AIR WAR COLLEGE

AIR UNIVERSITY

VIRTUAL REALITY AS A TOOL FOR INSIDER THREAT MITGATION AND BACKGROUND SECURITY INVESTIGATION IMPROVEMENT

by

Melissa S. Walker, Office of the Secretary of Defense, Office of the Chief Management Officer

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Tony Millican, Ph.D.

26 April 2018

DISCLAIMER

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

Table of Contents

Biography

Melissa S. Walker is assigned to the Air War College, Air University, Maxwell AFB, Alabama. In her current position as a Senior Policy Analyst in the Office of the Secretary of Defense (OSD), Office of the Chief Management Officer, Ms. Walker is responsible for working with staff and the public to facilitate solutions to Freedom of Information Act (FOIA) issues throughout 33 DoD Components including Air Force, Army, Navy, OSD, Defense Contract Management Agency (DCMA), and others. She also authors the annual Department of Defense (DoD) Chief FOIA Officer's Report. Ms. Walker previously served as the Director of Navy Archives where she directed an archival staff and contractors in supporting a 180 million-page archival collection. Prior to that, she was the Director of Correspondence Control and Policy at DCMA where she served as a senior operations officer responsible for six major agency-wide programs including correspondence and tasking, policy, protocol and FOIA programs. Previously, Ms. Walker served as the Chief of the Army Declassification Activity where she executed automatic declassification review for the Department of the Army and worked closely with the staff of the Undersecretary of Defense for Intelligence on changes to the Executive Orders on classification and the Manual governing the DoD Information Security Program.

Abstract

This research paper suggests that augmented reality/virtual reality (AR/VR) can improve security by reducing insider threat risk and introducing efficiencies in the background investigation security clearance processes. Insider threats may refer to classified information leaks, such as those by Private Manning and Edward Snowden, or physical attacks similar to that of the Washington Navy Yard in 2013. The background security clearance process is partially designed to evaluate whether individuals are trustworthy, and the amount of information and interviews involved in the processes of evaluating someone for a clearance inevitably introduces backlogs spanning months and years. VR technology originally dates from the 1960s and new developments in both software and hardware have transformed the field. In fact, VR and related technologies are poised to generate a significant leap forward in security professional efficiency by combining VR with basic human psychology and biological indicators to evaluate trustworthiness when determining who may represent an insider threat and who should be granted a clearance. Additionally, AR/VR offers multiple levels of training opportunities for the incoming security professional, the seasoned professional, and the individuals entrusted with national security information. The technology also offers a significant return on investment because commercially available equipment is relatively inexpensive and, if widely implemented, using the technology may generate immediate savings in travel costs, manpower, and a dramatic decline in backlogs. Challenges include the predictable concerns with defeating or tricking a system, system security, data integrity, and professional acceptance.

Introduction

This research paper uses a qualitative approach to argue that augmented reality/virtual reality (AR/VR) can improve security by reducing insider threat risk and improving security professional efficiency in background investigation security clearance processes. The current Department of Defense and Headquarters United States Air Force requirements to implement insider threat mitigation and find solutions for security clearance delays are not mutually exclusive challenges. New research on trustworthiness indicators suggest the need to reevaluate existing risk models for both insider threats and the security clearance process.[1]. Based on this new research, VR has potential to provide an avenue to dramatically change how the United States identifies insider threats, grants clearances, educates, and trains about national security. Potential returns on investment stretch beyond the millions of dollars spent on manpower to the fundamental point of securing the nation's secrets.

Surmounting the aforementioned challenges includes formulating a risk model that focuses efforts on those who are not as trustworthy as others and concentrating immersive training on reinforcing positive behavior to mitigate insider threat potential coupled with improving overall security professional effectiveness.

While the term "insider threat" generally has broader understanding in the information technology (IT) world, it holds a particular place of interest in the United States government as it relates to damage that can be caused by personnel trusted with access to controlled, sensitive, and national security information. Insider threats may refer to classified information leaks, such as those by Private Manning and Edward Snowden, or physical attacks similar to that of the Washington Navy Yard in 2013. Security professionals hold a wide range of positions, from a weapon-carrying guard charged with physical security, to the personal data-driven investigator charged with personnel security, to the information-holders charged with information security. Of the many strands in the security profession, the focus here is on two aspects: insider threats to national security information, and security professionals concerned with personnel security.

This paper is divided into sections that establish a common understanding of the insider threat problem, explain the fundamental process of background investigations for security clearances and costs, and review the history of AR/VR including the technology’s professional applications. Then the potential intersections of AR/VR with insider threat and security clearances are explored and how those, in turn, can produce efficiencies in training within the security profession. Training possibilities are explored for the incoming security professional, the seasoned professional, and the individuals who are required to protect information. Finally, recommendations for implementing the technology in the security profession are discussed, as well as an examination of the challenges of using this technology as a form of polygraph in determining trustworthiness.

Insider Threat

The insider threat risk gained much attention after the dramatic world-wide unauthorized information release by Private First Class Bradley (now private citizen Chelsea) Manning to the online organization WikiLeaks. As a result of the significant loss of information control the President signed Executive Order (EO) 13587 and released a Fact Sheet related to improving the way agencies guard against and handle insider threats. The EO established additional criteria for appropriately safeguarding and sharing information on classified networks and established the National Insider Threat Task Force (NITTF).[2]

Further calls for insider threat reform after EO 13587 were followed by the shooting at the Washington Navy Yard (WNY), DC, as well as additional unauthorized information releases by Edward Snowden. The United States Congress held multiple hearings on insider threats and what actions federal agencies were taking to mitigate dangers presented by these different insider threat situations. There was particular concern when it was revealed in the after-action review of the Edward Snowden incident that his security clearance background investigation was incomplete, yet it did not prevent his final clearance from being granted.[3] More questions followed concerns regarding how the WNY shooter could have undisclosed felony weapons charges and still manage to obtain a clearance.[4]

Others have criticized the United States for waiting for attackers to strike instead of taking proactive measures to prevent attacks. One insider threat expert, Gary Jackson, said, "[p]redictive, proactive security is the answer…" and that the United States must "…combine computer science with psychology to get at the root of the problem, not just treat the symptom."[5] He went on to indicate that applied behavior analysis recognizes that behavior change, "…occurs in response to preceding events and situations we call antecedents and is encouraged to occur or not occur by the consequences of the behavior that immediately follow."[6] He summarizes this concept as, "[p]rediction of behavior is based on the underlying antecedents and consequences associated with past behavior."[7] Jackson went on to partner with the Air Force Research Lab (AFRL) in creating a predictive system for networked use as well as initiating similar experiments for VR which will be discussed below.

Additionally, the NITTF has been very active and released the *Insider Threat Program Maturity Framework*, on November 1, 2018, to aid agency programs in moving beyond the initial standards stemming from EO 13587. The *Maturity Framework* document recognized that, "[t]he insider threat is a dynamic problem set, requiring resilient and adaptable programs to address an evolving threat landscape, advances in technology, and organizational change."[8]

Professionals also generally agree that, "…insider threats remain statistically rare, making them more difficult to analyze, defend against, or anticipate."[9] The insider threat remains a significant issue for the United States government, and the language in the *Maturity Framework* document is an acknowledgement that, despite presidential administration changes, ongoing broad concerns about insider threats remain.

Background Investigations

One mechanism that has long been in place to prevent some incoming insider threats is the security clearance process. Security clearance background investigations are partly designed to determine the trustworthiness of individuals and whether they can be trusted with information that is classified in the interests of national security.[10] Trustworthiness is defined here as, "…*the propensity to fulfill another's positive implicit or explicit expectations regarding a particular action.*"[11] Unfortunately, many people find themselves awaiting completion of some portion of the background clearance investigation processes. In 2016, the number of personnel working with classified information and outside the period their clearances were to be updated was 374,000.[12] While that may seem like a large number of people waiting for updates, the number is a fraction of the overall number of clearance-holders. In her 2013 testimony, Government Accountability Office (GAO) employee Brenda Farrell indicated that 4.9 million personnel held, or were eligible to hold, clearances.[13] Part of the reform associated with insider threat is a reduction in the levels and overall numbers of clearances and as of October 2017, the number had been reduced to just over four million personnel holding clearances.[14] Despite the reductions, over 700,000 cases awaited completion of some portion of the process in September 2017, which precipitated GAO adding security clearances back on to the United States government high-risk list.[15] The high-risk list is a representation of areas of material weakness to the government that require mitigation either through more resources or reform.[16]

Furthermore, a large segment of the cleared population is within the Department of Defense (DoD) and Farrell also indicated that, "…DoD spent $787 million on suitability and security clearance background investigations in fiscal year 2011."[17] Another consideration is that as of 2016 the background investigation security clearance process for 75,000 new top secret clearances was taking an average of 200 days each to process from initiation to adjudication.[18] The total actual cost of the time elapsed to grant clearances is undetermined because personnel hired for positions requiring this level of clearance cannot do that work until the clearance is granted. Personnel in this situation may find themselves doing work incongruent with position requirements or decide to find another position. There were also over 150,000 clearances requiring periodic updates in 2016 and those each took an average of over 220 days.[19] At least personnel awaiting updates can generally continue doing the work in their own offices, but they may not be able to work with other offices because their clearance is technically out of scope.

The high-level overview of the background investigation process includes the candidate filling out the standard form 86 (SF-86), which can run over 100 pages in length, and electronically submitting it to an office that checks for completeness and then assigns the case to an investigator. The investigator reviews the SF-86, executes public information checks, engages in discussion with the person requiring a clearance, interviews the person's family, co-workers, and other character witnesses, and follows up on other leads generated during those discussions. The investigator writes the report and submits it for a completion check and then another security professional reviews the case and adjudicates whether the individual can be granted the clearance. If granted a clearance, the candidate then meets with their local security officer to complete the non-disclosure agreement acknowledging granting of the clearance and associated responsibilities that come with the clearance approval.

The time it takes an investigator to complete a report on an individual depends on how much the individual has moved around, traveled and/or acquired interests in real estate, the stock market or businesses. Time to completion also depends on whether the candidate's associates to be interviewed are physically local to the investigator's area or are passed to other investigators for contact. The more complicated a person's background, the more time it takes to execute the process because it involves human-driven methods to check information, verify authenticity, and establish connections required for finalizing reporting. Ultimately, as Gregory Marshall, Chief Security Officer, Department of Homeland Security said in his congressional testimony, "[a] background investigation is an exercise in risk management establishing some basic facts, but cannot guarantee any individual's continuing fitness to carry out their duties or to behave in a lawful or safe manner."[20] Moreover, Gary Jackson, an insider threat expert, indicates that, "[p]rediction of human behavior must begin with the basic understanding of human behavior – not statistics."[21] He completes that thought with two significant statements about insider threat, the first is that, "The key to espionage is deception and hiding."[22] The second statement is that, "Knowledge of behaviors requiring both expertise and deception can assist in the identification of an individual engaging in this type of theft."[23] The background clearance investigation is designed to unearth deception or attempts to hide information and thereby reduce risk to the government in sharing sensitive information, but the insider threat problem persists throughout an individual's career.

Nevertheless, holding a security clearance is not the only prerequisite to someone being an insider threat. In a report on espionage, the Defense Personnel and Security Research Center

(PERSEREC) indicated that between the periods of 1947-1979 and 1990-2007, of all espionage convictions, those of non-clearance holders increased from 20% to 37% during that time.[24] The same report indicates that, "[o]ne analysis argues that opportunity, conception, motive, lack of internal constraints, and ineffective external constraints are the necessary dimensions to commit espionage."[25] PERSERECs work in this arena continues to expand in both classified and unclassified reporting.[26] While it is in the interest of the United States to reduce insider threat, the fact that it remains high means more measures are required. This is an area where AR/VR may provide another tool facilitating more effective external constraints.

Augmented Reality and Virtual Reality

VR/AR started in the 1960s with Ivan Sutherland creating the "Sword of Damocles" prototype and the subsequent National Aeronautics and Space Administration (NASA) work which augmented reality with three-dimensional (3D) graphics as seen through a head mounted display (HMD) suspended from the ceiling.[27] Technology has progressed significantly since then and advanced to the point where multiple vendors now offer AR handheld devices, AR HMDs, and VR HMDs. These devices support excellent visual and auditory interaction. Anyone using a smartphone has access to applications supporting AR. A quick search for "augmented reality" will return applications for using the phone's camera, recording, and Global Positioning System (GPS) features. These AR applications have a broad range of unique capabilities that enable measuring things in real life, seeing what different paint colors look like on walls and how furniture will look like in personal spaces, stargazing using GPS to identify stars versus satellites based on the device's location, accessing additional features which appear to make real-life books, wine bottles, golf holes and any number of other things become 3D and interactive.[28]

However, VR is an entirely different experience than that of AR. The immersive quality of VR makes the experience seem real to the mind. The sense of presence, or having a real experience in the VR world in comparison to watching something on television, was described by students in one fear-based experiment as being unable to, "…accept how one could possibly experience the same feelings with 'just a screen.'"[29] Peter Rubin describes it as, "[w]hen VR is working well, your physical senses tell your brain that you're really experiencing the thing you're virtually experiencing, and your brain prompts your body to respond in kind. That's presence."[30] While the often-used aphorism that "a picture is worth a thousand words" is one with which most are familiar, it is exponentially true in VR with a quality HMD designed for and specifically dedicated to VR. The nature of VR allows people to become immersed in the experience in ways they do not with simple computer or television two-dimensional viewing. In fact, Jeremy Bailenson indicates from projects at his Stanford University research lab that, "VR feels real, and its effects on us resemble the effects of real experiences. Consequently, a VR experience is often better understood *not as a media experience, but as an actual experience*, with the attendant results for our behavior."[31] Despite some experiences not replicating a phot-realistic environment, the brain fills in visual gaps and the immersive nature of VR results in the mind focusing on the sense of presence, or being, in another place. It is this aspect that led Gary Jackson to explore the use of VR in understanding insider threats.

Professional Applications for AR/VR

At the Air Force Research Lab, Jackson developed an experiment to see whether real-world (RW) characteristics of participants could be predicted based on their behavior and characteristics in the virtual world (VW).[32] The participants in the VW use avatars, or digital representations of themselves, to participate in the experience. Sometimes avatars resemble humans, robots, or other imaginative digital images such as dinosaurs or objects. Jackson set up the test using the same theories used in the system for networked computers for finding insider threats. His team determined, "…that accurate predictors of RW person characteristics could be identified in the VW."[33] They also determined that, "[o]nce identified, the VW predictors can be used to determine characteristics of those who operate the avatars without any knowledge of the real-world person."[34] The personal characteristics used in Jackson's test are in the Neuroticism-Extraversion-Openness (NEO) Inventory, one of the five-factor personality assessments which provides insight into personality structures.

There are also a number of standalone HMDs on the commercial market that require wireless internet access but do not require a connection to a computer or a smartphone, though they have limited capabilities and hours of run-times between charges.[35] The standalone wireless-only HMD experiences, as of this writing, also cannot support as much graphics-intensive interaction because they lack the necessary graphics card processing capacity to deliver more in-depth experiences. Longer and more graphics-intensive experiences without battery limitations are available through HMDs connected to a laptop or desktop computer, although the rate at which technology is improving may lead to wireless experiences quickly imitating wired ones.

Another significant development in the field of VR/AR is that equipment has reached sufficient maturity level to facilitate reliable physiological information-gathering. Eye-tracking information can be gathered using HMDs and there are non-intrusive heart-rate monitors that can be added for simultaneous data-gathering.[36] Eye-tracking facilitates an understanding of what a user is allowing their gaze to rest on while the heart rate monitoring provides an expanded understanding of the body's reaction to stimuli. VR/AR applications vary from simplistic to extremely complex and VR applications are highly immersive due to the HMD directing focus to the sights and sounds delivered by the experience. In fact, “[a]pplications with gaze control in this field include the use of fixation on a particular item to facilitate selection, the use of gaze to infer intention.”[37] For centuries, two and three-dimensional artists have used color and other techniques to draw the eye to particular elements of their work. Yet, research is now demonstrating that VR allows for data collection that is, “…intimate and revealing: unlike speech, nonverbal behavior is automatic, a direct pipeline to our mental states, emotions, and identities.”[38] Xuezhong Wang and Brent Winslow further indicate that, “[i]t is reasonable to expect that insights with regard to underlying cognitive load will be obtained by investigating eye movements and patterns.”[39] For instance, James Bliss et al. indicate that, “[r]esearch has shown that pupil diameter varies according to changes in task demands with a range of cognitively based actions that index perception, reasoning, and memory.”[40] This information combined with heart rate data can be evaluated to more impartially judge the feedback from decision-making scenarios.

Existing Professional Applications with Potential for Adding to VR

Eye-tracking and heart-rate monitoring are only two aspects of revealing physiological information that can be gathered with portable systems. Electroencephalography (EEG) and electrodermal conductance, otherwise known as galvanic skin response (GSR), sensors are now available in small, portable formats that are candidates for incorporation into HMD and handset systems. EEG information is used for capturing responses to presented stimulus and registering detection, such as hit, miss, and false alarm.[41] There is a small, EEG monitoring lightweight headset available on the open market at the time of this writing that uses Bluetooth to communicate with a computer and does not require   unwieldy attachments to the user’s skin or scalp like most EEG monitors.[42] Another company, building on the technology used to support a brain scanner-driven voice Stephen Hawking tested towards the end of his life, has already added their EEG monitors to an existent HMD and are actively researching how, "…user interfaces can be designed for VR that function as a natural extension of brain activity."[43]

GSR, uses sensors to measure skin conductance levels allowing measurements of cognition, attention, emotion, engagement, anxiety, and stress.[44] This is the technology most commonly used in supporting polygraph machines. There is a small, lightweight GSR kit that uses a variety of connected or wireless methods for communicating with a computer and is available on the open market at time of writing.[45] Since the GSR uses measurements from the finger area closest to the hand, the sensors could potentially be added onto or embedded into the handset(s) used for controlling actions while wearing an HMD. Both of the EEG and GSR products are small, lightweight and unobtrusive enough to incorporate into existing equipment for facilitating this kind of physiological data-gathering.

Furthermore, adding these types of data collection tools permits clearer understanding into the individuals using them. Bailenson indicates that his research lab at Stanford University has collected enough data that, "[t]his work has allowed us to see the behavioral 'tells' that predict mistakes on factory floors, or bad driving behavior, or even when someone is intrigued by a product during online shopping."[46] James Bliss also states that advances in both technology and research provides, "…the ability for researchers to use psychophysiological baseline data to predict individuals' performance in areas such as task functional state, task performance, workload, adaptability, accuracy, and anxiety…" and that this allows them to "…predict future performance…"[47] Another key aspect is that, "Augmented cognition design and evaluation techniques, in comparison, use sensors to capture data on a continual basis, do not *interrupt* an interaction with a VE [Virtual Environment] during task performance, can be captured without conscious awareness, and are objective measures of human cognitive and affective states."[48]

VR and Insider Threat Intersection

Given that these types of measurements can provide insight into a person's state of mind, if properly calibrated and measured together, data-collection from VR decision-making scenarios could lead to an ability to physiologically measure trustworthiness. From the previous definition of trustworthiness, it can be derived that, "…being trustworthy requires recognizing that another party has expectations, and feeling responsible for fulfilling those expectations."[49] VR affords the opportunity to see oneself with an identity as a person inside the immersive experience, which causes people to act as they would in real life even though they are in a simulation or artificial world. Researcher Sandra Calvert indicates that, "[o]verall, people's actions in VEs [Virtual Environments] parallel what they do in *real* environments, in part because they bring an ongoing thread of who they are to all experiences."[50]

Since individuals have difficulty separating their *real* self from their *virtual* self, one approach to measure trustworthiness is to examine an individual's indicators in a virtual experience. Guilt-proneness is observed as, "…individual differences in the extent to which people anticipate feeling guilty about wrong-doing…"[51] In fact, the researchers making the statement regarding guilt-proneness indicate that, "…guilt-proneness is a better predictor of trustworthiness than the Big Five [neuroticism, extraversion, openness, conscientiousness, and agreeableness] personality traits…"[52] Choose-your-own-adventure style immersion experiences could be constructed to incorporate modules that gauge individual guilt-proneness. Since Jackson's prediction methods for insider threat seem to be successful and are based on the NEO

Inventory, incorporating a measurement of guilt-proneness in order to reach a metric for trustworthiness is a logical next step.

A trustworthiness model similar to the structured models for credit scores could be used to group individuals into a tiered scale depicting those most likely to violate trust to those most likely to uphold trust. A range of investigatory tools, options, and training could be applied against each tier to produce the most efficiency for the subject matter expert (SME) tasked with identifying and mitigating potential insider threats. Individual results demonstrating lower levels of trustworthiness could be flagged for a series of follow-up actions. For instance, registers for low levels of trustworthiness could be tiered against insider threat triggers and a range of scrutinization or different re-training opportunities applied to mitigate risk from correctable individual behaviors.

Beyond measuring trustworthiness, if insider threat expert Jackson is right about future behavior prediction, then re-training inside VR might be another avenue for effectively emphasizing consequences. He concluded his thoughts about behavior with the following statement: "[t]he prediction of future behavior is the result of identifying the precursor antecedents that set the stage for the behavior to occur and the consequences of the behavior that determine if behavior will increase or decrease in the future."[53] VR training that includes positive outcomes from correct choices and negative outcomes from incorrect choices can combine an experience the mind treats as real with associated consequences supporting future behavior predictions of desired results. It will be important for training to remain in conformance with existing and new regulations which are derived from the constitutionally-enumerated rights of American citizens.

VR and Background Investigation Intersection

If appropriately associated with calibrated rubrics and tested sufficiently for reliability, trustworthiness could be used for insider threat mitigation and as a tool for clearance processing. By ranking individuals based on their trustworthiness, security professionals could focus their scrutiny on those on the lower end of the spectrum who represent the greatest risk to the enterprise. This would free security professionals from expending significant resources on individuals who do not represent significant security threats and increase focus on those who do. Individual results with higher levels of trustworthiness could also be expedited into the cleared workforce and placed into a pool for future randomized re-checks in a similar fashion as randomized drug screening is currently conducted. This would allow individuals with high levels of trustworthiness to be fully cleared and put to work until a random clearance trustworthiness screening determines otherwise. Moreover, this randomization could facilitate many more frequent checks while being less expensive than current processes. It would also mitigate the Defense Personnel and Security Research Center's concerns about the observation that espionage offenders experienced ineffective external constraints.

VR and SME Training

Another key, relatively quick implementation aspect of VR/AR is that it presents a significant opportunity for SME training improvement. These improvements could be achieved by using VR because it would enable training from anywhere in the world without the need for travel, provide a safe environment for repetition of high-risk learning, and achieve cost and organizational efficiencies without diminishing the quality of training. Bailenson indicates that, "Study after study has shown the experiences that people have in VR have an impact on them. Their behaviors can change, and these changes don't disappear right away."[54] This means that training in a VR environment is equivalent to training in the real world, but the technology can increase the return on investment in both the instruction and practice elements of the learning environment. Admiral Christopher Grady agrees. In his capacity as the Commander of U.S. Fleet Forces Command, he delivered the keynote address to the Interservice/Industry Training, Simulation and Education Conference in November 2018, and said of AR/VR: "…it is training that sticks…."[55]

Using VR for instruction would allow the instructor and students to be located anywhere in the world with the appropriate electricity, internet access, and equipment. The location-independent nature of training facilitates learning with the foremost expert available during the instructional period. Neither the educator nor the student would need to physically travel to conduct the training. The sense of presence generated by human-like avatars in VR space allows students who are geographically separated to feel like they are co-present in the same place. The mind registers the avatars as fellow students or instructors and the ear hears their voices as clearly as any direct telephone or recording system replicates the human voice. The classroom setting can be generated by any multi-user co-presence platform, and there are many such applications on the open market, including one specifically designed for federal IT security controls.[56] There are platforms that offer virtual spaces that are more familiar to the formal learning environment such as a traditional lecture hall, an auditorium, a classroom, or a school where students sit in the chairs while the instructor stands at the lectern or chalkboard. There are also spaces provided by these co-presence platforms that resemble atypical learning settings to include holding class by the lake, outside at the beach, in an outdoor movie area, or in a museum. The meeting space can be as creative as desired and can be created specifically to facilitate the kind of learning necessary to the skill being taught.

Veracity of Training in VR

In addition to the practicalities of remote learning, there is much academic research on learning theories and educational knowledge transference in AR/VR, which is a key understanding in the application to high-risk learning. One of the reasons is that, “[i]t requires interaction and encourages active participation rather than passivity.”[57] Jorge Bacca et al., focused on an AR tool for vocational education and looked at John M. Keller’s ARCS model of motivational learning theory: Attention, Relevance, Confidence, and Satisfaction (ARCS). They found that, “[t]wo of the most relevant advantages of AR applications in education are: increased learning outcomes and increased motivation.”[58] They were concerned that their sample size was too small, but the AR application they developed supported a vocational learning environment that had particular required steps for completing projects. While security professional training is not as technically scaled, it does require certain steps in assembling a picture of someone’s suitability for a security clearance for the adjudicator to render a sound decision.

AR/VR also, “…allows a learner to learn by doing, a constructivist approach.”[59] Learning gained from doing something connects learning with activity. The constructivist learning theory supports learning, “…authentic tasks that contextualize rather than providing abstract instruction…” and allows “…real world, case-based learning environments, rather than predetermined instructional sequences.”[60] Since the VR world is so immersive and the mind treats experiences as real, VR also creates a safe space for experimentation without negative results for high-risk training scenarios. For instance, in the medical community, nurses practicing venipuncture, or intravenous blood sample collection, may cause their human test subjects a great deal of pain whereas, practice in a VR hospital setting on an avatar will facilitate good habit-learning without subjecting a human to painful repetitions. Other training areas such as learning to pilot an aircraft, learning good safety precautions on a construction site, practicing psychological counseling, or good supervisory counseling techniques benefit from limitless numbers of practice attempts which do not cause personal harm to students or test subjects.

Bloom's Taxonomy introduced the concept that learning builds upon itself and facilitates particular focus to, "…consider what the learner can do as a result of the instruction."[61] The background security professional's development mirrors both constructivism and Bloom's Taxonomy very well, and in fact the community generally considers the most skillful investigators as the ones that have the most experience. Those experts can facilitate learning by novices through the concept that, "…application of new knowledge using a MUVE [Multi-User Virtual Environment] platform requires the learner to compare simulated situations to real-life situations and vice versa. Applying the concept in this manner allows the learner to reflect on its veracity and utility."[62] Currently, background investigator experience is obtained through computer and classroom learning, role-playing and practice on live subjects. Training through AR/VR applications has the potential to facilitate experience-acquisition on a more rapid scale. Practicing through AR or VR could allow significantly more practice sessions in a "safe to fail" environment through use of computer-generated subjects or scenarios.

Return on Investment

Moreover, new investigators could practice interview techniques in VR scenarios for as long as necessary to gain the appropriate skills and instincts required to succeed in background investigatory work. Applications built with artificial characters can be programmed to interact with the trainee much like a human role-player. Likewise, the VR character can be tested for as long as the trainee needs the practice and rather than a one-to-one ratio as with live role-players, once created, artificial characters can be replicated as many times as there are trainees that need them. Another way of ensuring positive professional growth for real-world face-to-face interviewing techniques is if new investigators wore AR HMDs for their trial period. SMEs could then monitor more than one investigator at a time while correcting errors, suggesting modifications, and generally prompting the new investigator to mirror effective habits of the SME. AR/VR could also be used by investigators' supervisors to verify work quality against triggers established in the system. Actions or physiological responses that should precipitate investigator behavior or line of questioning changes could be flagged for immediate correction. Alternatively, a randomized process could facilitate unobtrusive quality assurance AR/VR drop-ins by supervisors. Data-gathering could be automated on work completed in AR/VR to ensure that investigators are reaching appropriate metrics accomplishments.

While AR/VR represents yet another tool for security personnel to learn, it also has potential to be a powerful tool that introduces efficiency. A simple VR "kit" costs less than $2,000 at the time of this writing. A kit consists of commercial, off-the-shelf equipment including an HMD, peripherals, and a suitably equipped laptop. This investment is minimal in comparison to the cost for new investigators, SMEs and other support professionals to engage in live training which often necessitates travel outside of home areas. If AR/VR is used to transform background investigator training, then perhaps issuing a kit to each investigator would be a way to reduce training and ongoing professional development costs and simultaneously improve quality. Another consideration for using AR/VR is its potential as a useful tool for promoting cohesion within the security profession itself. Personnel could have round-table events, training refreshers, even conferences with SMEs and guest speakers in VR. The professionals scattered around the world would be able to come together on a regular basis for socialization and professional development without the difficulties and expense of international or far-flung domestic travel.

Another cost-saving measure could be achieved if VR integrated with physiological metrics-gathering becomes the preferred way of conducting initial candidate screenings. The clearance seeker could go through the decision-making scenario to determine their trustworthiness, and those candidates who fell below appropriate trustworthiness indicators could use the kit for follow up meetings with the background investigator. Neither person would be inconvenienced by traffic or multiple trips to meet in person in order to accomplish the requirements. Interviews done this way could reduce the overall amount of time a background investigator spends traveling for interviews, handing off/picking up interview cases completed by personnel located elsewhere, and asking multiple questions about the same thing solely to ascertain interviewee truthfulness.

Challenges of Developing and Implementing VR as a Trustworthiness Tool

VR can provide tools and solutions to the insider threats and the background investigation process problems, however, like any solution VR is not a panacea. VR technologies bring their own limitations and challenges that must be acknowledged and managed. For instance, the potential drawbacks of using an AR/VR tool to reach trustworthiness conclusions may be similar to those surrounding the use of the polygraph tool. There could be a risk of personnel learning how to physiologically beat the tool and trick the system into indicating high trustworthiness. Fortunately, AR/VR HMDs can already track eye and hand movement and may provide a very reliable measure of otherwise imperceptible reactions. This is an area that requires more scientific study, but VR technologies are already demonstrating promise in this area.

Scenario-development is another area that represents a potential challenge. New scenarios would need to be developed on an ongoing basis; it would be a poor test if the same scenario was the only one available every time personnel were subjects for evaluation. However, decision-making scenarios require input from insider threat and security professionals as well as psychologists before a thorough testing period. The cross-domain collaboration required for producing scenarios may reach into very sensitive or classified territory that may make the scenario creation process itself sensitive. The ultimate insider threat would be the individuals developing the decision-making modules and grading schemes for trustworthiness. Notwithstanding, the goal should be for the decision-making scenarios to be accessible through unclassified applications, so that kits can be sent into any environment through any shipping means. Kit portability is important to reducing background investigator travel and development in this area will be required to ensure VR can deliver training at any location and achieve desired cost and organizational efficiencies.

Additional concerns with an AR/VR tool are identity management, system security, and integrity. Clear methods have to be established for credentials to access the system as well as verification that the correct person is the one actually accessing and working through the scenario. Decision-based scenario results must be secure and cannot be replaced or otherwise modified by outside actors. Data-integrity is also vital to system reliability and could affect how the application is developed.

The resource implications for AR/VR tools are substantial, but due to how the technology has evolved, they are lower than many traditional technological solutions. AR/VR application development no longer requires a programming expert and instead can be done by those with the right equipment, training, and time. Development. In fact, high school students in Mississippi have access to cutting edge training in AR/VR development which requires skills similar to movie production: writer, director, videographer, editor, model-maker, sound technician, actor, a code-writer, and production.[63] However, specialists in each area are not required as VR development tools are currently designed to help manage these areas within a small team of developers, most of whom do not need extensive programming experience. Likewise, the same VR kit issued for testing or training can, with the addition of a video camera and sound recording equipment, be used for application development. Although, more intricate applications are typically built on computer systems with greater processing power to enable faster, more efficient production.

A feasibility concern of AR/VR tools is whether there are any restrictions in public law, judicial decisions, presidential orders, or agency regulations preventing the use of this technology in the security arena. Other areas for consideration are related to privacy and long-term storage of results. There are specific DoD requirements and elements necessary to factor into potential decisions regarding gathering new data from potential employees, active employees, and contractors.[64] Additionally, if security professionals use AR/VR for conducting interviews, reviewing personal information, and gathering more information, then the platforms and applications will have to meet IT security requirements for this type of usage as well as any privacy and records management requirements. A review of documentation governing insider threat and background investigation was completed and nothing was found that actively prevents the use of AR/VR tools as described in this paper; however, experts in both fields should be consulted before significant resource investment is made toward piloting development. It will be very important to establish clear requirements governing design, structure, acquisition, and use of such personal information consistent with constitutional rights. Exploring the legal and associated ramifications of using a polygraph-like AR/VR tool more broadly across the government is also an area that requires more consideration.

The last challenge to address in implementing VR tools is one that plagues all new technologies: community adaptation. Security professionals are, understandably, most concerned about security. A new system, especially one that could revolutionize insider threat or background security clearance investigatory methods, may meet with stiff resistance unless the community is involved from the ground-up in development, testing, and deployment. Buy-in is critical to potential adoptability, as the United States Air Force has found with its successful experiment with VR in high-risk pilot training environments. Furthermore, the success of similar experimentation illustrates the potential that test-bed AR/VR programs represent low-cost opportunities to begin resolving significant national security challenges.

Conclusion

AR/VR has great potential as a tool to reduce the insider threat risk and improve security professional efficiency in background investigation security clearance processes. Combining existing professional equipment with HMDs and handsets with eye-tracking and other biometric sensors can generate a powerful tool for measuring physiological responses to immersion scenarios. Combining these technologies in this way could allow the formulation of a risk model that focuses SME efforts on those who do not score as trustworthy as others. Using AR/VR tools to facilitate immersive training reinforcing positive behavior could mitigate insider threat potential and improve security professional effectiveness.

This paper established a common understanding of the insider threat problem, explained the fundamental process of background investigations for security clearances and costs, and reviewed the history of AR/VR including the technology’s professional applications. The paper explored the intersections of AR/VR with insider threat and security clearances and how those, in turn, could produce efficiencies for training within the security profession. After reviewing several recommendations and challenges for implementing the technology in the security profession it is recommended that is be used as a form of polygraph in determining trustworthiness.

While AR/VR technologies are not without challenges, , there are near-term prospects that these issues can be surmounted. Consequently, AR/VR tools represent immediate opportunities to improve training for security professionals and promote cohesion within the profession. Implementing these new opportunities could result in significant efficiencies and return on investment. Most importantly, by leveraging these tools to improve screening and training, there is a potential for dramatic reductions in security clearance backlogs and in the number of days clearances await adjudication. If DoD can embrace AR/VR technologies in these processes, it could deliver proactive solutions to neutralize insider threats, improve national security and potentially save lives.

Notes

[1] See research by: Emily E. Levine, T.B. Bitterly, T.R., Cohen, and M.E Schweitzer, "Who is trustworthy? Predicting trustworthy intentions and behavior," *Journal of Personality and Social Psychology,* 115 no 3 (2018).
[2] Executive Order (EO) 13587, Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.
[3] House, *The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process,* 113 Cong., 1st sess., 2013, https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg87372/html/CHRG-113hhrg87372.htm
[4] Ibid.
[5] Gary M. Jackson, *Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security,* Indianapolis, IN: John Wiley & Sons, Inc., 2012, xxvii.
[6] Ibid, xxx.
[7] Ibid, 5.
[8] National Insider Threat Task Force, *Insider Threat Program Maturity Framework,* November 1, 2018, 3.
[9] Nick Catrantzos, *Managing the Insider Threat: No Dark Corners,* Boca Raton, FL: Taylor & Francis Group, 2012, 3.
[10] Defense Security Service, *Receive and Maintain Your Security Clearance Eligibility,* (Linthicum, MD: Center for Development of Security Excellence, May 2017, https://www.cdse.edu/documents/cdse/Receive_and_Maint_Sct_Clnc.pdf, 4.
[11] Emily E. Levine, T.B. Bitterly, T.R., Cohen, and M.E Schweitzer, "Who is trustworthy? Predicting trustworthy intentions and behavior," *Journal of Personality and Social Psychology,* 115 no 3 (2018), 469.
[12] Andrew Maycock, "Insider Threat and Security Clearance Reform, Cross Agency Priority Goal Quarterly Update FY2016, Quarter 3," *White House Office of Management and Budget*, accessed July 26, 2018, https://fas.org/sgp/othergov/omb/insider-2016-03.pdf.
[13] House, *The Insider Threat to Homeland Security*; Brenda S. Farrell, "Personnel Security Clearances: Opportunities Exist to Improve Quality Throughout the Process," *Testimony Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, U.S. House of Representatives,* November 13, 2013, 1.
[14] Office of the Director of National Intelligence, *Fiscal Year 2017 Annual Report on Security Clearance Determinations,* (Washington, DC: National Counterintelligence and Security Center), https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf, 5.
[15] Government Accountability Office, *GAO Adds Government-wide Personnel Security Clearance Process to "High Risk List"*, January 25, 2018, https://www.gao.gov/about/press-center/press-releases/read/high_risk_security_clearance_process.htm.
[16] Government Accountability Office, *High Risk List*, accessed February 9, 2019, https://www.gao.gov/highrisk/overview.
[17] House, *The Insider Threat to Homeland Security*; Brenda S. Farrell, "Personnel Security Clearances: Opportunities Exist to Improve Quality Throughout the Process," 4.

[18] Andrew Maycock, "Insider Threat and Security Clearance Reform.

[19] Ibid.

[20] House, *The Insider Threat to Homeland Security*; Gregory Marshall, "Written Testimony of Gregory Marshall," *Testimony Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, U.S. House of Representatives*, November 13, 2013, 5.

[21] Gary M. Jackson, *Predicting Malicious Behavior*, 206.

[22] Ibid, 244.

[23] Ibid, 244.

[24] Katherine L. Herbig, *Changes in Espionage by Americans: 1947-2007*, Technical Report 08-05, Monterey, CA: Defense Personnel Security Research Center, March 2008, 14.

[25] Ibid, 5.

[26] Defense Human Resource Activity, "Initiatives," PERSEREC website accessed December 4, 2018, http://www.dhra.mil/PERSEREC/Initiatives/.

[27] D.W.F. van Krevelen, Augmented Reality: Technologies, Applications, and Limitations, Department of Computer Science Technical Report, Amsterdam, The Netherlands: University of Amsterdam, 2007, 2.

[28] Author, Search for "Augmented" on November 23, 2018, returned individual applications entitled: Measure, Color Snap Visualize, Ikea Place, Night Sky, Bookful, Living Wine Labels, and Golf Shot.

[29] George Lambrakopoulos, Nikolaos Begetis, Akrivi Katifori, Manos Karvounis, and Yannis Ioannidis, "Experimental Evaluation of the Impact of Virtual Reality on the Sentiment of Fear," *Institute of Electrical and Electronics Engineers, 2017 23rd International Conference on Virtual System & Multimedia (VSMM)* (October 2017), 4.

[30] Peter Rubin, *Future Presence: How Virtual Reality Is Changing Human Connection, Intimacy, and the Limits of Ordinary Life,* New York, NY: HarperOne, April 2018, 31.

[31] Jeremy Bailenson, *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do,* New York, NY: W.W. Norton & Company, January 2018, 46.

[32] Gary M. Jackson, *Predicting Malicious Behavior*, 279-280.

[33] Ibid, 280.

[34] Ibid, 280.

[35] Will Greenwald, "The Best VR (Virtual Reality) Headsets of 2018," PCMagazine, November 18, 2018, https://www.pcmag.com/article/342537/the-best-virtual-reality-vr-headsets.

[36] Xuezhong Wang and Brent Winslow, "Eye Tracking in Virtual Environments," In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.,* edited by Kelly S. Hale and Kay M. Stanney, 197-206. Boca Raton: CRC Press, 2014, 201.

[37] Ibid, 202.

[38] Jeremy Bailenson, *Experience on Demand*, 240.

[39] Xuezhong Wang and Brent Winslow, "Eye Tracking in Virtual Environments," 202.

[40]James P. Bliss, Alexandra B. Proaps, and Eric T. Chancey, "Human Performance Measurement in Virtual Environments," In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.*, edited by Kelly S. Hale and Kay M. Stanney, 750-774. Boca Raton: CRC Press, 2014, 748.

[41] Kelly S. Hale, Kay M. Stanney, Dylan Schmorrow, and Lee W. Sciarini, "Augmented Cognition for Virtual Environment Evaluation," In *Handbook of Virtual Environments: Design,*

Implementation, and Applications, 2nd Ed., edited by Kelly S. Hale and Kay M. Stanney, 873-8. Boca Raton: CRC Press, 2014, 877.

[42] "EMOTIV INSIGHT 5-channel mobile EEG," Emotive, accessed December 8, 2018, https://www.emotiv.com/product/emotiv-insight-5-channel-mobile-eeg/.

[43] "Brain-Computer Interface," Nureable, accessed December 9, 2018, http://neurable.com/about/science/neurable; Peter Murray, "Brain Scanner Being Used To Give Stephen Hawking A New Voice," Singularity Hub, accessed January 9, 2019, https://singularityhub.com/2012/04/06/brain-scanner-being-used-to-give-stephen-hawking-a-new-voice/#sm.00016thr5ziq9e2ptl91sz1ip7fhm.

[44] Kelly S. Hale, Kay M. Stanney, Dylan Schmorrow, and Lee W. Sciarini, "Augmented Cognition for Virtual Environment Evaluation," 877.

[45] "GSR logger sensor NUL-217," NeuLog, accessed December 9, 2018, https://neulog.com/gsr/.

[46] Jeremy Bailenson, *Experience on Demand*, 240.

[47] James P. Bliss, Alexandra B. Proaps, and Eric T. Chancey, "Human Performance Measurement in Virtual Environments," 759-760.

[48] Kelly S. Hale, Kay M. Stanney, Dylan Schmorrow, and Lee W. Sciarini, "Augmented Cognition for Virtual Environment Evaluation," 876.

[49] Emily E. Levine, T.B. Bitterly, T.R., Cohen, and M.E Schweitzer, "Who is trustworthy? Predicting trustworthy intentions and behavior," 469.

[50] Sandra L. Calvert, "Social Impact of Virtual Environments," In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.*, edited by Kelly S. Hale and Kay M. Stanney, 699-715. Boca Raton: CRC Press, 2014, 715.

[51] Emily E. Levine, T.B. Bitterly, T.R., Cohen, and M.E Schweitzer, "Who is trustworthy? Predicting trustworthy intentions and behavior," 488.

[52] Ibid, 488.

[53] Gary M. Jackson, *Predicting Malicious Behavior*, 494.

[54] Jeremy Bailenson, *Experience on Demand*, 46.

[55] Admiral Christopher Grady, Commander of U.S. Fleet Forces Command, Keynote Address, Interservice/Industry Training, Simulation and Education Conference, Orlando, FL, 27 November 2018, https://www.youtube.com/watch?v=TODAb51dPQQ.

[56] Mat Chacon, "US Federal Workforce," *Doghead Simulations*, PowerPoint presentation emailed to author, December 18, 2018, 6.

[57] Veronica S. Pantelidis, "Reasons to Use Virtual Reality in Education and Training Courses and a Model to Determine When to Use Virtual Reality," In *Themes in Science and Technology Education*, 2. 59-70, Klidarithmos Computer Books: Athens, Greece, January 2009, 63.

[58] Jorge Bacca, Silvia Baldiris, Ramon Fabregat and Kinshuk, "Insights Into the Factors Influencing Student Motivation in Augmented Reality Learning Experiences in Vocational Education and Training," *Frontiers in Psychology*, no. 9 (August 2018), 1.

[59] Veronica S. Pantelidis, "Reasons to Use Virtual Reality in Education and Training Courses and a Model to Determine When to Use Virtual Reality," 64.

[60] Phillipe Bertrand, Jérôme Guegan, Léonore Robieux, Cade Andrew McCall, and Franck Zenasni, "Learning Empathy Through Virtual Reality: Multiple Strategies for Training Empathy-Related Abilities Using Body Ownership Illusions in Embodied Virtual Reality," *Journal of Robotics and AI* 5, no. 26 (March 2018), 5.

[61] Nancy E. Adams, “Bloom’s taxonomy of cognitive learning objectives,” *Journal of the Medical Library Association, 103*, no. 3 (July 2015), 153.
[62] Burgess, Melissa L. and Phil Ice, “Using the Community of Inquiry (COI) Model and Bloom’s Revised Taxonomy to Support 21st Century Teaching and Learning in Multi-User Virtual Environments,” In *Transforming Virtual World Learning: Cutting-Edge Technologies in Higher Education, Volume 4*, by Randy Hinrichs and Charles Wankel, 167-186. Emerald Group Publishing Limited: Bingley United Kingdom, 2011, 176.
[63] “VR Academy,” *Lobaki*, accessed April 13, 2019, https://www.lobaki.com/vr-academy.
[64] Department of Defense, *Department of Defense Privacy Program: DoD 5400.11-R*. Washington, DC: Office of the Assistant Secretary of Defense (Director, Administration and Management), May 14, 2007.

Bibliography

Adams, Nancy E. “Bloom’s taxonomy of cognitive learning objectives.” *Journal of the Medical Library Association, 103,* no. 3 (July 2015): 152–153.

Bacca, Jorge, Silvia Baldiris, Ramon Fabregat and Kinshuk. “Insights Into the Factors Influencing Student Motivation in Augmented Reality Learning Experiences in Vocational Education and Training.” *Frontiers in Psychology*, no. 9 (August 2018): 1-13. DOI: http://dx.doi.org.pentagonlibrary.idm.oclc.org/10.3389/fpsyg.2018.01486.

Bailenson, Jeremy. *Experience on Demand: What Virtual Reality Is, How It Works, and What It Can Do.* New York, NY: W.W. Norton & Company, January 2018.

Bertrand, Phillipe, Jérôme Guegan, Léonore Robieux, Cade Andrew McCall, and Franck Zenasni. “Learning Empathy Through Virtual Reality: Multiple Strategies for Training Empathy-Related Abilities Using Body Ownership Illusions in Embodied Virtual Reality.” *Journal of Robotics and AI* 5, no. 26 (March 2018): 1-18. https://doi.org/10.3389/frobt.2018.00026.

Bliss, James P., Alexandra B. Proaps, and Eric T. Chancey. “Human Performance Measurement in Virtual Environments.” In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.*, edited by Kelly S. Hale and Kay M. Stanney, 750-774. Boca Raton: CRC Press, 2014.

“Brain-Computer Interface.” Nureable. Accessed December 9, 2018, http://neurable.com/about/science/neurable.

Burgess, Melissa L. and Phil Ice. “Using the Community of Inquiry (COI) Model and Bloom’s Revised Taxonomy to Support 21st Century Teaching and Learning in Multi-User Virtual Environments.” In *Transforming Virtual World Learning: Cutting-Edge Technologies in Higher Education, Volume 4,* by Randy Hinrichs and Charles Wankel, 167-186. Emerald Group Publishing Limited: Bingley United Kingdom, 2011.

Calvert, Sandra L. “Social Impact of Virtual Environments.” In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.*, edited by Kelly S. Hale and Kay M. Stanney, 699-715. Boca Raton: CRC Press, 2014.

Catrantzos, Nick. *Managing the Insider Threat: No Dark Corners*. Boca Raton, FL: Taylor & Francis Group, 2012.

Chacon, Mat. “US Federal Workforce.” *Doghead Simulations*. PowerPoint presentation emailed to author. December 18, 2018.

Defense Security Service. *Receive and Maintain Your Security Clearance Eligibility*. Linthicum, MD: Center for Development of Security Excellence. May 2017. https://www.cdse.edu/documents/cdse/Receive_and_Maint_Sct_Clnc.pdf, 4.

Department of Defense. *Department of Defense Privacy Program: DoD 5400.11-R*. Washington, DC: Office of the Assistant Secretary of Defense (Director, Administration and Management), May 14, 2007.

"EMOTIV INSIGHT 5-channel mobile EEG." Emotive. Accessed December 8, 2018. https://www.emotiv.com/product/emotiv-insight-5-channel-mobile-eeg/.

Executive Order 13587. Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. October 7, 2011.

Government Accountability Office. *GAO Adds Government-wide Personnel Security Clearance Process to "High Risk List"*. January 25, 2018. https://www.gao.gov/about/press-center/press-releases/read/high_risk_security_clearance_process.htm.

Government Accountability Office. *High Risk List.* Accessed February 9, 2019. https://www.gao.gov/highrisk/overview.

Grady, Admiral Christopher, Commander of U.S. Fleet Forces Command. Keynote Address. Interservice/Industry Training, Simulation and Education Conference, Orlando, FL, 27 November 2018. https://www.youtube.com/watch?v=TODAb51dPQQ.

Greenwald, Will. "The Best VR (Virtual Reality) Headsets of 2018." PCMagazine. November 18, 2018. https://www.pcmag.com/article/342537/the-best-virtual-reality-vr-headsets.

"GSR logger sensor NUL-217." NeuLog. Accessed December 9, 2018, https://neulog.com/gsr/.

Hale, Kelly S., Kay M. Stanney, Dylan Schmorrow, and Lee W. Sciarini. "Augmented Cognition for Virtual Environment Evaluation." In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.*, edited by Kelly S. Hale and Kay M. Stanney, 873-8. Boca Raton: CRC Press, 2014.

Herbig, K. L. *Changes in Espionage by Americans: 1947-2007.* Technical Report 08-05, Monterey, CA: Defense Personnel Security Research Center, March 2008.

House. *The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process*. 113 Cong., 1st sess., 2013. https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg87372/html/CHRG-113hhrg87372.htm.

Jackson, Gary M. *Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security.* Indianapolis, IN: John Wiley & Sons, Inc., 2012.

Jan, Shazia K., and Panos Vlachopoulos. "Influence of Learning Design of the Formation of Online Communities of Learning." *International Review of Research in Open and Distributed Learning* 19, no. 4 (September 2018): 1-16.

Lambrakopoulos, George, Nikolaos Begetis, Akrivi Katifori, Manos Karvounis, and Yannis Ioannidis. "Experimental Evaluation of the Impact of Virtual Reality on the Sentiment of Fear." *Institute of Electrical and Electronics Engineers, 2017 23rd International*

Conference on Virtual System & Multimedia (VSMM) (October 2017). 10.1109/VSMM.2017.8346251.

Levine, Emily E., Bitterly, T.B., Cohen T.R., and Schweitzer, M.E. "Who is trustworthy? Predicting trustworthy intentions and behavior." *Journal of Personality and Social Psychology. 115 no* 3 (2018), 468-494.

Murray, Peter. "Brain Scanner Being Used To Give Stephen Hawking A New Voice." Singularity Hub. Accessed January 9, 2019, https://singularityhub.com/2012/04/06/brain-scanner-being-used-to-give-stephen-hawking-a-new-voice/#sm.00016thr5ziq9e2ptl91sz1ip7fhm

National Insider Threat Task Force. *Insider Threat Program Maturity Framework.* November 1, 2018.

Office of the Director of National Intelligence. *Fiscal Year 2017 Annual Report on Security Clearance Determinations.* (Washington, DC: National Counterintelligence and Security Center). https://www.dni.gov/files/NCSC/documents/features/20180827-security-clearance-determinations.pdf.

Pantelidis, Veronica S. "Reasons to Use Virtual Reality in Education and Training Courses and a Model to Determine When to Use Virtual Reality." In *Themes in Science and Technology Education,* 2. 59-70. Klidarithmos Computer Books: Athens, Greece. January 2009.

Parson, Vanessa and Simon Bignell. "Using Problem-Based Learning within 3D Virtual Worlds." In *Transforming Virtual World Learning: Cutting-Edge Technologies in Higher Education, Volume 4,* by Randy Hinrichs and Charles Wankel, 241-261. Emerald Group Publishing Limited: Bingley United Kingdom, 2011.

Rubin, Peter. *Future Presence: How Virtual Reality Is Changing Human Connection, Intimacy, and the Limits of Ordinary Life.* (New York, NY: HarperOne, April 2018).

Slater, Mel, Xavi Navarro, Jose Valenzuela, Ramon Oliva, Alejandro Beacco, Jacob Thorn and Zillah Watson. "Virtually Being Lenin Enhances Presence and Engagement in a Scene From the Russian Revolution." *Frontiers in Robotics and AI* 5, no. 91 (August 2018): 1-15. https://doi.org/10.3389/frobt.2018.00091.

Srivastava, Shirish C., and Shalini Chandra. "Social Presence in Virtual World Collaboration: An Uncertainty Reduction Perspective Using a Mixed Methods Approach." *MIS Quarterly* 42, no. 3 (September 2018): 779-803.

Tcha-Tokey, Katy, Olivier Christmann, Emilie Loup-Escande, Guillaume Loup, and Simon Richir. "Towards a Model of User Experience in Immersive Virtual Environments." *Advances in Human-Computer Interaction,* (September 2018): 1-10. https://doi.org/10.1155/2018/7827286.

van Krevelen, D.W.F. *Augmented Reality: Technologies, Applications, and Limitations. Department of Computer Science Technical Report*. Amsterdam, The Netherlands: University of Amsterdam, 2007.

van Loon, Austin, Jeremy Bailenson, Jamil Zaki, Joshua Bostick, and Robb Willer. "Virtual reality perspective-taking increases cognitive empathy for specific others." *PLOS One*, (August 2018): 1-19. https://doi.org/10.1371/journal.pone.0202442.

Wang, Xuezhong and Brent Winslow. "Eye Tracking in Virtual Environments." In *Handbook of Virtual Environments: Design, Implementation, and Applications, 2nd Ed.*, edited by Kelly S. Hale and Kay M. Stanney, 197-206. Boca Raton: CRC Press, 2014.

White House. Office of the Press Secretary. *Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks*, October 7, 2011. https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/fact-sheet-safeguarding-us-governments-classified-information-and-networ.