.

C. METHODOLOGY AND SCOPE

The research methodologies this thesis employs ties directly to its purposes. The first purpose as outlined above, provides an in-depth overview of the current unclassified practices the intelligence communities within the DOD and the Marine Corps use to detect deception during operations. It will do this through an in-depth review of Joint Publications (JP), Marine Corps and Army service doctrine, and Intelligence Community Directive (ICD)-203. The second purpose of this thesis will be to evaluate the potential benefits of leveraging human-machine team pairing to detect deception during human intelligence gathering operations. To accomplish this, I examine (a) the methodologies used to conduct interviews and interrogations, (b) the most current technologies proven to increase the accuracy in detecting deception, and (c) the trust relationship between humans and machines. The third purpose is to propose a method of integrating the current emerging technologies to aid human operators in the detection of deception during interrogations and interviews. This proposal will consist of two models, an employment model, and a system design model. The employment model's design gives initial insights into appropriate roles and responsibilities for human and machine agents, within the developed system, Warfare Integrated Lie Detection System (WILDS). The proposed system design is based on an operator function model (OFM), stemming from a human factors systems engineering approach.

There are three major approaches to detecting deception: human only, machine only, and a mix of human and machine paired together. While there is a vast amount of research pertaining to human-only and machine-only deception detection, this study focuses on their combined use, human-machine team pairing. Human-only techniques and machine-only techniques will be discussed but remain outside the scope of this research. This study focuses primarily on integrating currently existing non-invasive technology and algorithms into a joint cognitive system that includes both human and machine agents. To investigate, I draw on two major themes within the

discipline of psychology: 1) the development of trust between humans and machines; and 2) the impact of interview styles during interrogations.

D. CHAPTER OVERVIEW

This thesis includes five chapters. The first chapter provides an overview of the problem, its relevance, and then discusses the scope of study. The second chapter identifies the DOD's and Marine Corps' current approach to deception detection. Additionally, it explores the current tactics, techniques, and procedure implemented by military police (MP), interrogators, and intelligence gathering professionals. It identifies a heavy focus on human-only deception detection methodologies, through interviewing styles, while also providing employment strategies for older less reliable technologies such as the polygraph. Employing this approach towards deception detection, requires the acceptance of a higher-than-necessary risk for tactical leaders. Because there have been technological advances made towards accurately identifying deception, the Marine Corps and the DOD should employ that technology to reduce the risk which tactical leaders must accept on the battlefield. The scholarly works reviewed provides an understanding of the enabling technologies including sensors, algorithms, and the human components needed for the proposed deception detection system.

The third chapter details the proposed integrated deception detection system designed for use with detainee interrogations by the Marine Corps, WILDS, and its proposed employment model. The proposed system takes a cognitive systems engineering modeling approach, to create an OFM. The approach selected enables us to model human-machine interaction, human-human interaction, and the overall system. Other approaches and models to design a system failed to consider either the human element, the machine element, or where the human and machine elements overlapped. Additionally, this model will help identify potential design flaws, training requirements, and qualification standards associated with the human role in automated deception detection.

The fourth chapter provides a detailed analysis of OFM employment with specific focus on key roles and responsibilities of humans and machines. This chapter will also discuss the potential benefits and limitations. Finally, Chapter V presents the conclusions and recommendations for further research into this topic.

II. STATE OF THE FIELD

A. CURRENT MILITARY APPROACH TO DECEPTION DETECTION

1. Department of Defense / U.S. Army Doctrine

International Law, Joint and Service level doctrine provide insight into the DOD's current approach to detecting deception. The Geneva Conventions and various Joint and Army publications provide relevant information regarding the rights of prisoners of war, the detention process, and current practices used by DOD intelligence personnel to gather information. Additionally, these publications provide current deception detection methodologies which assist in the collection of valuable information.

a. Geneva Conventions

The Geneva Conventions are international treaties which govern how members of the treaties will conduct warfare, and the rights of those who engage in warfare.[6] There are four articles of the Geneva Conventions which apply to prisoners of war. JP 3-63 explains these four articles and their application to the Joint Forces.

> (1) Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GWS) (2) Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea (3) The Geneva Convention Relative to the Treatment of Prisoners of War (GPW)… (4) The Geneva Convention Relative to the Protection of Civilian Persons in Time of War (GC).[7]

Article 1 details the protections for those who were previously engaging in hostile actions on the battlefield, but due to injury or illness, they are no longer actively hostile. Additionally, it sets forth the rights for the collection of human remains and prohibits their abuse. Article 2 details the protections for those shipwrecked. It requires the humane treatment and rescue of persons at sea and the procedure for death at sea. Article 3 details the rights of enemy prisoners of war (EPW),

---

[6] Joint Chiefs of Staff, *Detainee Operations*, JP 3-63 (Washington, DC: Joint Chiefs of Staff, 2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_63.pdf.

[7] Joint Chiefs of Staff, 15.

regulating their detention, facilities and treatments. Article 4 details the rights of civilians detained due to enemy actions. This article applies when non-state actors are involved in hostile actions. Articles 3 and 4 clearly prohibit the use of torture on any EPW or any persons detained by those adhering to the treaty.

There are two major implications from this. First is that prisoners of war (POW's) have rights that the U.S. must adhere to by International Law. Torture is strictly prohibited.[8] Second, to expect an enemy to treat our friendly forces with dignity and respect, we must afford their detainees basic human rights. Not only does this foster a moral high ground, but to some degree, it provides a level of protection for friendly forces engaged in combat operations.

b. Joint Publication's 3–63: Detainee Operations

Joint Publication 3-63, *Detainee Operations,* initially provides a background and legal considerations for the detainee operations. It then goes on to explain the detainee categories, as illustrated in Figure 1, defining each category subsequently.

> The word "detainee" include any person captured, detained, or otherwise under the control of DOD personnel…Belligerent: a person who is engaged in hostilities against the U.S. or its multinational partners during an armed conflict…Privileged belligerents are EPWs upon capture, and are entitled to combatant immunity for their lawful pre-capture war-like acts…Unprivileged enemy belligerents are belligerents who do not qualify for the distinct privileges of combatant status…Retained Personnel. An individual who is described by Article 28 of the GWS and Article GPW and who is in the custody or control of DOD. Personnel who into the following categories: official med personnel of the armed forces of the parties to the conflict…Civilian Internee. Any civilian, including those described by Article 4 of GC, who is in the custody or control of DOD during an armed conflict or occupation, such as those held for imperative reasons of security or protection. [9]

Following the defining of detainee categories JP 3-63 proceeds to explains the processes relating to the conduct of detainee operations, including the capture, screening processes, and the disposition, classification, and approval process. It is through this process by which intelligence

---

[8] Joint Chiefs of Staff, *Detainee Operations*.

[9] Joint Chiefs of Staff, 17.

personnel have access to the detainees and begin to assess if gathering viable intelligence information is possible.

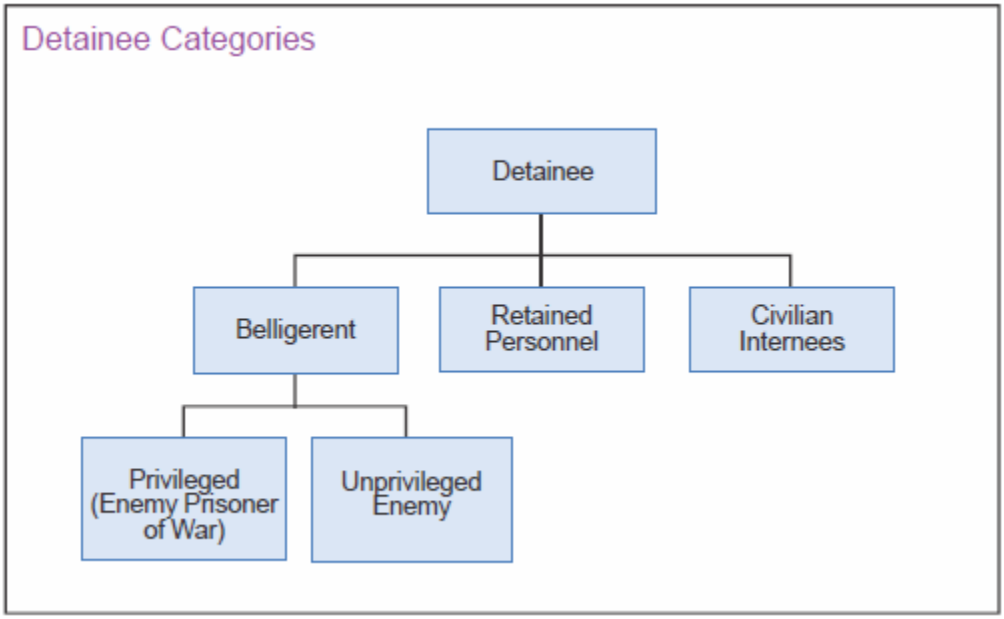

Figure 1. Detainee Categories[10]

c. U.S. Army Field Manual 2-22.3: Human Intelligence Collection Operations

The U.S. Army Field Manual 2-22.3 (FM 2-22.3), *Human Intelligence Collection Operations*, provides three primary points of discussion. First, it provides an overview of the entire HUMINT process. Second, it provides the current recommendations for approach techniques and questioning methodologies. Finally, it provides insight into how to detect deceit.

The HUMINT collections process begins with screening. Essentially, all human sources have the potential to provide valuable information during times of warfare. The screening process not only identifies who may have the requisite knowledge; that friendly forces are seeking, but also who may be willing to share that information. After the screening process, an intelligence professional proceeds with collection planning and preparation informed by research. The research conducted usually pertains to background information regarding the interviewee, operational

[10] Source: Joint Chiefs of Staff, 17.

information, or basic verifiable information. The collections plan includes the approach, the questioning methodology, and resources necessary to verify all information gathered.[11] The final preparations are typically administrative items such as coordination for an interview room, coordination to use a polygraph, obtaining any equipment necessary, or coordinating the use of an interpreter. After completing the planning phase, the intelligence professional moves into the execution phase, which includes the actual approach, questioning, and reporting. The collections process ends with an analysis of the information gained, and the application of it for follow-on operations.

FM 2-22.3 states the objective of the approach phases is: "to establish a relationship with the source [detainee] that results in the source providing accurate and reliable information in response to the HUMINT collector's questions." [12] Importantly, it emphasizes the necessity to build rapport with the detainee and provides various approach methodologies to do so. Once the intelligence professional has built rapport with the detainee, various questioning approaches can be taken to gain intelligence information. Listed below are the various questioning approaches with a brief description.

- Direct Approach- Essentially, this approach begins with control-type questions and then transitions to pertinent questions posed.[13]
- Incentive Approach- This approach has the collector trade something the source wants for the information given.[14]
- Emotional Approaches- These set of approaches use emotional vulnerabilities to gain information. Typically, interviewers leverage incentives.[15]

---

[11] Department of the Army, *Human Intelligence Collector Operations*, FM 2-22.3 (Washington, DC: Department of the Army, 2006), 133, https://fas.org/irp/doddir/army/fm2-22-3.pdf.

[12] Department of the Army, 140.

[13] Department of the Army, 144.

[14] Department of the Army, 145.

[15] Department of the Army, 146.

- We Know All- Interviewer suggest to the detainee that they are already aware of the information provided.[16]
- File and Dossier-The interviewer prepares a file which has an excess of information to present in the interview. When paired with We Know All and extensive research it can be effective.[17]
- Repetition- Used to induce cooperation from hostile detainee, essentially asking the same question continuously until the detainee answers.[18]
- Rapid Fire- Multiple interviewers asking questions rapidly to cause flustering in the detainee which may result in detailed explanation.[19]
- Silent- Interviewer uses silence to make the detainee speak due to discomfort.[20]
- Change of Scenery- Moving the detainee from either an intimidating atmosphere to one of less intimidation, or the reverse.[21]
- Mutt and Jeff- Using two interviewers with opposite dispositions to create a situation where the detainee builds rapport with one of them.[22]
- False Flag- Interviewer poses as a non-U.S. military personnel to gain cooperation.[23]

---

[16] Department of the Army, 152.

[17] Department of the Army, 153.

[18] Department of the Army, 154.

[19] Department of the Army, 154.

[20] Department of the Army, 154.

[21] Department of the Army, 155.

[22] Department of the Army, 155.

[23] Department of the Army, 156.

From the list of approaches, we notice that all but the direct approach relies on emotional based techniques to manipulate the detainee's willingness to share information. Relying heavily on emotional control by the interviewer presents challenges. These challenges include loss of control due to detainee actions or inactions, extreme stress due to warfare conditions, and other situational causations. The consequences can include bolstering the detainee unwillingness to respond, loss of established rapport, or even the accidental use of torture methods.[24]

FM 2-22.3 explains that within the various approaches there are different types of questions including, initial, follow-up, non-pertinent repeat, control, and prepared.[25] Each type of question has a purpose relating to the gathering of information. Additionally, it suggests avoiding leading, negative, compound, and vague questions.[26]

Finally, FM 2-22.3 details a framework for how to detect deception with examples of application.

- Repeat and control questions.
- Internal inconsistencies. Frequently when a source is lying, the HUMINT collector will be able to identify inconsistencies in the timeline, the circumstances surrounding key events, or other areas within the questioning. For example, the source may spend a long time explaining something that took a short time to happen, or a short time telling of an event that took a relatively long time to happen. These internal inconsistencies often indicate deception.
- Body language does not match verbal message. An extreme example of this would be the source relating a harrowing experience while sitting back in a relaxed position. The HUMINT collector must be careful in using this clue since body language is culturally dependent. Failing to make eye contact in the U.S. is considered a sign of deceit while in some Asian countries it is considered polite.
- Knowledge does not match duty position or access. Based on the source's job, duty position, or access the HUMINT collector should have developed a basic idea of the type and degree of information that an individual source should know. When the source's answers show that he does not have the expected level of information (too much or too little or different information than expected), this may be an indicator of deceit. The HUMINT collector needs to determine the source of unexpected information.

---

[24] Vrij et al., "Psychological Perspectives on Interrogation."

[25] Department of the Army, *Human Intelligence Collector Operations*.

[26] Department of the Army.

- Information is self-serving. Reporting of information that is self-serving to an individual or his group should be suspect. For example, a member of one ethnic group reporting generic atrocities by an opposing ethnic group or a source reporting exactly the right information needed to receive a promised incentive should be suspect. That is not to say that the information is necessarily false, just that the HUMINT collector needs to be sure to verify the information.
- Lack of extraneous detail. Often false information will lack the detail of truthful information, especially when the lie is spontaneous. The HUMINT collector needs to ask follow-up questions to obtain the detail. When the source is unable to provide the details that they should know, it is an indicator of deceit. If the source does provide this additional information, it needs to be checked for internal inconsistencies and verified by repeat questions.
- Repeated answers with exact wording and details. Often if a source plans on lying about a topic, he will memorize what he is going to say. If the source always relates an incident using exactly the same wording or answers repeat questions identically (word for word) to the original question, it may be an indicator of deceit. In an extreme case, if the source is interrupted in the middle of a statement on a given topic, he will have to start at the beginning in order to "get his story straight."
- Source appearance does not match story. If the source's physical appearance does not match his story, it may be an indication of deceit. Examples of this include the source who says he is a farmer but lacks calluses on his hands or the supposed private who has a tailored uniform.
- Source's language usage does not match story. If the type of language, including sentence structure and vocabulary, does not match the source's story, this may be an indicator of deceit. Examples of this include a farmer using university level language or a civilian using military slang.
- Lack of technical vocabulary. Every occupation has its own jargon and technical vocabulary. If the source does not use the proper technical vocabulary to match his story, this may be an indicator of deceit. The HUMINT collector may require the support of an analyst or technical expert to identify this type of deceit.
- Physical cues. The source may display physical signs of nervousness such as sweating or nervous movement. These signs may be indicators of deceit. The fact that an individual is being questioned may in itself be cause for some individuals to display nervousness. The HUMINT collector must be able to distinguish between this type of activity and nervous activity related to a particular topic. Physical reaction to a particular topic may simply indicate a strong emotional response rather than lying, but it should key the HUMINT collector to look for other indicators of deceit.
- Failure to answer the question asked. When a source wishes to evade a topic, he will often provide an answer that is evasive and not in response to the question asked. For example, if the source is asked, "Are you a member of the insurgent organization?" and he replies, "I support the opposition party in the legislature," he has truthfully answered a question, but not the question that was

asked. This is a subtle form of deceit since the source is seemingly cooperative but is in fact evading providing complete answers.[27]

We can draw two primary conclusions from this evidence. First, the DOD has various ways of approaching and questioning a detainee. However, the majority of these tactics use emotion-based logic, to persuade the detainee to provide information. Second, the interviewer has three tasks to accomplish simultaneously in an interview; control of the situation, gain pertinent information, and detect any deception which the detainee maybe attempting.

2. Marine Corps

The Marine Corps adheres to all the tactics and procedures outlined in the previous section. In addition to complying with the Joint Doctrine the Marine Corps has its own doctrine, Marine Corp Warfighting Publication 2–6 (MCWP 2-6), *Counterintelligence.* The Marine Corps traditionally operates as a component of the Joint Force. Because of the legal and sensitive nature of detention operations, most interviews occur at joint detention facilities, run by the U.S. Army. As such, the Marine Corps' primary role is typically conducting tactical CI.[28] This is the process by which the initial screening occurs after capture. Upon the transfer of the detainee from the care of the Marines into the care of the detention facility, the information collected during the tactical CI interview informs further HUMINT operations. Specifically, this information informs joint-level intelligence professionals on which detainees maybe the best candidates for further questioning.

3. Intelligence Community Directive (ICD) -203

ICD-203 is a directive given to all intelligence professionals by the Director of National Intelligence. Designed to standardize the intelligence analyst's products across all communities, it contributes to analysis and products produced by intelligence professionals. The directive "establishes the Intelligence Community Analytic Standards that govern the production and evaluation of analytic products; articulates the responsibility of the intelligence analysts to strive

---

[27] Department of the Army, 168–70.

[28] US Marine Corps, *Counterintelligence*, MCWP 2-6 (Quantico, VA: U.S. Marine Corps, 2004), 109–12, https://www.marines.mil/Portals/1/Publications/MCWP%202-6%20W%20Erratum%20Counterintelligence.pdf.

for excellence, integrity, and rigor in their analytic thinking and work practices."[29] Additionally, the directive establishes two primary outputs: a likelihood or probability level and a confidence level. The likelihood level is a measurement of an event occurring. Table 1 is the example provided in ICD-203 illustrating three examples of assessing the likelihood/probability levels.[30] The table presents seven categories of likeliness for an event to occur and three options on how an analysist can verbalize the assessment, in chance, in probability, and in assigned percentages. This enables the analyst to present the information in either a qualitative or quantitative form. The second category is the confidence level. The confidence level provides the user and indication on the logic behind why the analysts assigned a probability level. The assessment of the confidence level can be based on the types of sources used in gathering the information, the timeliness of the information gathered, or the even the gathering processes used. Combining these two outputs together gives the user of the intelligence information gathered two standards by which they can rely on the information provided to them. HUMINT intelligence products comply with these standards, including those produced during detainee operations.

Table 1. Likelihood Metric[31]

almost no chance	very unlikely	unlikely	roughly even chance	likely	very likely	almost certain(ly)
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Now that we have a better understanding of the DOD's and Marine Corps' doctrine relating to deception detection, we can analyze how this doctrine was established.

[29] Director of National Intelligence, *Analytic Standards*, IC Directive 203 (Washington, DC: Office of the Director of National Intelligence, 2015), 1, https://fas.org/irp/dni/icd/icd-203.pdf.

[30] Director of National Intelligence, 3.

[31] Adapted from Director of National Intelligence, 3.

B. HISTORICAL DECEPTION DETECTION AND THE POLYGRAPH

History provides a strong foundation to analyze how the current practices developed overtime. So, how did the IC, DOD, and Marine Corps arrive with these standards for detainee operations and deception detection methodologies? To answer this within the next section, we review historic interviewing methodologies used by the IC, DOD, and Marine Corps and the history and current doctrine of the polygraph.

1. Interviewing Methodologies

Previous scholarship outlines varying methodologies to elicit information from a detainee. I summarize those most commonly discussed in the literature along with the most commonly used practices. These include physical coercion (torture), psychological coercion (the Reid model), and rapport-based strategies (PEACE model and cognitive interview).

a. Physical Coercion

Torture is legally defined as, "specifically intended to inflict severe physical or mental pain or suffering."[32] The term "severe" is further defined as "excruciating or agonizing pain or pain equivalent in intensity to the pain accompanying serious physical injury such as organ failure, impairment of bodily function or even death."[33] Concurrent medical definition of torture is "an act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person, for a purpose such as obtaining information or confession, punishment, intimidation, coercion, or for any reason based on discrimination of any kind."[34] As we can see there are differences between what medical professionals and legal professionals consider torture. There is also subjectivity relating to what constitutes pain, physical or mental, for individuals. For these reasons, it is difficult in some cases to define what does and does not constitute acts of torture. To best apply both of these definitions into a single concept, we define torture as the process by which force, or the threat of force is used in order to elicit information from a detained person.

---

[32] "Definition of Torture," 18 § 2340–2340A (2004), https://www.justice.gov/file/18791/download.

[33] Definition of Torture.

[34] Jay W. Marks, "Medical Definition of Torture," MedicineNet, June 3, 2021, https://www.medicinenet.com/torture/definition.htm.

Throughout history torture has been used for three primary purposes; to illicit a fear response which will produce "valuable" information, to intimidate, and to create propaganda.[35] As such, torture conducted by uniformed personnel is strictly prohibited by International Law, covered in the Geneva Conventions as well as Joint Publications, and service doctrine.[36] The use of torture not only is subject to punishment by the UCMJ but it is also considered a war crime and can therefore can be adjudicated by the International Criminal Courts. Additionally, various studies have shown that the use of torture is an ineffective way of gaining information, despite popular opinion.[37] This is inclusive of combating insurgencies, attempting to protect friendly forces, and for the purposes of major combat operations.[38] We see each use of torture being ineffective through analyzing the effects of Operation TEARDROP during World War II, Operation Condor in the 1970s, and the Abu Ghraib incident during the Iraq War. It is for these various reasons that the use of torture during the conduct of CI operations is not only illegal but unproductive.

b. Psychological Coercion

A step up from physical coercion is psychological coercion. Essentially, this the process by which no physical contact occurs, but rather the are questions asked and psychological pressure put on a detainee elicits information. One of the primary models used to create this psychological pressure is the Reid Model. Though this model can be employed by the IC, DOD, and Marine

---

35 Vrij et al., "Psychological Perspectives on Interrogation."

36 Department of the Army, *Human Intelligence Collector Operations*; U.S. Marine Corps, *Counterintelligence*; Joint Chiefs of Staff, *Detainee Operations*.

37 Vrij et al., "Psychological Perspectives on Interrogation"; Houck et al., "When Beliefs Lead to (Im)Moral Action"; Joeann M. Salvati and Shannon C. Houck, "Examining the Causes and Consequences of Confession-Eliciting Tactics during Interrogation," *Journal of Applied Security Research* 14, no. 3 (July 3, 2019): 241–56, https://doi.org/10.1080/19361610.2019.1621508; Christopher Michael Sullivan, "The (in)Effectiveness of Torture for Combating Insurgency," *Journal of Peace Research* 51, no. 3 (May 1, 2014): 388–404, https://doi.org/10.1177/0022343313520023; Ronnie Janoff-Bulman, "Erroneous Assumptions: Popular Belief in the Effectiveness of Torture Interrogation," *Peace and Conflict: Journal of Peace Psychology* 13, no. 4 (November 2007): 429–35, http://dx.doi.org.libproxy.nps.edu/10.1080/10781910701665766.

38 Janoff-Bulman, "Erroneous Assumptions"; Salvati and Houck, "Examining the Causes and Consequences of Confession-Eliciting Tactics during Interrogation"; Houck et al., "When Beliefs Lead to (Im)Moral Action"; Sullivan, "The (in)Effectiveness of Torture for Combating Insurgency"; Vrij et al., "Psychological Perspectives on Interrogation."

Corps, in recent years the influence of scholarly work has reduced its use. The Reid Model is an accusatorial method which has three parts: factual analysis, interviewing, and interrogation. During the factual analysis, the interviewer asks standard questions to establish a control reference of the detainee's behavior, as well as basic facts of event occurrence. Following that is a behavior analysis interview. The interviewer's task is to purposefully cause the detainee to lie or tell the truth. They observe any changes in physical or language pattern characteristics which the detainee displays. Once the interviewer has observed behavioral pattern changes not associated with the relevant event, they can transition to the interrogation stage. The purpose of this stage is to gain information which the detainee has but the interviewer lacks.[39] One of the primary issues with this strategy is that it results in a high false confession rate. When applying that false information to the intelligence gathering process contamination occurs within the information provided to tactical leaders.

c. Rapport-based Strategies

As scholarly research continues to examine how to best gain accurate HUMINT from detained persons, rapport-based strategies are emerging as the best approach. Two of the most commonly used methods are the PEACE Model and the cognitive interview.

The PEACE Model consists of the following steps: preparation and planning, engage and explain, account, closure, and evaluate.[40] This methodology mirrors that which is currently used in doctrine.[41] Essentially, the interviewer prepares to question the detainee, questions them using rapport building skills and active listening, upon completion any need for clarifications should be allowed and finally the interviewer should evaluate if any of the information gathered can be useful to follow on operations based on previous research.

---

[39] Salvati and Houck, "Examining the Causes and Consequences of Confession-Eliciting Tactics during Interrogation"; James Orlando, "Interrogation Techniques," Office of Legislative Research, accessed June 4, 2021, https://www.cga.ct.gov/2014/rpt/2014-R-0071.htm.

[40] Orlando, "Interrogation Techniques."

[41] Salvati and Houck, "Examining the Causes and Consequences of Confession-Eliciting Tactics during Interrogation"; Department of the Army, *Human Intelligence Collector Operations*; U.S. Marine Corps, *Counterintelligence*.

The Cognitive Interview Methodology has its foundation in psychology. It was developed in the 1970s and since then, has been used by various law enforcement and military personnel.[42] The technique is "a series of memory retrieval and communications techniques designed to increase the amount of information that can be obtained from an interviewee."[43] There are four main types of interview strategies: context reinstatement, report everything, variety of perspectives, and temporal order.[44] Essentially, the methodology stimulates the area of recall for the brain and requires a significant amount of cognitive functionality using open-ended questioning tactics.[45] In a meta-analysis study conducted by Amina Memon, Christian Meissner, and Joanne Fraser, "*The Cognitive Interview: A Meta Analytic Review and Study Space Analysis of the Past 25 Years*" observed that there is a "rather substantial increase in correct recall with the CI as compared with a structured interview." [46] This suggests that the information gathered as part of rapport-based strategies may in fact be more useful to CI personnel than that of the other methodology of interviews. It is obvious that both methodologies are a better option than the use of physical or psychological coercion; however, the overall ability to detect deception remains at a 50% average.[47]

2. Polygraph

The use of a polygraph test is the only means which the DOD leverages to the presence of the physical responses typically associated with deception. Understanding its history,

---

[42] Keller-McNulty, "Quest for Truth: Deception and Intent Detection"; Salvati and Houck, "Examining the Causes and Consequences of Confession-Eliciting Tactics during Interrogation"; Amina Memon et al., "The Cognitive Interview: A Meta-Analytic Review and Study Space Analysis of the Past 25 Years," *Psychology, Public Policy, and Law* 16, no. 4 (November 2010): 340–72, http://dx.doi.org.libproxy.nps.edu/10.1037/a0020518.

[43] Memon et al., "The Cognitive Interview," 340.

[44] Memon et al., "The Cognitive Interview"; Aldert Vrij et al., "Increasing Cognitive Load to Facilitate Lie Detection: The Benefit of Recalling an Event in Reverse Order," *Law and Human Behavior* 32, no. 3 (June 2008): 253–65, http://dx.doi.org.libproxy.nps.edu/10.1007/s10979-007-9103-y; Keller-McNulty, "Quest for Truth: Deception and Intent Detection."

[45] Keller-McNulty, "Quest for Truth: Deception and Intent Detection"; Memon et al., "The Cognitive Interview."

[46] Memon et al., "The Cognitive Interview," 357.

[47] Houck et al., "When Beliefs Lead to (Im)Moral Action"; Vrij et al., "Psychological Perspectives on Interrogation"; Pérez-Rosas et al., "Deception Detection Using Real-Life Trial Data."

implementation procedure, results, and limitations is key to a comparison of current practices vice the implementation of emerging technologies.

The idea of detecting deception has been around since lying has been around. Various historical examples can point to different cultures, times, and peoples using various abstract events to prove that the person in question is lying. From the Salem Witch Trials, to chewing rice powder in China, there has been a societal attempt to detect if a person is lying, with the assumption that lying is an emotional event.[48] It is from this belief, paired with the advancement of medical technologies, that motivation for the polygraph's invention was derived. The first iteration of it occurred in 1921, when John Larson attempted to create a device which accurately measured blood pressure, pulse rate, and respiration.[49] The process behind this, which was tested by Larson, was to ask a subject a yes or no question; once there was an aggregated amount of data, the difference in a single profile suggested that individual with the differences was attempting to be deceptive.[50] From here, other devices similar to the one which John Larson created were adapted for mobility, but essentially since 1921, the premise of the polygraph has not changed.

To employ a polygraph test, the DOD and Marine Corps have directives and doctrine establishing regulations. DOD Directive (DoDD) 5210.91, *Polygraph and Credibility Assessment Procedures*, set forth the authorized uses and rules for conducting an examination. MCWP 2-6 provides operational context for the implementation and appropriate uses of the information gathered for intelligence professionals.

Figure 2 illustrates the authorized uses of the polygraph for the DOD. It lists CI investigations and operations as an authorized use. DoDD 5210.91 lists the steps to be conducted as pre-test, data collection, test data analysis, and post-test. MCWP 2-6 concurs with this process. There are two types of tests: the Guilt Knowledge Test, also known as Concealed Information

---

[48] Don Grubin and Lars Madsen, "Lie Detection and the Polygraph: A Historical Review," *Journal of Forensic Psychiatry & Psychology* 16, no. 2 (June 2005): 357–69, https://doi.org/10.1080/14789940412331337353.

[49] Grubin and Madsen, 360.

[50] Grubin and Madsen, 360–61.

Test, and Comparison Question Test.[51] The possible results of the testing as used by DOD include No Deception Indicated, Deception Indicated, No opinion, No significant response, and Significant Response.[52] These responses are congruent with the American Polygraph Association standards. MCWP 2-6, acknowledges the following list may affect the results of a polygraph.

- Mental health disorder of any type.
- History of heart or respiratory, circulatory, or nervous disorders.
- Current medical disorder, including colds, allergies, or other conditions.
- Drugs or alcohol use before the examination.
- Mental or physical fatigue.
- Pain or physical discomfort.[53]

The research presents two outlooks on the results of the polygraph. The first typically is the outlook which states the polygraph is unable to accurately detect deception, rather it detects a physiological response to questions asked which produces inconsistent results. This is the position held by the U.S. Supreme Court.[54] The second outlook is that with the proper training and questioning techniques the polygraph can increase the ability to detect deception from the average of 54% to 69.4%.[55]

---

[51] Charles R. Honts, Steven Thurber, and Mark Handler, "A Comprehensive Meta-analysis of the Comparison Question Polygraph Test," *Applied Cognitive Psychology* 35, no. 2 (March 2021): 411–27, https://doi.org/10.1002/acp.3779; Jerry A. Lewis and Michelle Cuppari, "The Polygraph: The Truth Lies Within," *Journal of Psychiatry & Law* 37, no. 1 (Spring 2009): 85–92, https://doi.org/10.1177/009318530903700107.

[52] US Marine Corps, *Counterintelligence*; Department of Defense, *Polygraph and Credibility Assessment Procedures*, DoD Directive 5210.91 (Washington, DC: Department of Defense, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/521091p.pdf?ver=2019-04-22-104603-167.

[53] US Marine Corps, *Counterintelligence*.

[54] "The Truth About Lie Detectors (Aka Polygraph Tests)," American Psychological Association, August 5, 2004, https://www.apa.org/research/action/polygraph.

[55] Honts, Thurber, and Handler, "A Comprehensive Meta-analysis of the Comparison Question Polygraph Test"; Vrij et al., "Increasing Cognitive Load to Facilitate Lie Detection."

Issue-Based Examinations	Narrowly focused on specific issues or allegations: - Criminal investigations - CI investigations and operations - Counterterrorism (CT) investigations and operations - Personnel security investigations (PSI) - Foreign intelligence operations - Asset validation (source testing) - Exculpation of alleged wrongdoing, fault, or guilt
PSS – 2 types: - CSP examinations - ESS examinations	Not predicated on a specific issue or allegation: - Designated intelligence positions - SAP - Adjudicative resolution of foreign relationships - Accelerated sensitive compartmented information (SCI) access - Classified access for foreign nationals

Figure 2. Authorized Uses of the Polygraph[56]

C. EMERGING MACHINE TECHNOLOGIES FOR DECEPTION DETECTION

From the previous section we have a complete picture of the current practices within the DOD, Intelligence Community, and Marine Corps. We understand the history of these methods and their associated accuracy. In the following section we aim to analyze emerging technologies that increase the accuracy of detecting deception, including neuroimaging, video, audio, and other biometric technologies.

1. Neuroimaging

Neuroimaging is the process of measuring different forms of brain activity. Studies have shown that during deception events there is increase in the activity of the pre-frontal cortex.[57] There are three primary neuroimaging sensors used to detect changes in brain activity.[58] The first is electroencephalogram (EEG), which measures electrical activity within the brain. The drawback

[56] Adapted from Department of Defense, *Polygraph and Credibility Assessment Procedures*.

[57] F. Andrew Kozel et al., "Detecting Deception Using Functional Magnetic Resonance Imaging," *Biological Psychiatry* 58, no. 8 (October 15, 2005): 605–13, https://doi.org/10.1016/j.biopsych.2005.07.040.

[58] S.A. Bunge and I. Kahn, "Cognition: An Overview of Neuroimaging Techniques," in *Encyclopedia of Neuroscience* (Elsevier, 2009), 1063–67, https://doi.org/10.1016/B978-008045046-9.00298-9.

of this methodology is the limited special resolution. The second neuroimaging technique that scientist have used to study deception is functional magnetic resonance imaging, FMRI. This technique measures activation of brain regions through the measurement of blood flow. This technique is not practical for DOD combat operations due to the nature of the equipment required for its conduct. The equipment is cost prohibitive requiring highly specialized personnel and training to operate. The final and newest neuroimaging technique is functional near-infrared spectroscopy, FNIRS. This optical imaging technique is portable and measures blood flow; at a depth penetration of 3cm.[59] For deception detection this penetration depth is sufficient. The DOD has funded deception detection studies to explore the implementation of EEG and FMRI techniques. The U.S. Navy demonstrated a capability to classify deception, utilizing EEG, with a median 95% statistical confidence with less than 1% error rate for a concealed information test.[60] Nongovernmental scientist have also conducted successful research in classifying deception for both EEG and FNIRS.[61] Of these studies the most successful employed EEG capabilities alone to identify if a yes-no answer was an intentional deception. They found they were able to classify

---

[59] "FAQ on NIRS" NIRx Medical Technologies, accessed June 4, 2021, https://nirx.net/faq.

[60] Lawrence A. Farwell et al., "Brain Fingerprinting Classification Concealed Information Test Detects US Navy Military Medical Information with P300," *Frontiers in Neuroscience* 8 (December 23, 2014), https://doi.org/10.3389/fnins.2014.00410.

[61] Jiang Zhang et al., "A Look Into the Power of FNIRS Signals by Using the Welch Power Spectral Estimate for Deception Detection," *Frontiers in Human Neuroscience* 14 (January 18, 2021): 606238, https://doi.org/10.3389/fnhum.2020.606238; Marzieh Daneshi Kohan et al., "Interview Based Connectivity Analysis of EEG in Order to Detect Deception," *Medical Hypotheses* 136 (March 2020): 109517, https://doi.org/10.1016/j.mehy.2019.109517; Marzieh Daneshi Kohan et al., "EEG/PPG Effective Connectivity Fusion for Analyzing Deception in Interview," *Signal, Image and Video Processing* 14, no. 5 (July 2020): 907–14, https://doi.org/10.1007/s11760-019-01622-1; Wenwen Chang et al., "Comparison of Different Functional Connectives Based on EEG during Concealed Information Test," *Biomedical Signal Processing and Control* 49 (March 2019): 149–59, https://doi.org/10.1016/j.bspc.2018.12.008; Haizhou Leng et al., "Sophisticated Deception in Junior Middle School Students: An ERP Study," *Frontiers in Psychology* 9 (January 11, 2019): 2675, https://doi.org/10.3389/fpsyg.2018.02675; Yijun Xiong, junfeng Gao, and Ran Chen, "Connectivity Network Analysis of EEG Signals for Detecting Deception," *Journal of Physics: Conference Series* 1176 (March 2019): 032051, https://doi.org/10.1088/1742-6596/1176/3/032051; Zhen Yuan and Xiaohong Lin, "Mapping of the Brain Activation Associated with Deception Using Fused EEG and FNIRS," in *Neural Imaging and Sensing 2019*, ed. Qingming Luo, Jun Ding, and Ling Fu (Neural Imaging and Sensing 2019, San Francisco, United States: SPIE, 2019), 14, https://doi.org/10.1117/12.2508257; Roberto Vega et al., "Hemodynamic Pattern Recognition During Deception Process Using Functional Near-Infrared Spectroscopy," *Journal of Medical and Biological Engineering* 36, no. 1 (February 2016): 22–31, https://doi.org/10.1007/s40846-016-0103-6; Junfeng Gao et al., "A Novel Algorithm to Enhance P300 in Single Trials: Application to Lie Detection Using F-Score and SVM," ed. Hans A. Kestler, *PLoS ONE* 9, no. 11 (November 3, 2014): e109700, https://doi.org/10.1371/journal.pone.0109700.

deception with a 99.85% accuracy.[62] Studies pertaining to FNIRS indicated a capability of classifying deception with a 95.63% accuracy.[63] However, neither of these results mimicked battlefield usage. More realistic battlefield conditions resulted in a lower accuracy rate of approximately 84%.[64] Through combining both EEG and FNIRS, improvement in deception detection occurs.[65] Overwhelming neuroimaging is still possible. In one study, which compared frequent liars to infrequent lairs, they showed that infrequent liar's attempts at deception were easier to classify when compared to those who frequently lie.[66] This means those trained in evasion tactics maybe able to employ them more effectively without detection.

2. Natural Language Processing

Natural Language Processing (NLP) is a subcomponent of artificial intelligence which enables machines to understand human languages. One potential application of NLP is the analysis of speech patterns during an interrogation to gauge deception. Though various studies suggest different methodologies and approaches, they are mostly inclusive of contextual applications such as word count and sentence count, or various other linguistics attributes such as repetition, complexity, and uncertainty.[67] The DOD services and its research-based infrastructure has not

---

[62] Xiong, Gao, and Chen, "Connectivity Network Analysis of EEG Signals for Detecting Deception."

[63] Vega et al., "Hemodynamic Pattern Recognition During Deception Process Using Functional Near-Infrared Spectroscopy."

[64] Daneshi Kohan et al., "EEG/PPG Effective Connectivity Fusion for Analyzing Deception in Interview"; Vega et al., "Hemodynamic Pattern Recognition During Deception Process Using Functional Near-Infrared Spectroscopy."

[65] Yuan and Lin, "Mapping of the Brain Activation Associated with Deception Using Fused EEG and FNIRS."

[66] Fang Li et al., "Lie Detection Using FNIRS Monitoring of Inhibition-Related Brain Regions Discriminates Infrequent but Not Frequent Liars," *Frontiers in Human Neuroscience* 12 (March 13, 2018): 71, https://doi.org/10.3389/fnhum.2018.00071.

[67] Christie M. Fuller, David P. Biros, and Rick L. Wilson, "Decision Support for Determining Veracity via Linguistic-Based Cues," *Decision Support Systems* 46, no. 3 (February 2009): 695–703, https://doi.org/10.1016/j.dss.2008.11.001; Jeffrey T. Hancock et al., "On Lying and Being Lied To: A Linguistic Analysis of Deception in Computer-Mediated Communication," *Discourse Processes* 45, no. 1 (December 17, 2007): 1–23, https://doi.org/10.1080/01638530701739181; Victoria L. Rubin and Tatiana Lukoianova, "Truth and Deception at the Rhetorical Structure Level," *Journal of the Association for Information Science and Technology* 66, no. 5 (2015): 905–17, https://doi.org/10.1002/asi.23216; Pérez-Rosas et al., "Deception Detection Using Real-Life Trial Data"; Lina Zhou et al., "Automating Linguistics-Based Cues for Detecting Deception in Text-Based Asynchronous Computer-Mediated Communications," *Group Decision and Negotiation* 13, no. 1 (January 2004): 81–106.

directly tied counterintelligence operations and NLP together to study statement accuracy; however, there are two studies regarding the DOD's use of all artificial intelligence capabilities, and both recommend the continuation of research into artificial intelligence and NLP.[68] Linguistic Inquiry and Word Count (LIWC) is one of the most common commercially available programs currently used. Essentially the user inputs a string of text, and the program analyzes it and compares it to a dictionary. Based on the various categories of requested analysis, it produces a percent-based result.[69] Outside military researchers, various other professionals are assessing the results of applying NLP to deception detection. Though studies vary from 60% to 74% accuracy, based on the approach, type of text, and algorithms used, the consensus is that natural language processing can help identify deception.[70]

3. Other Biometric Monitoring

In addition to neuroimaging and NLP, there are other technologies that studies have shown may produce more accurate results in attempting to detect deception. One is audio analysis, which includes frequency and pitch characterizations. Facial expression analysis, including facial expression, micro-facial expressions, and eye tracking, has been studied. Body language analysis, including hand gestures, head nodding, and posture is another studied technique. Thermal imaging, heart rate monitoring, and various other methodologies have also been studied.[71]

D. ALGORITHMS

To produce a desired output, the raw data collected by the various sensors needs processing. To do this, there are various algorithms that can be employed to remove noise and classify between deceptive and non-deceptive events. For example, the literature showed that

---

[68] Kristin E. Schaefer et al., "A Meta-Analysis of Factors Influencing the Development of Trust in Automation: Implications for Human-Robot Interaction:" (Fort Belvoir, VA: Defense Technical Information Center, July 1, 2014), https://doi.org/10.21236/ADA607926; Potember, "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD."

[69] "How It Works," LIWC, accessed June 5, 2021, http://liwc.wpengine.com/how-it-works/.

[70] Rubin and Lukoianova, "Truth and Deception at the Rhetorical Structure Level"; Hancock et al., "On Lying and Being Lied To"; Pérez-Rosas et al., "Deception Detection Using Real-Life Trial Data."

[71] Keller-McNulty, "Quest for Truth: Deception and Intent Detection"; Pérez-Rosas et al., "Deception Detection Using Real-Life Trial Data."

classifiers using linear discriminant analysis, support vector machines and convolutional neural networks could all successfully classify deception when processing brain signals.[72] In order for NLP to successfully classify deception, various raw data inputs are provided to algorithms which constitute programs and toolkits. These algorithms conduct a comparison of known information to the entry. The most used algorithms are keyword extractions, named entity recognition, topic modelling, and knowledge graphs.[73] From video signals scientists can use eye movement and facial expressions to classify deceptive events. For facial expressions, the use of traditional statistical methods like multivariate regression and Bayesian Methods is common, in addition to more modern methods like the Convolutional Neural Networks.[74] These various algorithms are essentially what produces the data which can inform intelligence professionals if a detainee is attempting to be deceitful. Ensuring that parallel processing is available to minimize processing time and maximize feedback rates will be a critical element in any system looking to detect deception.

---

[72] Faryal Amber et al., "P300 Based Deception Detection Using Convolutional Neural Network," in *2019 2nd International Conference on Communication, Computing and Digital Systems (C-CODE)* (2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE), Islamabad, Pakistan: IEEE, 2019), 201–4, https://doi.org/10.1109/C-CODE.2019.8681025; Daneshi Kohan et al., "EEG/PPG Effective Connectivity Fusion for Analyzing Deception in Interview"; Daneshi Kohan et al., "Interview Based Connectivity Analysis of EEG in Order to Detect Deception"; Xiong, Gao, and Chen, "Connectivity Network Analysis of EEG Signals for Detecting Deception"; Vega et al., "Hemodynamic Pattern Recognition During Deception Process Using Functional Near-Infrared Spectroscopy."

[73] "Top Natural Language Processing (NLP) Algorithms And Techniques For Beginners," Programmer Backpack, June 21, 2020, https://programmerbackpack.com/top-natural-language-processing-nlp-algorithms-and-techniques-for-beginners/; Hancock et al., "On Lying and Being Lied To"; "How It Works."

[74] Guosheng Hu et al., "Deep Multi-Task Learning to Recognise Subtle Facial Expressions of Mental States," in *Computer Vision – ECCV 2018*, ed. Vittorio Ferrari et al., vol. 11216, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2018), 106–23, https://doi.org/10.1007/978-3-030-01258-8_7; Steven J. Pentland et al., "A Video-Based Screening System for Automated Risk Assessment Using Nuanced Facial Features," *Journal of Management Information Systems* 34, no. 4 (October 2, 2017): 970–93, https://doi.org/10.1080/07421222.2017.1393304; Lin Su and Martin Levine, "Does 'Lie to Me' Lie to You? An Evaluation of Facial Clues to High-Stakes Deception," *Computer Vision and Image Understanding*, Spontaneous Facial Behaviour Analysis, 147 (June 1, 2016): 52–68, https://doi.org/10.1016/j.cviu.2016.01.009; Mircea Zloteanu et al., "Veracity Judgement, Not Accuracy: Reconsidering the Role of Facial Expressions, Empathy, and Emotion Recognition Training on Deception Detection," *Quarterly Journal of Experimental Psychology* 74, no. 5 (May 1, 2021): 910–27, https://doi.org/10.1177/1747021820978851.

E. JOINT COGNITIVE SYSTEM AND HUMAN MACHINE TEAMING

As technology has advanced, there are various sensing methods which may help intelligence professional gather accurate information through the detection of deception. However, attempting to replace the interviewer with a robot is unlikely to yield positive results. Building a system that leverages all the technological advances while keeping the interviewer in the loop may present the best solution to gain an asymmetrical advantage. To do this, we can investigate the Joint Cognitive System's development which facilitates a machine and human team pair to achieve a goal.

1. Joint Cognitive Systems Engineering: A Model for Human-Machine Teaming

Systems engineering is defined as "a transdisciplinary and integrative approach to enable the successful realization, use, and retirement of engineered systems, using systems principles and concepts, and scientific, technological, and management methods."[75] It focuses on the development of a project's life cycle inclusive of goals, purposes, needs, and design. It considers the people, end results, as well as processes which facilitate the accomplishment of goals.[76] Our focus will be on defining anticipated customers' needs and defining an operational concept by using methodologies related to Cognitive Systems Engineering (CSE) resulting in a Joint Cognitive System's development.

CSE is concerned with the modeling of human-machine interaction in such a way as to treat both human and machine agent(s) as individual "thinking" agents working together in a team in a given environment.[77] This will facilitate both an interviewer being present as well as a machine that can help in detecting deception during the interview process. An essential component of cognitive engineering is human operator modeling. The goals of the modeling process are to

---

[75] INCOSE, "Systems Engineering Definition," Incose.org, accessed June 4, 2021, https://www.incose.org/about-systems-engineering/system-and-se-definition/systems-engineering-definition#ENGINEERED_SYSTEM.

[76] INCOSE.

[77] Erik Hollnagel and David D. Woods, "Cognitive Systems Engineering: New Wine in New Bottles," *International Journal of Man-Machine Studies* 18, no. 6 (June 1983): 583–600, https://doi.org/10.1016/S0020-7373(83)80034-0.

determine the type and style of information presented to the human user, and to establish the technical demands of the system in the context of the user's needs.[78] The primary resultant of CSE is a Joint Cognitive System, defined as "the combination of human problem solver and automation technologies which act as co-agents to achieve goals and objectives in a complex work domain."[79]

One way to help design teams create a system is to create a model of processes. The Operation Function Model (OFM), typically used in CSE, is a tool designed specifically to assist in cognitive engineering of human–computer systems. Organized hierarchically, the model structurally accounts for where the human operator focuses his or her attention during a complex task. It consists of nodes, representing operator tasks and functions, and arcs, representing triggering events that cause the operator to change to another task or function. Operator function models help the designing of decision aids for search-and-rescue missions, ship navigation, ground control of orbiting satellites, and information retrieval in a corporate environment.[80] We selected the OFM for the development of this system because it captures the cognitive events that occur between human agents, between human and machine agents, and the transitions between those events.

2. Human-Machine Trust

For any Joint Cognitive System or human-machine team pair to be effective, a trusting relationship between the human and the machine is necessary.[81] There is an extensive amount of psychological research regarding trust. As technology continues to emerge linking humans to machine more research is on-going to understand how a machine component will differ from the established human-to-human trust relationship.

---

[78] Amanda C. Muller and S. Narayanan, "Cognitively-Engineered Multisensor Image Fusion for Military Applications," *Information Fusion* 10, no. 2 (April 2009): 137–49, https://doi.org/10.1016/j.inffus.2008.08.008.

[79] Scott S. Potter et al., "Evaluating the Effectiveness of a Joint Cognitive System: Metrics, Techniques, and Frameworks," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 50, no. 3 (October 2006): 314–18, https://doi.org/10.1177/154193120605000322.

[80] Muller and Narayanan, "Cognitively-Engineered Multisensor Image Fusion for Military Applications."

[81] Ella Glikson and Anita Williams Woolley, "Human Trust in Artificial Intelligence: Review of Empirical Research," *Academy of Management Annals* 14, no. 2 (July 2020): 627–60, https://doi.org/10.5465/annals.2018.0057.

Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."[82] A machine, which for the purposes of this research has reference to AI, is "a highly capable and complex technology that aims to simulate human intelligence."[83] The steps which the machine performs typically includes sensing the outside world, processing the raw sensed information, producing a result, and conducting an assessment of the results produced.[84] It is critical to understand how different factors can affect the establishment, maintenance, and destruction of trust between human and machines that they team with.

According to psychological research, there are two types of trust which influence the development of a trusting relationship between human and machine: cognitive and emotional. Cognitive trust usually is referring to the logical trust which can be developed through use and time through a clear understanding of the contractual roles which the human is expecting the machine to perform.[85] Elements which influence this include previous experience with machines, competence and knowledge level in the task being perform, ease of use, as well as the expectations of the machine.[86] Emotional trust usually refers to how the human participants feels about the machine. Factors of influence include, attitudes, confidence level, satisfaction, and comfort.[87]

---

[82] Glikson and Woolley; Roger C. Mayer, James H. Davis, and F. David Schoorman, "An Integrative Model of Organizational Trust," *The Academy of Management Review* 20, no. 3 (1995): 709–34, https://doi.org/10.2307/258792.

[83] Glikson and Woolley, "Human Trust in Artificial Intelligence."

[84] Glikson and Woolley; Potember, "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD."

[85] Glikson and Woolley, "Human Trust in Artificial Intelligence"; Alon Jacovi et al., "Formalizing Trust in Artificial Intelligence: Prerequisites, Causes and Goals of Human Trust in AI," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '21 (New York, NY, USA: Association for Computing Machinery, 2021), 624–35, https://doi.org/10.1145/3442188.3445923; Schaefer et al., "A Meta-Analysis of Factors Influencing the Development of Trust in Automation."

[86] Schaefer et al., "A Meta-Analysis of Factors Influencing the Development of Trust in Automation"; Tiffany Clark, "Integrity-Based Trust Violations within Human-Machine Teaming" (Master's Thesis, Monterey, CA, Naval Postgraduate School, 2018), http://calhoun.nps.edu/handle/10945/59637.

[87] Schaefer et al., "A Meta-Analysis of Factors Influencing the Development of Trust in Automation," 13–14.

Each of these factors needs consideration during the development phase to yield the most advantageous system.

Like human trust relationships, the maintenance of a relationship between a human and machine is key, particularly in stressful situations. Warfare is inherently chaotic and therefore stressful. It is critical that during stress that a system designed to assist a uniformed military member in the conduct of their job will perform its assigned role. As a study conducted by Drs. Paul Robinette, Alan Wagner, and Ayanna Howard, suggests, self-reported trust in AI decreases 53% when the AI committed a known error.[88] Additionally, the report also suggested that there was a strong correlation between trust and a willingness to use the AI in time critical situations.[89] Further studies suggest that even outside of time critical situations, when a machine errors, this has a negative influence on the trust relationship, and the operator has a tendency to avoid use of the system.[90] In order to prevent this, three primary training suggestions were made: 1) ensure that training with a system encompasses common errors or failures, 2) integrate realistic scenario based training to overcome hesitations to use automation after failure, and 3) ensure participants are educated on the system through a full understanding of capabilities and limitations.[91]

---

[88] Paul Robinette, Ayanna M. Howard, and Alan R. Wagner, "Effect of Robot Performance on Human–Robot Trust in Time-Critical Situations," *IEEE Transactions on Human-Machine Systems* 47, no. 4 (August 2017): 425–36, https://doi.org/10.1109/THMS.2017.2648849.

[89] Robinette, Howard, and Wagner.

[90] Schaefer et al., "A Meta-Analysis of Factors Influencing the Development of Trust in Automation," 16.

[91] Schaefer et al., 26.

III. PROPOSED SYSTEMS MODEL: WILDS

A. PROPOSED EMPLOYMENT MODEL

Figure 3 presents the proposed employment model of Warfare Integrated Lie Detection System (WILDS). The model identifies three major players in the employment of WILDS: the enemy, the interviewer, and WILDS. Further discussion on the roles of each major player and the relationships between each of them will occur later in this section.

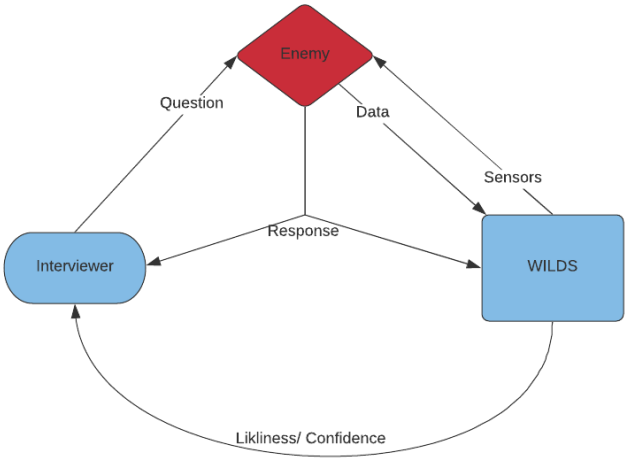

Figure 3. Proposed Employment Model

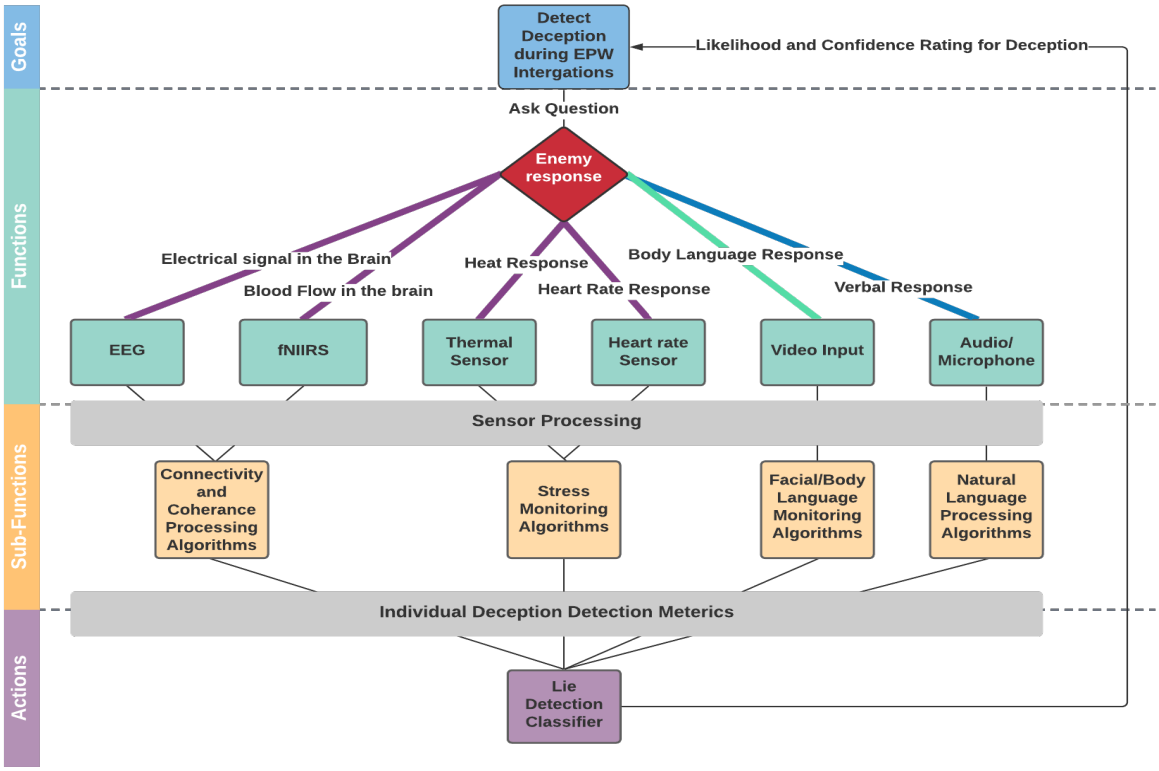

Figure 4. Proposed Operator Function Model[92]

[92] Adapted from J.D. Lee and T.F. Sanquist, "Augmenting the Operator Function Model with Cognitive Operations: Assessing the Cognitive Demands of Technological Innovation in Ship Navigation," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 30, no. 3 (May 2000): 273–85, https://doi.org/10.1109/3468.844353; Benjamin Weyers et al., eds., *The Handbook of Formal Methods in Human-Computer Interaction*, Human–Computer Interaction Series (Cham: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-51838-1; Muller and Narayanan, "Cognitively-Engineered Multisensor Image Fusion for Military Applications."

B. PROPOSED OPERATOR FUNCTION MODEL

Figure 4 presents the proposed operator functional model for WILDS.[93] The model sets the primary goal as detecting deception during EPW interrogations. It sets the functions for the machine sensors, such as the Brain Computer Interface (BCI), thermal imaging, heart rate sensors, and audio/visual inputs. The sub-functions are set as the algorithms required to process the raw data. The final action of the system produces a likelihood rating and associated confidence metric in compliance with the ICD-203.

C. DISCUSSION OF OFM

1. Overview

WILDS' operator function model, as illustrated in Figure 4, is an application of Joint Cognitive Systems Engineering. Essentially with an identified goal, the model enables the development of functions and subfunctions which supports an action to achieve the identified goal. We selected this form of modeling for two primary reasons. The first is because it is a goal-oriented model. Goal-oriented models facilitate keeping the focus on a defined end-state, rather than task-oriented models which focus on key performance metrics. The difference allows for more creative and innovative solutions development, regardless of who or what is performing each task to achieve the goal. This ties directly to the second reason, which is OFM facilitates human and machine interactions. Many other system model designs rely on the premise that either a human or a machine will achieve a goal independently. The OFM, however, recognizes there are tasks which are better suited for machines. Those tasks inform human decisions. Rather than designing a system discounting either the human or machine element, OFM leverages what a machine can do and provides a design which considers how the human will interact with the machine in order to achieve the defined end state.[94] In doing this the model considers both the

[93] Lee and Sanquist, "Augmenting the Operator Function Model with Cognitive Operations"; Weyers et al., *The Handbook of Formal Methods in Human-Computer Interaction*; Muller and Narayanan, "Cognitively-Engineered Multisensor Image Fusion for Military Applications."

[94] Potter et al., "Evaluating the Effectiveness of a Joint Cognitive System."

capabilities and limitation for the human and for the machine, permitting the machine to provide the human with the necessary information while leaving the human to understand the context and make continued decisions based on the information provided.[95] For these two reasons the operator function model was selected to develop WILDS.

2. Goals

The goal Figure 4 presents is detecting deception during detainee interviews. Because an OFM's purpose is to identify each stage and functionality of a developed system, the goal identified presents the main purpose of the system. It's development stems from identifying the problem space, examining current processes, examining current technologies, and finding areas for improvements. As Chapter II outlines, the problem space is the capability of human operators being able to accurately detect deception with the intent of using the information gathered from human intelligence sources for operational purposes. After examining the current processes and technologies within this field, one viable solution would be creating a machine which detects deception accurately and provides results in a timely manner. This machine's design must include detecting deception accurately and providing its results to a human, who can leverage the results in a context enabling tactical leaders to make better decisions. It is from this goal that the design of the operational function model for WILDS promulgated from.

3. Functions

The functions section of the OFM explains the methodology of achieving the goal. In the case of WILDS, to detect deception there are various sensors which will be present during the interview process. These sensors include thermal imaging, audio feeds, video feeds, FNIRS, and EEG sensors. To achieve the goal, the interviewer sets up the sensors and records. They then ask the detainee questions, and the detainee responds. The sensors are detecting changes in heart rate, temperature, blood flow to the brain, electrical signals within the brain, vocal pitches, body positioning, and language used by the detainee. This

[95] Potter et al.

is the raw data input to WILDS. This data is subsequently processed in such a way that a computer can understand it.

4. Subfunctions

For the raw data to be meaningful it needs processing in such a way that the results produced after processing are interpretable by a human. Therefore, upon the receipt of the sensing data, various algorithms are applied to the processed data. These are the subfunctions of WILDS. They include the connectivity and coherence processing algorithm, the stress monitoring algorithm, facial/body language monitoring algorithm, and the natural language processing algorithms. Each of these algorithms produce a result that is indicative if the detainee is lying. It is based on this information that the final steps can occur, and the goal is achievable.

5. Actions

The actions section of the OFM combines all the outputs of the subfunctions together to produce a meaningful result. For WILDS, these final steps which occur is the combination of each algorithm into a single useable percentage provided to the interviewer. This percentage informs the interviewer of the likeliness that the detainee is attempting to be deceptive. Additionally, it informs the interviewer of a confidence level in that percentage. This confidence level is based on the number of functions and subfunctions implemented during the process. A high confidence level is indicative of all the sensors and algorithms employment, while a low confidence level is indicative of either a sensor or algorithm failing to produce an initial result. These outputs are congruent with the requirements set forth in ICD-203, which ultimately enables further decisions made in the interview room.

D. DISCUSSION OF PROPOSED EMPLOYMENT

1. Overview

The proposed employment model presented illustrates how WILDS can fits into EPW interviewers. The proposed model assumes that the HUMINT interviewer employing

WILDS has completed all necessary preparatory actions, including but not limited to coordinating and getting the approval for conducting the interview, planning the approach for questioning and responses, reserving a private interview room, setting up the interview room and sensors required for WILDS, and conducting a proper handover of the EPW with the proper military police handler. Upon completion of the handover, there are three pertinent relationships involved: the relationship between the prisoner and the interviewer, the relationship between the prisoner and WILDS, and the relationship between the interviewer and WILDS.

For each relationship to be functional there is a flow of information which must occur. First, as indicated on Figure 3, WILDS must be sensing what the detainee is doing. Then the interviewer must ask a question. The type of question asked is dependent on the methodology by which the interviewer is working. Both closed ended—yes or no—or open-ended questions are acceptable for the use of WILDS. Once the prisoner responds to the question, the interviewer and WILDS processes that information. WILDS then produces a percentage of likeliness that the detainee is lying along with a confidence level in that percentage. The interviewer receives these results. Based on the training of the interviewer and the trust relationship built between WILDS and the interviewer, the interviewer would proceed with further planned questioning, adjusting for the honesty or lying occurring at the time. WILDS would continue to monitor and provide feedback on every question until the interview's completion.

2. Role of Enemy

As discussed in Chapter II, there are three primary types of detainees which can provide useful information during an interview: an enemy-state actor, an enemy non-state actor (belligerent), and civilians (non-belligerent). Though there are various legal considerations for interviewing the different types of detainees, for effective counterintelligence gathering all detainees must provide a response. Therefore, the primary role of the detainee is to respond to the questions of the interviewer. Though on the surface this seems rather simple, two barriers may have a significant influence on if the detainee responds: failed communication and trained resistance.

Trained resistance to the interviewing process, traditionally seen in state or non-state actors, is an attempt to protect the information they have. Typical resistance methodologies include failing to answer any questions posed regardless of by whom, failing to answer any question not related directly to their health or welfare, and providing only mandated requirements of the Geneva Conventions (name, rank, service number, and date of birth) when asked any questions. If these methodologies are being employed, the ability to gather intelligence through the employment of WILDS is drastically limited. Though the sensors are still able to monitor any changes that occur in the detainee, the reasons for these changes occurring cannot be correlated directly to a lie or intention to deceive.

The second barrier to receiving a response is communication failure. Figure 5 shows two paths of communication presented by Wilber Schramm.[96] They illustrate that the recipient of the information must be able to understand questions posed to them. Therefore, if there is a foreign language involved, context from the questions is missing, or if there are multiple ways of interpreting a situation or question then the result may be no response to the questions posed by the interviewer. Being able to ensure that the pathways from is clear of any obstruction ensures clear communication and will yield better results for the interviewer.

[96] Wilber Schramm and Donald Roberts, "How Communication Works," in *The Process and Effects of Mass Communication*, Rev (Urbana: University Of Illinois Press, 1971), 1–24.

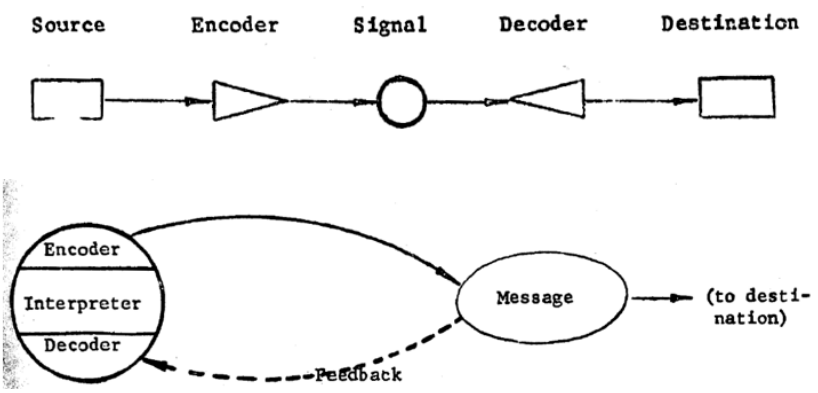

Figure 5. Schramm's Communication Model[97]

3. Role of WILDS

WILDS fits into the employment model as a member for the interviewing team. It works in conjunction with the interviewer, being able to detect changes in the detainee which are imperceivable to the human eye. These changes provide an indication that the detainee is lying or has the intent to be deceitful. If employed effectively this system can help to gather HUMINT from detainees which may be critical to operations conducted by military forces. To be employed effectively there are two primary inputs into WILDS and two primary outputs it provides.

The two primary inputs into WILDS are the data collected by the sensors and the verbal response from the detainee. The data collected by the sensors is passive data, to include heart rate response, thermal imaging, and the other functions, as illustrated in Figure 4. For this input to be optimal, it should establish a baseline, meaning that the interviewer should have the sensors already turned on and working prior to the detainee answering any questions. This will allow the system to establish a baseline and then detect any changes regardless of verbal response from the detainee. The second input is the verbal response to the interviewer's question from the detainee. The information analyzed in the verbal response includes, at minimum, a vocal analysis of pitch and language choice. Again, the sensors should be set prior to the detainee answering relevant questions to gain

[97] Schramm and Roberts.

a baseline. Additional to sensors being set prior to the detainee's responses, the interviewer's initial questions should provide a baseline to establish language patterns used by the detainee. The reasons these two inputs must remain separated is because the former requires only the presence of the detainee, while the later requires that the detainee provides a verbal response to the interviewer's questions. Therefore, if the detainee is employing resistance tactics, as discussed in the previous section, the results may not be as accurate as when the detainee does at least provide an answer, deceptive or honest.

As discussed in Chapter II, the Intelligence Community adheres to ICD-203, which requires analysist to provide a percentage of likeliness for an event to occur while also providing the confidence level in their assessment. As such, the two primary outputs of WILDS are the likeliness rating and the confidence rating. The likeliness rating WILDS would produce is a percentage on if the detainee is lying. 0% would indict a truthful answer, while 100% would indict that the detainee is lying. This would allow the interviewer to ask follow on questions, informed of what the detainee previous responses were. Additionally, WILDS would produce a confidence level. This confidence level would be based on the number of sensors applied. A reduction in the number of sensors applied to a single question would produce a lower confidence level output. One example of when the confidence level would be lower than 100% is if the detainee is applying resistance tactics to the interview. If the detainee fails to provide a response to the question, vocal analysis nor language processing occurs. The consequence is that the natural language processor and its congruent algorithms do not feed into the overall result. Therefore, the number of sensors contributing to the output would decrease, and the confidence level would reflect that decrease. The interviewer receives this percentage and confidence level near instantaneously.

4. Role of Interviewer

The interviewer is the other team member involved during the deception detection process. Though they remain the primary responsible party for the overall conduct of the interview, WILDS is performing the actual task of determining if a detainee is lying. Unlike either the detainee or WILDS the role of the interviewer starts prior to the interview and

finishes after processing the information gained in the interview. As such the interviewer's roles has three sections: the preparation, the execution, and the results.

Like the conduct of the preparation phase outlined in Chapter II, many of the responsibilities remain on the interviewer. This is inclusive of getting the approval to conduct the interview by the detention facility commanders, coordinating the interview room requirements, and developing an approach for the questions asked during the interview process.[98] This last step, in particular, alters the conduct of the current processes. As explained in Chapter II, the current process of developing questions stems from the methodology employed. The interviewer selects a methodology they are most comfortable with, develops a list of potential questions to ask the detainee, and then moves into the execution phase. However, because there is an immediate feedback loop integrated into WILDS to inform the interviewer of deception, the ways which the interviewer develops question order changes from a list of questions to flow chart style. Figure 6 is a partial list of questions provided to counterintelligence specialists to help in the preparation of interview questions.[99] Figure 7 illustrates what could be employed with WILDS providing feedback. The implementation of this plan would help to optimize time spent in the interview room as well as facilitate the gathering of information necessary for military operations.

During the execution phase, the interviewer will have one output and two inputs, as depicted in Figure 3. The one output is the question directed at the detainee. We can see through the examination of Figure 7 that a proposed series of questions developed during the preparation phase would no longer rely on the detainee's truthfulness, but rather the attempt to deceive would simply trigger a different line of questioning. An anecdotal example would follow along with Figure 7. The interviewer asks the initial question: What individual weapons does unit X have? The detainee's answer produces a high likeliness and high confidence level of deception. Rather than repeating the question, the interviewer

---

[98] Department of the Army, *Human Intelligence Collector Operations*; US Marine Corps, *Counterintelligence*.

[99] Department of the Army, *Human Intelligence Collector Operations*.

proceeds with the following question: Does the unit have AK-47? The detainee answers no, again a high likeliness and confidence level of deception result. This would confirm that the enemy unit does have AK-47's. Therefore, the attempt to deceive when detected could be just as informative as the detainee telling the truth. Due to the innate nature of EPW interviews, the interviewer is going to have two inputs the observed response of the detainee, and the assessment WILDS provides. Though the ultimate decision and responsibility will remain with the interviewer for the assessment on if the detainee is being deceitful, with the proper training the interviewer will learn to trust the inputs that WILDS provides. This will result in an increased likeliness of detecting deception by EPWs during interviews.

Composition:

What is the command and control element of (the target unit)?
What types of units are directly subordinate to (the target unit)?
What is the designation of (each of the subordinate units)?
How many units of that type are directly subordinate to (target unit)?
What units are attached? When? Why? What unit(s) are they detached from?
What units are detached? When? Why? What unit(s) are they attached to now?

Weapons and Equipment Strength:

Individual Weapons:
What individual weapons are there in (target unit)?
How many?
What is the distribution of the weapons?
Crew-Served Weapons: What crew-served weapons are in (target unit)?
How many?
What is the distribution of the weapons?
Other Weapons: What other weapons are there in (target unit)?
What types?
How many?
How are they distributed?
Vehicles: What armored vehicles are in (unit)?
How many?
What nomenclature?
What other vehicles are in (unit)?

Figure 6. Questioning Reference[100]

[100] Source: Department of the Army.

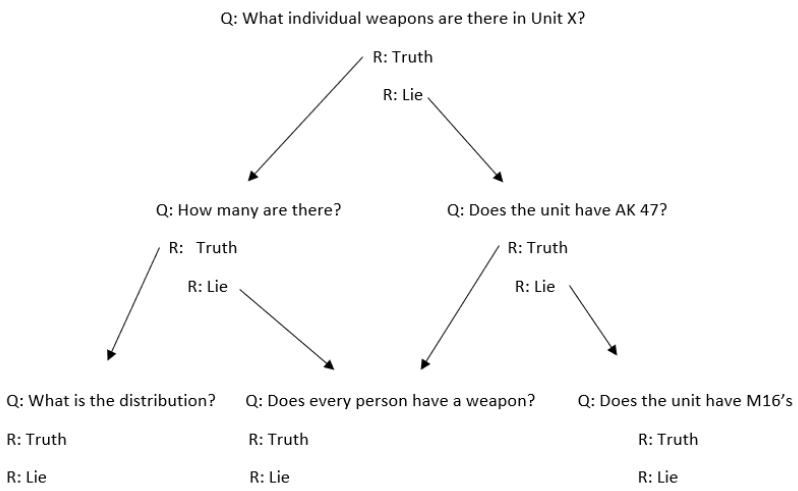

Figure 7. Question Diagram

E. TRUST IN WILDS

In Chapter II, we explored the current research regarding trust between humans and machines. From that exploration, three major conclusions are applicable to the implementation of WILDS and the ability to detect deception during EPW interviews.

1. Clearly defining the responsibilities, capabilities, and limitation of the system to be employed can foster trust in a human-machine team pair.[101]
2. Implementing scenario-based training that is tough and realistic can improve the trust relationship between the human and machine.[102]
3. Within the training environment, purposefully causing errors for a valid reason will improve the trust relationship between human and machine.[103]

Trust is a relationship formed between two entities in which each entity relies on the other to fulfill a set of understood responsibilities. As with any relationship, clearly defining what responsibilities are within the capacity of the trusted entity is one of the keys

---

[101] Jacovi et al., "Formalizing Trust in Artificial Intelligence."

[102] Schaefer et al., "A Meta-Analysis of Factors Influencing the Development of Trust in Automation."

[103] Schaefer et al.

to its success. Additionally, the trustee must clearly understand what realistic capabilities and limitations are for the trusted. Ultimately the trustee's expectations have to be managed for trust to be established and retained.[104] Figure 3 and its subsequent explanation clearly provides a set of responsibilities and designed outputs which WILDS is to provide to the interviewer during the execution phase. This includes accurately sensing various biometric elements of the detainee during the interview process and providing the interviewer with a percentage of likeliness that the detainee is attempting to be deceptive and an associated confidence level with that percentage. Through a clear identification of what WILDS' roles are during the interview process, the process of developing trust within the interviewer-WILDS team pair can begin.

Once the interviewer understands the roles for which they are responsible and the roles for which WILDS is responsible, familiarization with employing WILDS in the toughest, yet most realistic environments can help to foster a trust relationship between the team pair. Prior to the execution of the tough realistic training event preparatory actions should occur. These preparatory actions should include education on the theory, including historical examples, if possible, familiarization events, and low stress employment opportunities. Each action works to develop the knowledge and understanding of the events expected to occur and provides a foundational reference for when situations do not match perfectly with training. Upon completion of these preparatory actions, tough realistic training scenarios should be employed. These scenarios should cover both the breadth and depth of problems which may occur in a realistic fashion. The scenario should attempt to induce a high level of stress for the personnel in training to complete an action. Upon the completion of the training scenario, there should be an in-depth review of decisions made and the congruent reasonings. This immediate review enables the development of trust between the human machine team (HMT) pair.

Finally, for the establishment of a truly trusting relationship between the HMT pair a test should occur. The best way to do this is to purposefully cause WILDS to produce an inaccurate percentage of likeliness, in a scenario where that would be possible. One

[104] Jacovi et al., "Formalizing Trust in Artificial Intelligence."

example would be in a detainee attempting to employee evasive tactics through not providing any information. Though the system can monitor the detainee's heart rate, temperature, blood flow, and electrical impulses, the refusal of the detainee to respond to a question may produce a result with lower confidence or a false positive. A potential result of this is distrust for WILDS. However, after working through this, the team pair will gain a better understanding of the limitations of WILDS. With this knowledge and experience, a higher level of trust and confidence is achievable so that when employed during a combat operation the result is deception detection with near perfect accuracy.

IV. CONCLUSIONS

A. SUMMARY OF RESULTS

This thesis identified a clear gap in HUMINT operations. The IC, DOD, and Marine Corps do not have a tool that enables high fidelity deception detection during interrogations. WILDS encompasses emerging sensor technologies and leverages advanced integration techniques. We demonstrate this human-machine teaming through an operator functional model. This model identified the goals of the system, the functions, sub-functions, and actions that operators would need to take to achieve the desired goals. The proposed system, WILDS, addresses the identified gap through leveraging various sensors inputs, fusing the collected data to produce a likelihood and confidence rating which can contribute to the interrogation and provide intelligence professionals with insight. To optimize the results, our proposal considered the interview and interrogation methodology as well as the trust relationship between the human agent and WILDS. The implementation of this proposal will translate into fewer casualties, reduced collateral damage, and improve the overall outcome in warfare for friendly forces.

B. FUTURE WORK

There are three major categories for future work: Future work on the development of WILDS, future work pertaining to employment options of WILDS, and future work regarding deception detection technologies.

The next step in the development of WILDS would be the legal and ethical review. Following that verification, all parties involved in the implementation of WILDS—the interrogation teams, including military police and intelligence personnel—need to validate WILDS meets all the necessary requirements during interrogation operations. Upon completion of both reviews, the prototyping phase should begin. Prototyping development would require an in-depth knowledge on the following areas: BCI, thermal sensors, heart rate sensors, facial recognition, natural language processing, and the algorithms needed to integrate the data from these sensors. Additional considerations should include a basic understanding in material engineering, to build a field-ready system, and sensor processing.

The prototyping would consist of developing a single machine which would be present in the interrogation room and provided the inputs required for WILDS. Finally, a user-friendly display would need development; this display would communicate both a likelihood rating and a confidence level to the operator. Upon the completion of prototyping WILDS, there would be a need for testing and evaluation. This testing and evaluation phase would need to include 1) testing the designed machine to ensure all sensors are functional in both the laboratory environment as well as in a field environment and 2) the comparison of human only vice the employment of WILDS deception detection.

Separate from the future work on the development of WILDS would be the development of employment options for WILDS. This would include investigating other military applications, other intelligence community applications, and generally other government agencies. Future work could include the development of a variation on WILDS which could assist during Key Leader Engagements or other various Human Intelligence gathering operations where it would be critical to know if a person is lying outside of the interrogation room. Outside the military but still inside the Intelligence Community employing WILDS for the purpose of conducting interrogations or other Human Intelligence operations not specified to military operations, such as the identification of insider threats could be beneficial. Additionally, investigating if the same type of system is leverageable for the purposes of the Department of Homeland Security operations, Federal Bureau of Investigation criminal investigations, or even the local police force conducting criminal investigations. These domestic applications would again require both legal and ethical reviews to ensure the maintenance of rights to privacy.

As various technologies continue to emerge and develop, it is critical that military planners and leaders continue to monitor their advancement for the purposes of leveraging them for deception detection. Fields of study which are continuing to develop rapidly include biometric sensors, cognitive science, and artificial intelligence. Additionally, any advancement in network security and computer security would also be of benefit to the deception detection field. Future work in any of these fields, while pairing it with the psychological perspectives on deception detection will provide continual advancements within this field.

C. FINAL THOUGHTS

If, as Sun Tze asserts, all warfare is based on deception, then being able to detect deception provides a significant advantage on the battlefield. The DOD's and the Marine Corps' current approach to detecting deception during interrogation is as accurate as guessing heads or tails when flipping a coin. Improvement is both necessary and achievable. A system that can take advantage of the multiple biometric indicators present, in real time at the moment of deception, would fundamentally shift HUMINT operations. This is particularly the case if this system engenders trust by providing likelihood and confidence metrics to the operator. By leveraging these various technologies, integrating them into a dynamic system, and employing them with the purpose of detecting deception in enemy combatants, the DOD and Marine Corps can take what would be the flip of a coin and produce higher fidelity results, ultimately enhancing intelligence collected and counterintelligence operations.

Within the discipline of systems engineering, there are various modeling approaches to systems designing. We selected the OFM as the best approach because it enables both human processes and machine processes modeling within a single design concept, contributing directly to achieving the goal of the model. Other various models fall short in modeling the human processes impact on the design of a given system. OFM is inclusive and holistic for human-machine team pairing system design.

The DOD and the Marine Corps have the opportunity to gain an advantage over any enemy. Being able to detect deception when the stakes are high is just as critical as accurately inputting targeting data. On today's battlefield, we rely heavily on human-machine teams to do everything from monitoring maintenance to putting bombs on a target. Detecting deception can be no different. Employing a machine that can assist us in facilitating the gathering of information to be the best on the battlefield provides an asymmetric advantage.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Amber, Faryal, Adeel Yousaf, Muhammad Imran, and Khurram Khurshid. "P300 Based Deception Detection Using Convolutional Neural Network." In *2019 2nd International Conference on Communication, Computing and Digital Systems (C-CODE)*, 201–4. Islamabad, Pakistan: IEEE, 2019. https://doi.org/10.1109/C-CODE.2019.8681025.

American Psychological Association. "The Truth About Lie Detectors (Aka Polygraph Tests)." https://www.apa.org, August 5, 2004. https://www.apa.org/research/action/polygraph.

Andrew Kozel, F., Kevin A. Johnson, Emily L. Grenesko, Steven J. Laken, Samet Kose, Xinghua Lu, Dean Pollina, Andrew Ryan, and Mark S. George. "Functional MRI Detection of Deception after Committing a Mock Sabotage Crime*." *Journal of Forensic Sciences* 54, no. 1 (January 2009): 220–31. https://doi.org/10.1111/j.1556-4029.2008.00927.x.

Breuer, William B. *Hoodwinking Hitler: The Normandy Deception*. Westport: Praeger Publishers, 1993.

Bunge, S.A., and I. Kahn. "Cognition: An Overview of Neuroimaging Techniques." In *Encyclopedia of Neuroscience*, edited by Larry R. Squire, 1063–67. Cambridge: Academic Press, 2009. https://doi.org/10.1016/B978-008045046-9.00298-9.

Burgoon, Judee, Jay Jr, Joey George, and David Biros. *Detecting Deception in the Military Infosphere: Improving and Integrating Human Detection Capabilities with Automated Tools.* Report Number AFRL-SR-AR-TR-07-0193. Arlington, VA: AF Office of Scientific Research, April 25, 2007. https://www.researchgate.net/publication/235028335_Detecting_Deception_in_the_Military_Infosphere_Improving_and_Integrating_Human_Detection_Capabilities_with_Automated_Tools/link/0f31752e68cf733e76000000/download.

Chang, Wenwen, Hong Wang, Chengcheng Hua, Qiaoxiu Wang, and Yue Yuan. "Comparison of Different Functional Connectives Based on EEG during Concealed Information Test." *Biomedical Signal Processing and Control* 49 (March 2019): 149–59. https://doi.org/10.1016/j.bspc.2018.12.008.

Christ, S. E., D. C. Van Essen, J. M. Watson, L. E. Brubaker, and K. B. McDermott. "The Contributions of Prefrontal Cortex and Executive Control to Deception: Evidence from Activation Likelihood Estimate Meta-Analyses." *Cerebral Cortex* 19, no. 7 (July 1, 2009): 1557–66. https://doi.org/10.1093/cercor/bhn189.

Clark, Tiffany. "Integrity-Based Trust Violations within Human-Machine Teaming." Master's thesis, Naval Postgraduate School, 2018. http://calhoun.nps.edu/handle/10945/59637.

Conway, Lucian Gideon, Kathrene R. Conway, and Shannon C. Houck. "Validating Automated Integrative Complexity: Natural Language Processing and the Donald Trump Test." *Journal of Social and Political Psychology* 8, no. 2 (September 30, 2020): 504–24. https://doi.org/10.5964/jspp.v8i2.1307.

Daneshi Kohan, Marzieh, Ali Motie Nasrabadi, Mohammad Bagher Shamsollahi, and Ali Sharifi. "EEG/PPG Effective Connectivity Fusion for Analyzing Deception in Interview." *Signal, Image and Video Processing* 14, no. 5 (July 2020): 907–14. https://doi.org/10.1007/s11760-019-01622-1.

Daneshi Kohan, Marzieh, Ali Motie Nasrabadi, Ali sharifi, and Mohammad Bagher Shamsollahi. "Interview Based Connectivity Analysis of EEG in Order to Detect Deception." *Medical Hypotheses* 136 (March 2020): 109517. https://doi.org/10.1016/j.mehy.2019.109517.

Department of Defense. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. DOD Directive 3115.09. Washington, DC: Department of Defense, 2020. https://fas.org/irp/doddir/dod/d3115_09.pdf.

———. *Polygraph and Credibility Assessment Procedures*. DOD Directive 5210.91. Washington, DC: Department of Defense, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/521091p.pdf?ver=2019-04-22-104603-167.

Department of the Army. *Detainee Operations*. FM 3-63. Washington, DC: Department of the Army, 2020.

———. *Human Intelligence Collector Operations*. FM 2-22.3. Washington, DC: Department of the Army, 2006. https://fas.org/irp/doddir/army/fm2-22-3.pdf.

Director of National Intelligence. *Analytic Standards*. IC Directive 203. Washington, DC: Office of the Director of National Intelligence, 2015. https://fas.org/irp/dni/icd/icd-203.pdf.

Dong, Suh-Yeon, Bo-Kyeong Kim, and Soo-Young Lee. "Implicit Agreeing/Disagreeing Intention While Reading Self-Relevant Sentences: A Human FMRI Study." *Social Neuroscience* 11, no. 3 (May 3, 2016): 221–32. https://doi.org/10.1080/17470919.2015.1059362.

Ekman, Paul, and Maureen O'Sullivan. "Who Can Catch a Liar?" *American Psychologist* 46, no. 9 (1991): 913–20. https://doi.org/10.1037/0003-066X.46.9.913.

Elkins, Aaron C, Judee Burgoon, and Jay Nunamaker. "Vocal Analysis Software for Security Screening Validity and Deception Detection Potential." *Homeland Security Affairs* April (2012): 6.

NIRx Medical Technologies. "FAQ on NIRS." Accessed June 4, 2021. https://nirx.net/faq.

Farwell, Lawrence A., and Emanuel Donchin. "The Truth Will Out: Interrogative Polygraphy ('Lie Detection') With Event-Related Brain Potentials." *Psychophysiology* 28, no. 5 (September 1991): 531–47. https://doi.org/10.1111/j.1469-8986.1991.tb01990.x.

Farwell, Lawrence A., Drew C. Richardson, Graham M. Richardson, and John J. Furedy. "Brain Fingerprinting Classification Concealed Information Test Detects U.S. Navy Military Medical Information with P300." *Frontiers in Neuroscience* 8 (December 23, 2014). https://doi.org/10.3389/fnins.2014.00410.

Ferree, T.C, M.T Clay, and D.M Tucker. "The Spatial Resolution of Scalp EEG." *Neurocomputing* 38–40 (June 2001): 1209–16. https://doi.org/10.1016/S0925-2312(01)00568-9.

Fuller, Christie M., David P. Biros, and Rick L. Wilson. "Decision Support for Determining Veracity via Linguistic-Based Cues." *Decision Support Systems* 46, no. 3 (February 2009): 695–703. https://doi.org/10.1016/j.dss.2008.11.001.

Gamer, Matthias. "Mind Reading Using Neuroimaging: Is This the Future of Deception Detection?" *European Psychologist* 19, no. 3 (January 1, 2014): 172–83. https://doi.org/10.1027/1016-9040/a000193.

Gao, Junfeng, Hongjun Tian, Yong Yang, Xiaolin Yu, Chenhong Li, and Nini Rao. "A Novel Algorithm to Enhance P300 in Single Trials: Application to Lie Detection Using F-Score and SVM." Edited by Hans A. Kestler. *PLoS ONE* 9, no. 11 (November 3, 2014): e109700. https://doi.org/10.1371/journal.pone.0109700.

Glikson, Ella, and Anita Williams Woolley. "Human Trust in Artificial Intelligence: Review of Empirical Research." *Academy of Management Annals* 14, no. 2 (July 2020): 627–60. https://doi.org/10.5465/annals.2018.0057.

Grubin, Don, and Lars Madsen. "Lie Detection and the Polygraph: A Historical Review." *Journal of Forensic Psychiatry & Psychology* 16, no. 2 (June 2005): 357–69. https://doi.org/10.1080/14789940412331337353.

Hancock, Jeffrey T., Lauren E. Curry, Saurabh Goorha, and Michael Woodworth. "On Lying and Being Lied To: A Linguistic Analysis of Deception in Computer-Mediated Communication." *Discourse Processes* 45, no. 1 (December 17, 2007): 1–23. https://doi.org/10.1080/01638530701739181.

Haynes, John-Dylan, and Geraint Rees. "Decoding Mental States from Brain Activity in Humans." *Nature Reviews Neuroscience* 7, no. 7 (July 2006): 523–34. https://doi.org/10.1038/nrn1931.

Hernandez-Fernaud, Estefania, and Marisa Alonso-Quecuty. "The Cognitive Interview and Lie Detection: A New Magnifying Glass for Sherlock Holmes?" *Applied Cognitive Psychology* 11, no. 1 (1997): 55–68. https://doi.org/10.1002/(SICI)1099-0720(199702)11:1<55::AID-ACP423>3.0.CO;2-G

Hollnagel, Erik, and David D. Woods. "Cognitive Systems Engineering: New Wine in New Bottles." *International Journal of Man-Machine Studies* 18, no. 6 (June 1983): 583–600. https://doi.org/10.1016/S0020-7373(83)80034-0.

Honts, Charles R., Steven Thurber, and Mark Handler. "A Comprehensive Meta-analysis of the Comparison Question Polygraph Test." *Applied Cognitive Psychology* 35, no. 2 (March 2021): 411–27. https://doi.org/10.1002/acp.3779.

Houck, Shannon C., James McFarland, Laura V. Machia, and Lucian Gideon Conway. "When Beliefs Lead to (Im)Moral Action: How Believing in Torture's Effectiveness Shapes the Endorsement of Its Use." *Political Psychology* 40, no. 6 (2019): 1315–39. https://doi.org/10.1111/pops.12590.

LIWC. "How It Works." Accessed June 5, 2021. http://liwc.wpengine.com/how-it-works/.

Hu, Guosheng, Li Liu, Yang Yuan, Zehao Yu, Yang Hua, Zhihong Zhang, Fumin Shen et al. "Deep Multi-Task Learning to Recognise Subtle Facial Expressions of Mental States." In *Computer Vision – ECCV 2018*, edited by Vittorio Ferrari, Martial Hebert, Cristian Sminchisescu, and Yair Weiss, 11216:106–23. *Lecture Notes in Computer Science.* Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-030-01258-8_7.

INCOSE. "Systems Engineering Definition." Accessed June 4, 2021. https://www.incose.org/about-systems-engineering/system-and-se-definition/systems-engineering-definition#ENGINEERED_SYSTEM.

Jacovi, Alon, Ana Marasović, Tim Miller, and Yoav Goldberg. "Formalizing Trust in Artificial Intelligence: Prerequisites, Causes and Goals of Human Trust in AI." In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 624–35. FAccT '21. New York, NY, USA: Association for Computing Machinery, 2021. https://doi.org/10.1145/3442188.3445923.

Janoff-Bulman, Ronnie. "Erroneous Assumptions: Popular Belief in the Effectiveness of Torture Interrogation." *Peace and Conflict: Journal of Peace Psychology* 13, no. 4 (November 2007): 429–35. http://dx.doi.org.libproxy.nps.edu/10.1080/10781910701665766.

Joint Chiefs of Staff. *Detainee Operations*. JP 3-63. Washington, DC: Joint Chiefs of Staff, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_63.pdf.

Joint Chiefs of Staff. "Joint and National Intelligence Support to Military Operations." Fort Belvoir, VA: Defense Technical Information Center, October 7, 2004. https://doi.org/10.21236/ADA508665.

Keller-McNulty, S. "Quest for Truth: Deception and Intent Detection." Ft. Belvoir, VA: The MITRE Corporation; JASON Program Office, October 29, 2008. https://fas.org/irp/agency/dod/jason/quest.pdf.

Kim, Kiho, Go-eun Kim, and Jang-Han Lee. "Attentional Avoidance for Guilty Knowledge Among Deceptive Individuals." *Frontiers in Psychiatry* 10 (2019). https://doi.org/10.3389/fpsyt.2019.00114.

Kim, Kiho, Jiwon Kim, and Jang-Han Lee. "Guilt, Lying, and Attentional Avoidance of Concealed Information." *Social Behavior and Personality: An International Journal* 44, no. 9 (October 9, 2016): 1467–75. https://doi.org/10.2224/sbp.2016.44.9.1467.

Kleinberg, Bennett, and Bruno Verschuere. "How Humans Impair Automated Deception Detection Performance." *Acta Psychologica* 213 (February 2021): 103250. https://doi.org/10.1016/j.actpsy.2020.103250.

Kozel, F. Andrew, Kevin A. Johnson, Qiwen Mu, Emily L. Grenesko, Steven J. Laken, and Mark S. George. "Detecting Deception Using Functional Magnetic Resonance Imaging." *Biological Psychiatry* 58, no. 8 (October 15, 2005): 605–13. https://doi.org/10.1016/j.biopsych.2005.07.040.

Krapohl, Donald. Terminology Reference for the Science of Psychophysiological Detection of Deception. 3rd ed. Chattanooga, TN: American Polygraph Association, 2012.

Lai, Vivian, and Chenhao Tan. "On Human Predictions with Explanations and Predictions of Machine Learning Models: A Case Study on Deception Detection." In *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 29–38. Atlanta GA USA: ACM, 2019. https://doi.org/10.1145/3287560.3287590.

Lee, J.D., and T.F. Sanquist. "Augmenting the Operator Function Model with Cognitive Operations: Assessing the Cognitive Demands of Technological Innovation in Ship Navigation." *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 30, no. 3 (May 2000): 273–85. https://doi.org/10.1109/3468.844353.

Leng, Haizhou, Yanrong Wang, Qian Li, Lizhu Yang, and Yan Sun. "Sophisticated Deception in Junior Middle School Students: An ERP Study." *Frontiers in Psychology* 9 (January 11, 2019): 2675. https://doi.org/10.3389/fpsyg.2018.02675.

Lewis, Jerry A., and Michelle Cuppari. "The Polygraph: The Truth Lies Within." *Journal of Psychiatry & Law* 37, no. 1 (Spring 2009): 85–92. https://doi.org/10.1177/009318530903700107.

Li, Fang, Huilin Zhu, Jie Xu, Qianqian Gao, Huan Guo, Shijing Wu, Xinge Li, and Sailing He. "Lie Detection Using FNIRS Monitoring of Inhibition-Related Brain Regions Discriminates Infrequent but Not Frequent Liars." *Frontiers in Human Neuroscience* 12 (March 13, 2018): 71. https://doi.org/10.3389/fnhum.2018.00071.

Lisofsky, Nina, Philipp Kazzer, Hauke R. Heekeren, and Kristin Prehn. "Investigating Socio-Cognitive Processes in Deception: A Quantitative Meta-Analysis of Neuroimaging Studies." *Neuropsychologia* 61 (August 2014): 113–22. https://doi.org/10.1016/j.neuropsychologia.2014.06.001.

Lui, Ming, and J. Peter Rosenfeld. "The Application of Subliminal Priming in Lie Detection: Scenario for Identification of Members of a Terrorist Ring." *Psychophysiology* 46, no. 4 (July 2009): 889–903. https://doi.org/10.1111/j.1469-8986.2009.00810.x.

Mameli, Francesca, Cristina Scarpazza, Emanuele Tomasini, Roberta Ferrucci, Fabiana Ruggiero, Giuseppe Sartori, and Alberto Priori. "The Guilty Brain: The Utility of Neuroimaging and Neurostimulation Studies in Forensic Field." *Reviews in the Neurosciences* 28, no. 2 (February 1, 2017): 161–72. https://doi.org/10.1515/revneuro-2016-0048.

Marks, Jay W. "Medical Definition of Torture." MedicineNet, June 3, 2021. https://www.medicinenet.com/torture/definition.htm.

Mathur, Leena, and Maja J. Matarić. "Introducing Representations of Facial Affect in Automated Multimodal Deception Detection." In *Proceedings of the 2020 International Conference on Multimodal Interaction*, 305–14. Virtual Event Netherlands: ACM, 2020. https://doi.org/10.1145/3382507.3418864.

Mayer, Roger C., James H. Davis, and F. David Schoorman. "An Integrative Model of Organizational Trust." *The Academy of Management Review* 20, no. 3 (1995): 709–34. https://doi.org/10.2307/258792.

Meek, Scott W., Michelle C. Phillips, Corey P. Boswell, and Jennifer M.C. Vendemia. "Deception and the Misinformation Effect: An Event-Related Potential Study." *International Journal of Psychophysiology* 87, no. 1 (January 2013): 81–87. https://doi.org/10.1016/j.ijpsycho.2012.11.004.

Memon, Amina, Christian A. Meissner, this link will open in a new window Link to external site, and Joanne Fraser. "The Cognitive Interview: A Meta-Analytic Review and Study Space Analysis of the Past 25 Years." *Psychology, Public Policy, and Law* 16, no. 4 (November 2010): 340–72. http://dx.doi.org.libproxy.nps.edu/10.1037/a0020518.

Muller, Amanda C., and S. Narayanan. "Cognitively-Engineered Multisensor Image Fusion for Military Applications." *Information Fusion* 10, no. 2 (April 2009): 137–49. https://doi.org/10.1016/j.inffus.2008.08.008.

Nahari, Tal, Oryah Lancry-Dayan, Gershon Ben-Shakhar, and Yoni Pertzov. "Detecting Concealed Familiarity Using Eye Movements: The Role of Task Demands." *Cognitive Research: Principles and Implications* 4, no. 1 (March 29, 2019): 10. https://doi.org/10.1186/s41235-019-0162-7.

Neuman, Yair, Dan Assaf, and Navot Israeli. "Identifying the Location of a Concealed Object through Unintentional Eye Movements." *Frontiers in Psychology* 6 (April 8, 2015). https://doi.org/10.3389/fpsyg.2015.00381.

Ofen, Noa, Susan Whitfield-Gabrieli, Xiaoqian J. Chai, Rebecca F. Schwarzlose, and John D. E. Gabrieli. "Neural Correlates of Deception: Lying about Past Events and Personal Beliefs." *Social Cognitive and Affective Neuroscience* 12, no. 1 (January 1, 2017): 116–27. https://doi.org/10.1093/scan/nsw151.

Orlando, James. "Interrogation Techniques." Office of Legislative Research. Accessed June 4, 2021. https://www.cga.ct.gov/2014/rpt/2014-R-0071.htm.

OrShea, James, Keeley Crockett, Wasiq Khan, Philippos Kindynis, Athos Antoniades, and Georgios Boultadakis. "Intelligent Deception Detection through Machine Based Interviewing." In *2018 International Joint Conference on Neural Networks (IJCNN)*, 1–8. Rio de Janeiro: IEEE, 2018. https://doi.org/10.1109/IJCNN.2018.8489392.

Pentland, Steven J., Nathan W. Twyman, Judee K. Burgoon, Jay F. Nunamaker Jr, and Christopher B. R. Diller. "A Video-Based Screening System for Automated Risk Assessment Using Nuanced Facial Features." *Journal of Management Information Systems* 34, no. 4 (October 2, 2017): 970–93. https://doi.org/10.1080/07421222.2017.1393304.

Pérez-Rosas, Verónica, Mohamed Abouelenien, Rada Mihalcea, and Mihai Burzo. "Deception Detection Using Real-Life Trial Data." In *Proceedings of the 2015 ACM on International Conference on Multimodal Interaction*, 59–66. Seattle Washington USA: ACM, 2015. https://doi.org/10.1145/2818346.2820758.

Potember, Richard. “Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DOD.” Alexandria, VA: The MITRE Corporation; JASON Program Office, January 2017. https://fas.org/irp/agency/dod/jason/ai-dod.pdf.

Potter, Scott S., David D. Woods, Emilie M. Roth, Jennifer Fowlkes, and Robert R. Hoffman. “Evaluating the Effectiveness of a Joint Cognitive System: Metrics, Techniques, and Frameworks.” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 50, no. 3 (October 2006): 314–18. https://doi.org/10.1177/154193120605000322.

Robinette, Paul, Ayanna M. Howard, and Alan R. Wagner. “Effect of Robot Performance on Human–Robot Trust in Time-Critical Situations.” *IEEE Transactions on Human-Machine Systems* 47, no. 4 (August 2017): 425–36. https://doi.org/10.1109/THMS.2017.2648849.

Rubin, Victoria L. “On Deception and Deception Detection: Content Analysis of Computer-Mediated Stated Beliefs.” *Proceedings of the American Society for Information Science and Technology* 47, no. 1 (2010): 1–10. https://doi.org/10.1002/meet.14504701124.

Rubin, Victoria L., and Tatiana Lukoianova. “Truth and Deception at the Rhetorical Structure Level.” *Journal of the Association for Information Science and Technology* 66, no. 5 (2015): 905–17. https://doi.org/10.1002/asi.23216.

Salem, Maha, Gabriella Lakatos, Farshid Amirabdollahian, and Kerstin Dautenhahn. “Would You Trust a (Faulty) Robot?: Effects of Error, Task Type and Personality on Human-Robot Cooperation and Trust.” In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction*, 141–48. Portland Oregon USA: ACM, 2015. https://doi.org/10.1145/2696454.2696497.

Salvati, Joeann M., and Shannon C. Houck. “Examining the Causes and Consequences of Confession-Eliciting Tactics during Interrogation.” *Journal of Applied Security Research* 14, no. 3 (July 3, 2019): 241–56. https://doi.org/10.1080/19361610.2019.1621508.

Schaefer, Kristin E., Deborah R. Billings, James L. Szalma, Jeffrey K. Adams, Tracy L. Sanders, Jessie Y. Chen, and Peter A. Hancock. “A Meta-Analysis of Factors Influencing the Development of Trust in Automation: Implications for Human-Robot Interaction:” Fort Belvoir, VA: Defense Technical Information Center, July 1, 2014. https://doi.org/10.21236/ADA607926.

Schramm, Wilber, and Donald Roberts. “How Communication Works.” In *The Process and Effects of Mass Communication*, Rev., 1–24. Urbana: University Of Illinois Press, 1971.

Spence, Sean A., Tom F. D. Farrow, Amy E. Herford, Iain D. Wilkinson, Ying Zheng, and Peter W. R. Woodruff. "Behavioural and Functional Anatomical Correlates of Deception in Humans:" *Neuroreport* 12, no. 13 (September 2001): 2849–53. https://doi.org/10.1097/00001756-200109170-00019.

Spiroiu, Flavia. "The Impact of Beliefs Concerning Deception on Perceptions of Nonverbal Behavior: Implications for Neuro-Linguistic Programming-Based Lie Detection." *Journal of Police and Criminal Psychology* 33, no. 3 (September 1, 2018): 244–56. https://doi.org/10.1007/s11896-018-9278-9.

Su, Lin, and Martin Levine. "Does 'Lie to Me' Lie to You? An Evaluation of Facial Clues to High-Stakes Deception." *Computer Vision and Image Understanding*, Spontaneous Facial Behaviour Analysis, 147 (June 1, 2016): 52–68. https://doi.org/10.1016/j.cviu.2016.01.009.

Sullivan, Christopher Michael. "The (in)Effectiveness of Torture for Combating Insurgency." *Journal of Peace Research* 51, no. 3 (May 1, 2014): 388–404. https://doi.org/10.1177/0022343313520023.

https://www.apa.org. "The Truth About Lie Detectors (Aka Polygraph Tests)," August 5, 2004. https://www.apa.org/research/action/polygraph.

Programmer Backpack. "Top Natural Language Processing (NLP) Algorithms And Techniques For Beginners," June 21, 2020. https://programmerbackpack.com/top-natural-language-processing-nlp-algorithms-and-techniques-for-beginners/.

U.S. Marine Corps. *Counterintelligence*. MCWP 2-6. Quantico, VA: U.S. Marine Corps, 2004. https://www.marines.mil/Portals/1/Publications/MCWP%202-6%20W%20Erratum%20Counterintelligence.pdf.

———. *Enemy Prisoners of War, Retained Personnel, Civilian Interness, and Other Detainees*. MCO 3461.1. Quantico, VA: U.S. Marine Corps, 1997. https://www.marines.mil/Portals/1/Publications/MCO%203461.1.pdf.

Vega, Roberto, Ana G. Hernandez-Reynoso, Emily Kellison Linn, Rita Q. Fuentes-Aguilar, Gildardo Sanchez-Ante, Arturo Santos-Garcia, and Alejandro Garcia-Gonzalez. "Hemodynamic Pattern Recognition During Deception Process Using Functional Near-Infrared Spectroscopy." *Journal of Medical and Biological Engineering* 36, no. 1 (February 2016): 22–31. https://doi.org/10.1007/s40846-016-0103-6.

Vinanzi, Samuele, Massimiliano Patacchiola, Antonio Chella, and Angelo Cangelosi. "Would a Robot Trust You? Developmental Robotics Model of Trust and Theory of Mind." *Philosophical Transactions of the Royal Society B: Biological Sciences* 374, no. 1771 (April 29, 2019): 20180032. https://doi.org/10.1098/rstb.2018.0032.

Vrij, Aldert, Samantha A. Mann, Ronald P. Fisher, Sharon Leal, Rebecca Milne, and Ray Bull. "Increasing Cognitive Load to Facilitate Lie Detection: The Benefit of Recalling an Event in Reverse Order." *Law and Human Behavior* 32, no. 3 (June 2008): 253–65. http://dx.doi.org.libproxy.nps.edu/10.1007/s10979-007-9103-y.

Vrij, Aldert, Christian A. Meissner, Ronald P. Fisher, Saul M. Kassin, Charles A. Morgan, and Steven M. Kleinman. "Psychological Perspectives on Interrogation." *Perspectives on Psychological Science* 12, no. 6 (November 2017): 927–55. https://doi.org/10.1177/1745691617706515.

Warmelink, Lara, Anna Subramanian, Daria Tkacheva, and Neil McLatchie. "Unexpected Questions in Deception Detection Interviews: Does Question Order Matter?" *Legal and Criminological Psychology* 24, no. 2 (September 2019): 258–72. https://doi.org/10.1111/lcrp.12151.

Weyers, Benjamin, Judy Bowen, Alan Dix, and Philippe Palanque, eds. *The Handbook of Formal Methods in Human-Computer Interaction*. Human–Computer Interaction Series. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-51838-1.

Xiong, Yijun, junfeng Gao, and Ran Chen. "Connectivity Network Analysis of EEG Signals for Detecting Deception." *Journal of Physics: Conference Series* 1176 (March 2019): 032051. https://doi.org/10.1088/1742-6596/1176/3/032051.

Yagoda, Rosemarie E., and Douglas J. Gillan. "You Want Me to Trust a ROBOT? The Development of a Human–Robot Interaction Trust Scale." *International Journal of Social Robotics* 4, no. 3 (August 2012): 235–48. https://doi.org/10.1007/s12369-012-0144-0.

Yeung, Douglas, Rebecca Balebako, Carlos Gutierrez Gaviria, and Michael Chaykowsky. *Face Recognition Technologies: Designing Systems That Protect Privacy and Prevent Bias*. RAND Corporation, 2020. https://doi.org/10.7249/RR4226.

Yu, Junhong, Qian Tao, Ruibin Zhang, Chetwyn C.H. Chan, and Tatia M.C. Lee. "Can FMRI Discriminate between Deception and False Memory? A Meta-Analytic Comparison between Deception and False Memory Studies." *Neuroscience & Biobehavioral Reviews* 104 (September 2019): 43–55. https://doi.org/10.1016/j.neubiorev.2019.06.027.

Yuan, Zhen, and Xiaohong Lin. "Mapping of the Brain Activation Associated with Deception Using Fused EEG and FNIRS." In *Neural Imaging and Sensing 2019*, edited by Qingming Luo, Jun Ding, and Ling Fu, 14. San Francisco: SPIE, 2019. https://doi.org/10.1117/12.2508257.

Zhang, Jiang, Jingyue Zhang, Houhua Ren, Qihong Liu, Zhengcong Du, Lan Wu, Liyang Sai, Zhen Yuan, Site Mo, and Xiaohong Lin. “A Look Into the Power of FNIRS Signals by Using the Welch Power Spectral Estimate for Deception Detection.” *Frontiers in Human Neuroscience* 14 (January 18, 2021): 606238. https://doi.org/10.3389/fnhum.2020.606238.

Zhou, Lina, Judee K. Burgoon, Jay F. Nunamaker, and Doug Twitchell. “Automating Linguistics-Based Cues for Detecting Deception in Text-Based Asynchronous Computer-Mediated Communications.” *Group Decision and Negotiation* 13, no. 1 (January 2004): 81–106.

Zloteanu, Mircea, Peter Bull, Eva G Krumhuber, and Daniel C Richardson. “Veracity Judgement, Not Accuracy: Reconsidering the Role of Facial Expressions, Empathy, and Emotion Recognition Training on Deception Detection.” *Quarterly Journal of Experimental Psychology* 74, no. 5 (May 1, 2021): 910–27. https://doi.org/10.1177/1747021820978851.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California