SYM-AM-21-083

EXCERPT FROM THE PROCEEDINGS OF THE EIGHTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

Technology Trust: The Impact of Trust Metrics on the Adoption of Autonomous Systems Used in High-Risk Applications

May 11–13, 2021

Published: May 10, 2021

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

Technology Trust: The Impact of Trust Metrics on the Adoption of Autonomous Systems Used in High-Risk Applications

Michael Anderson is a PhD Candidate at the Naval Postgraduate School Information Sciences Department. His research interests include Technology Trust. Mr. Anderson has an extensive background in the design of wireless communication systems and the use and deployment of military technologies. His past experience includes over 10 years of work as adjunct faculty teaching university students and professional engineers and scientists in the areas of digital design and computer architecture. Mr. Anderson holds a BS and MS in Electrical Engineering from the University of Michigan, Ann Arbor. [-mail address: mganders@nps.edu]

Dr. Johnathan Mun and is a specialist in advanced decision analytics, quantitative risk modeling, strategic flexibility real options, predictive modeling, and portfolio optimization. He has authored 24 books; holds 22 patents and patents pending; created over a dozen software applications in advanced decision analytics; and has written over a hundred technical notes, journal articles, and white papers. He is currently the CEO of Real Options Valuation, Inc., and his prior positions include vice president of Analytics at Oracle/Crystal Ball and a senior manager at KPMG Consulting. Dr. Mun holds a PhD in Finance and Economics from Lehigh University, an MBA and MS from Southeastern University, and a BS in Physics and Biology from the University of Miami. [E-mail address: jcmun@nps.edu]

Abstract

As autonomous systems become more capable, end users must make decisions about how and when to deploy such technology. The use and adoption of a technology to replace a human actor depends on its ability to perform a desired task and on the user's experience-based trust that it will do so. The development of experience-based trust in autonomous systems is expensive and high risk. This work focuses on identifying a methodology for technology discovery that reduces the need for experience-based trust and contributes to increased adoption of autonomous systems. Initial research reveals two problems associated with the adoption of high-risk technologies; 1) end user's refusal to accept new systems without high levels of initial trust and 2) lost or uncollected experience-based trust data. The main research hypothesis is that a trust score, or trust metric, can influence the initial formation of trust by functioning as a surrogate for experience-based trust, and that trust in technology can be measured through a probability-based prediction of risk.

Introduction

We had better be quite sure that the purpose put into the machine

is the purpose which we desire.

- Norbert Wiener, Some moral and

technical consequences of automation

The use of technology by the Department of Defense (DoD) depends on its ability to perform a desired task. There are many issues associated with trust in technology that are increasing in importance as the U.S. military begins to acquire and deploy autonomous systems. In order to ensure the effective adoption of new innovations in technology, there is a need to establish a system of metrics that justify a level of technology trust. This proposed research has the explicit goal of investigating and recommending trust metrics by applying advanced analytical methodologies to increase the speed and effectiveness of the adoption of new technologies. This investigation proceeds by participating in an evaluation of technologies for use in evolving high-risk military applications. The trust metrics are measured in terms of the technology acceptance versus system control.

Technology Trust

Devitt (2018) implies that in order to meet the DoD requirements for increased speed of adoption for new technologies, there is a need to replace the model of developing trust over longer periods of time with a justifiable metric of trust. This research studies the effectiveness of establishing and introducing trust metrics on the evaluation and selection of technologies. The work participates in an ongoing assessment of autonomous systems for use in high-risk military applications throughout fiscal year 2019. A model is developed that optimizes the cognitive impacts of these trust metrics as they relate to the technology selection and adoption process. The approach will be extensible and can be adopted into private industry.

Research Problem

The recent increase in the use and deployment of commercial technologies by other countries is a disruptive threat to the United States' technological superiority. The rapidly changing technology landscape requires DoD laboratories to increase the speed at which they adopt new technologies (David & Nielsen, 2016). With declining budgets in research, it is imperative that the DoD establish new methods for rapidly adopting and effectively deploying new and emerging technologies whenever possible.

Research Purpose

As autonomous systems begin to surpass the capabilities of humans, there is a need to establish a level of confidence in a technology's ability to perform as expected. The complexity of modern systems makes it difficult to establish a comprehensive metric of trust. Past research in technology trust focused on automation and methods to measure interpersonal person-to-firm relations, such as trust in a Web vendor or a virtual team member (McKnight et al., 2011). This research has the goal of establishing and measuring a comprehensive trust metric for individual pieces of technologies, such as autonomous systems, used in high-risk military applications. The development of a trust metric serves two purposes: first, as a surrogate for experience-based trust by contributing to the formation of initial trust and, second, as a collection tool for capturing experience-based trust data.

Research into a "trust-discovery" methodology contributes to improved understanding of human-machine trust formation and the development of a technology-literate workforce capable of accurately assessing new technology for a given operational scenario. This work first establishes a baseline definition of what it means to "trust" technology. It concludes with the development of a methodology leading to trusting relations between humans and technology. This work contributes to the literature in areas of trust in autonomous systems, technology adoption, and technologies intended for use in high-risk applications where failure or improper application can lead to severe consequences.

Research Questions

This study attempts to answer the following questions:

1. How do varying levels of system control affect the development of trust in technologies used in high-risk military applications? The constructs researched include:
    a. Perceived ease of use
    b. Perceived usefulness
    c. Intent to use
2. How do anthropomorphic metrics affect the development of trust in technologies used in high-risk military applications? The constructs researched include:
    a. Hardware
    b. Algorithms
    c. Links

Research Approach

The following research approach is used:

1. Study the evaluation process of autonomous systems for use in high-risk military applications.
2. Develop a conceptual framework for trust metrics that optimizes the technology evaluation process.
3. Observe and record the results of both laboratory and field experimentation.

The basic tenets of the experimental design are realized through a 2 x 3 factorial design (Table 1-1).

Table 1-1. 2 x 3 Factorial Design

			SYSTEM CONTROL		
			LOW	MID	HIGH
TRUST METRIC		NOT USED	…	…	…
		USED	…	…	…

Contribution

The concept of a technology trust metric has applicability beyond the DoD. Private industry can greatly benefit from the concepts and methodologies developed in this research by applying trust metrics to the research and development of existing or new consumer technologies such as machine learning (ML), artificial intelligence (AI) systems, smart algorithms, and embedded technologies. These intelligent systems are transformative areas that will eventually integrate into all industries (e.g., self-driving cars, delivery drones, big data analytics, and the Internet of Things, where algorithms, machines, and computer systems are continually learning and evolving).

This research also contributes to trust theory and provides an increased understanding of military technology acceptance. The recommendations provide a conceptual framework for how a military community develops trust in technologies for high-risk missions and how varying factors influence the development of such a relationship. Currently, there is an effort to perform such trust analytics within the DoD in which this current research will participate.

Organization

Section 2: Literature Review

This review investigates existing literature that includes terms such as *technology trust and risk, decision making,* and *technology-adoption models*. A review of current and past theory on technology trust and decision making is developed, which is then used to develop a comprehensive metric for assessing technology trust within the DoD. A proposed framework for a comprehensive trust metric is identified and introduced to the technology evaluation process.

Section 3: Experimental Design

Both lab and field experiments are conducted to identify trust metrics. This research intends to leverage an ongoing DoD experiment reviewing and selecting a series of new autonomous systems. The existing data is collected from DoD active-duty technology end users,

as well as civilian scientist support staff. The study investigates how varying levels of trust influence cognitive decision making as well as technology adoption. The primary product of this investigation is the experimental data obtained.

Literature Review

The purpose of this section is to understand the formation of trust, as well as analyze the constructs of a trust relationship. The idea of trust metrics is broken down into quantifiable segments based on leading theories. We conclude by presenting a conceptual framework for a technology trust metric based on what was learned from the literature, as well as what is missing from the literature.

This research was initiated through informal interviews that attempted to identify the factors that contribute to the use of technology in high-risk environments. The participants were a small group of active-duty military and veterans that deploy, or have deployed, with technology that posed great risk of physical harm should it fail. A number in this group experienced significant injury due to the failure of technology, and the potential for bias was noted. The open-ended questions were based on what the users did or did not like about using technology in high-risk scenarios. The initial coding of interviews revealed the following themes:

1. Hands-on experience with technology is critical for establishing trust, and team-based reputation for a technology is as important as personal experience.
2. Users favor simple technology containing only the features needed to accomplish a mission, and users reject new technology in favor of older and more trusted systems.
3. Personal investment in a mission is key to learning how to use new technology.

These themes all have implications for the adoption of autonomous systems within the DoD. Advanced robotic systems have the ability to improve performance in a number of military roles while reducing risk to humans, and it is important to understand how to improve the adoption of such systems within the DoD. This initial research focused on technology in dangerous environments and reveals that adoption is highly dependent on the ability of the user to obtain the knowledge necessary to develop trust. This theme led to our initial literature review on understanding trust, and how it applies to technology adoption.

The literature review was developed through searches on both Web of Science and Google Scholar using combinations of search terms such as *trust, knowledge-trust, technology trust, human-computer, human-robot, technology acceptance, trust attribute, trust risk,* and *risk score*. The literature results were narrowed to 93 relevant articles.

Knowledge

The process of obtaining knowledge is fundamental to the establishment of trust. We therefore briefly review the epistemologies, or the processes for how a person gets to know something, as concepts important to this work. Early philosophers presented the two opposing views of the source of knowledge: rationalism or empiricism.

The French Philosopher Rene Descartes was an early rationalist who believed that we can only know something through reason, and that the only thing we can truly know is that we have consciousness. Descartes presented a methodology for knowing what is real that rejects a construct needed for the establishment of technology trust. He established a dualism that reduces our understanding to distinct areas of consciousness and matter but does not account for the senses. Our sense perception, he believed, is easily prone to error due to subjective interpretation. He believed that the senses are meant to simply get us around in the world rather than lead us to truth. In order to test our hypothesis of trust in technology we must identify

constructs that permit measurement of human interaction with technology, and technology interaction with its surroundings.

John Locke later introduced empiricism that, contrary to rationalism, stated that all knowledge must be obtained through experience. The empiricists claimed that the senses were the only way to true knowledge, and that experience is much more accurate than anything the mind could ever reproduce through memory or reason. The theories presented by rationalism and empiricism both stand to contribute to the formation of trust through the application of reason-based knowledge and experience-based knowledge. (However, there is a limitation in that we lack a method for integrating these two forms of obtaining knowledge.)

Further review reveals that modern philosophers reject the idea that knowledge is obtained exclusively through either rationalism or empiricism. The philosopher Immanuel Kant provided a synthesis between the two opposing theories. First, he noted that reason lacks the ability to create sensory experience; it is only through reason that we are able to accurately analyze the stimuli received through the senses. This theory represents a foundation for understanding the development of trust. The Figure 2-1 represents a causal model based on our finding in the literature that includes a synthesizing feedback loop to represent how we come to know something.

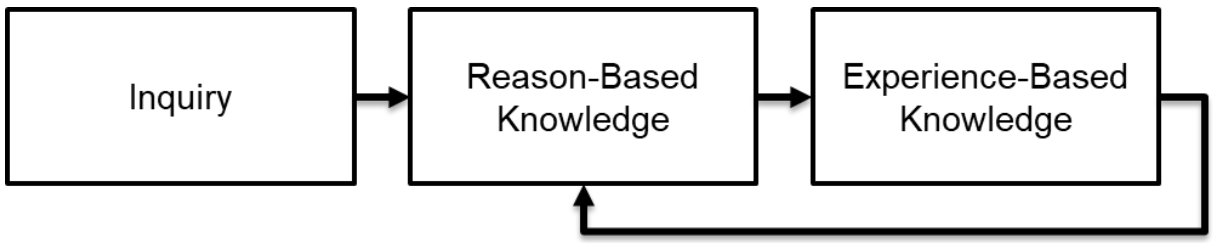

Figure 2-1. A Model of Inquiry Leading to Knowledge

Trust

Castelfranchi and Falcone (2010) review over 72 definitions of what it means to know something well enough to have trust, and their work reveals a great deal of confusion and ambiguity surrounding the use of the term. The concept of trust appears to be subjective in nature, and the literature does not provide a commonly accepted definition across research disciplines. Agreement in the literature was found for the definition of trust in two small areas: 1) the basic premise of trust involves two actors, and 2) trust is a relationship in which one entity relies on someone, or something, based on a given criterion. Research into the meaning of a "given criterion" reveals an interchangeable use of the terms *trust* and *confidence*. The only noticeable difference in the use of these terms is that trust is based on decisions involving risk, whereas confidence involves decisions devoid of consequence.

This literature review furthers its investigation into trust through researching interpersonal relationships. Leading theories on interpersonal trust present vulnerability and risk as the contributing factors unique to the development of such a relationship. Cho et al. (2015) surveyed the meaning of trust across academic disciplines and identified that it follows a basic premise involving risk. For example, they found that academic researchers of trust in psychology assess the probability that individual behaviors are repeatable in situations that entail risk, and in sociology researchers of trust assess the probability that one party will perform an action that will not hurt the interests of a dependent party or expose them to risk due to ignorance or uncertainty.

Rousseau et al. (1998) define interpersonal trust as a psychological state of a trustor accepting vulnerability in a situation involving risk, based on positive expectations of the intentions

or behavior of the trustee. Boon et al. (1991) simplify the definition of trust as a state involving confident predictions about another's motives in situations entailing risk. The majority of early research on trust involves person-person relationships and provides a starting point for our understanding of the process of developing trust. Figure 2-2 presents an operational model of interpersonal trust formation based on the reviewed literature.

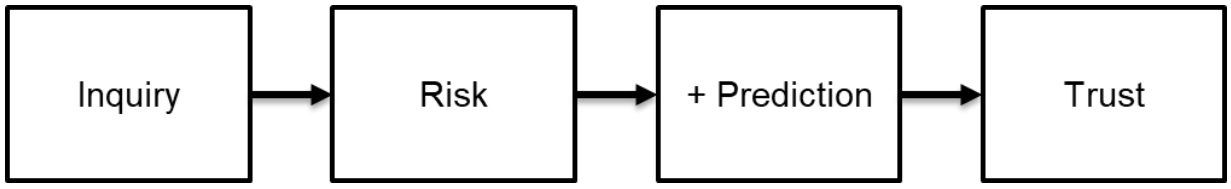

Figure 2-2. A Model of Interpersonal Trust Formation

Adams and Webb (2002) describe two broad processes of developing trust between two individuals. The first is defined as "person-based trust", which develops through repeated engagements, and the second is called "category-based trust", which develops in the absence of direct experience. These definitions parallel the theories identified in our previous research into the epistemologies. Consequently, we modify interpersonal trust terminology to match our research by replacing "category-based" with "reason-based", and "person-based" with "experience-based".

Kramer and Tyler (1996) assess reason-based trust and presents it as useful for understanding how one develops a trusting relationship when personal or social interaction is not possible. This type of trust often develops through someone's membership in a familiar group or category. The factors contributing to reason-based trust can be social roles, training, or experience. In reason-based trust, the relationship is most commonly developed through a reputation that serves as a proxy for personalized knowledge and direct experience. These concepts lead to our first research hypothesis regarding the experience-based trust relationships.

H1: An experience-based proxy will influence the tendency to trust or distrust.

Rempel, Holmes, and Zanna (1985) assess that experience-based trust relationships develop over a long period of time through personal interaction. In their early research on trust they describe three factors that influence the development of trust as competence, benevolence, and integrity. They also discuss the significance of the mental motivation behind the desires to establish a relationship and found it was strongly correlated to the factors that influence trust. Their work confirms a theme identified in our early interviews with users of technology in risk-application that emphasized the importance of personal investment. It also leads to our second hypothesis relating motivation to technology acceptance.

H2: Increased personal motivation will increase technology acceptance.

There appears general agreement in the literature reviewed that interpersonal trust consists of two categories: first, that trust is both reason-based and experience-based and, second, the strength of the trust bonds may differ. The concept of initial trust involves the development of a relationship based purely on reason and represents a weaker connection that can be explained by first impressions. The second category of experience-based trust involves direct knowledge and regular interaction. This type of trust represents a stronger connection and is explained by relationships that develop over a longer period of time through an experience-reason feedback loop. Figure 2-3 presents a model of interpersonal trust.

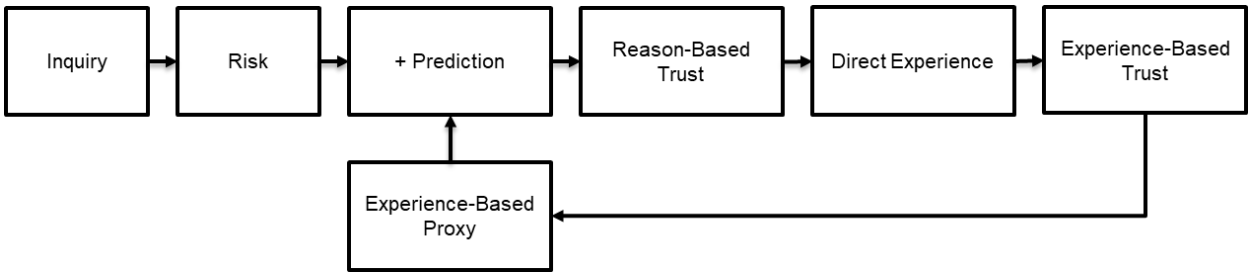

Figure 2-3. Interpersonal Trust Life Cycle

Technology

The past research on interpersonal trust applies in many ways to trust in technology. This study sought out literature that contributes to the development of a methodology of technology discovery leading to person-technology trust. The potential for integrating interpersonal trust research into technology trust was discussed by McKnight (et al., 2011). This research found that interpersonal trust is based on a trustee's expectations and reliance on a trustor to perform as expected through benevolence, even though the trustor possesses the volition to choose to do what is right or what is wrong. Since technology does not possess volition (ability to choose), some researchers went as far as to dismiss the idea of trust in technology as irrelevant. However, recent advances in artificial intelligence refute the claims that technology lacks volition. This is confirmed in the vast amount of current research into how autonomous systems make decisions that can either harm or protect human life.

Technology trust research is further represented in multiple disciplines of engineering and science. The major fields of technology trust research include, but are not limited to, artificial intelligence, command and control, human-computer interaction (HCI), data fusion, human-machine fusion, cyber security, and automation. Multiple models for researching trust are presented in the literature that combine both humanlike and systemlike terminology. Technology trust is a multifaceted area of research that integrates both humanlike measures and systemlike measures. Three of the most frequently used humanlike terms used to model technology are *competence, benevolence,* and *integrity*. The work by McKnight et al. (2011) and Lankton et al. (2015) consider the systemlike alternate terms for technology trust as *reliability, functionality,* and *helpfulness*. A number of systemlike measures of technology trust were identified that are outside the scope of this work but still important to ongoing trust research. These potential systemlike measures include supply chain management, past vendor performance, hardware/software-oriented security, and network security.

The majority of the language used to describe interpersonal trust can apply to technology trust. For example, the word *benevolence* is a very humanlike attribute that is likely to appear in future literature on the decision-making capabilities of self-driving cars. A total of 86 factors and attributes related to interpersonal and technology trust were collected from the literature to form a random nomological network of trust terms. A *factor* is described as situational consideration of technology use that has the potential to influence trust, such as risk and time to operate. An *attribute* is a characteristic inherent to the technology such as its speed, power, and processing capability. The combined and unsorted list is presented in Table 2-1. Future experimentation involves understanding the influence of these terms in the following areas:

1. Factors that measure reason-based and experience-based technology trust
2. Attributes that characterize technology trust as a proxy for experience

Table 2-1. Nomological Network of Trust Factors and Attributes (*Sources:* Cho et al., 2015; DeVitt, 2018; Hoff and Bashir, 2015; McKnight et al., 2011; Schaefer, 2016)

Ability	Character	Disappointment	Importance	Process	Skills
Adaptive	Communication	Disposition	Incompetent	Protect	Stability
Adoption	Competence	Dynamic	Integrity	Purpose	Supportive
Adversarial	Completeness	Easy	Intelligibility	Rationality	Teammate
Altruism	Confidence	Expectation	Intent	Recency	Trainable
Attractive	Contract	Experience	Knowledge	Reciprocation	Transparency
Autonomous	Control	Faith	Learning	Regret	Uncertain
Availability	Cooperation	Faults	Likeable	Relational	Understandability
Awareness	Credibility	Fear	Monitored	Relevance	Unstructured
Belief	Credit	Feeling	Motives	Reliability	Utility
Benevolence	Decisive	Frequency	Perception	Relief	Validity
Capability	Delegation	Frustration	Performance	Responsive	
Capital	Dependability	Helpfulness	Popular	Risk	
Centrality	Difficult	Honesty	Power	Robust	
Certainty	Directability	Hope	Predictability	Similarity	

Figure 2-4 represents the integration of technology trust with the interpersonal trust factors and attributes included in our nomological network of terms.

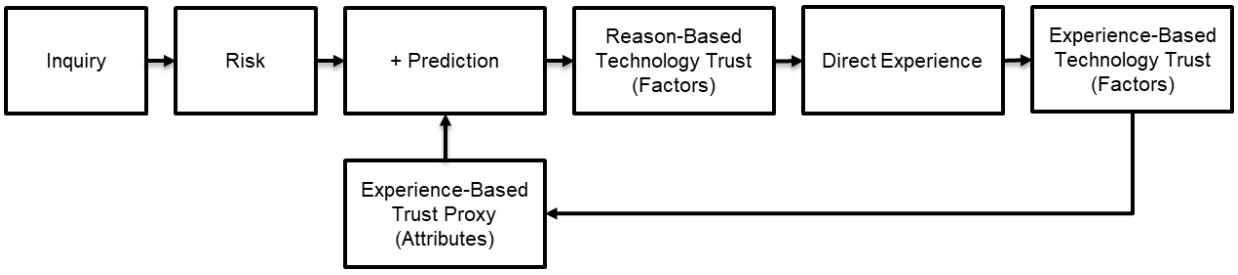

Figure 2-4. Technology Trust Life Cycle

A theory relevant to measuring and characterizing trust is found in the technology acceptance model (TAM) developed by Fred Davis nearly 30 years ago. This model plays a significant role in the majority of research investigating the factors and attributes that influence the acceptance of a technology. In the work by Venkatesh and Bala (2008), they present the TAM's ability to predict individual adoption and use of technology. The TAM assesses the

behavioral intention to use a technology through two constructs: perceived usefulness (PU), which is defined as the extent to which a person believes that using a technology will enhance his or her job performance, and perceived ease of use (PEOU), which is defined as the degree to which a person believes that using a technology will be free of effort. These two variables are used to establish a relationship between external influences and potential system usage (Gefen et al., 2003). In the work by McKnight et al. (2002), it was experimentally determined that the TAM variables do not predict continued use of a technology outside of initial acceptance, and that trust in a vendor's past technology does not translate to acceptance of subsequent technologies.

Tétard and Collan (2009) address the challenges of adopting new technology in their work on the lazy-user theory. This theory states that a user will select the technology that demands the least amount of effort to do the job. This theory also addresses one of the themes identified in our early grounded theory study interviewing operators of technology in high-risk scenarios. The application of this theory places technology users at a disadvantage, particularly in high-risk military applications where trustors are known to avoid more capable technology for systems that are easier to understand. If an experience-based proxy can improve the accuracy of developing trust through increased technology literacy, it may lead to increased acceptance of more complex and capable technologies thereby reducing the influence of the lazy-user theory. This leads to our third research hypothesis.

H3: An experience-based proxy will decrease the influence of the lazy-user theory on technology acceptance.

Conclusions

One intent of this section is to identify gaps in research on trust in autonomous systems. It appears that a methodology of technology discovery that leads to trust is not available. This review reveals a clear distinction between reason-based trust and experience-based trust. It also suggests that users are willing to trust technology in high-risk environments, and that an experience-based proxy may increase the quality of such a relationship and the pace at which it is established. Based on the finding in literature, Figure 2-5 illustrates a conceptual framework for a causal methodology of technology adoption by introducing an experience-based proxy that is hypothesized to improve technology adoption. The impact of a proxy introducing inaccurate information is noted as significant but is outside the scope of this work.

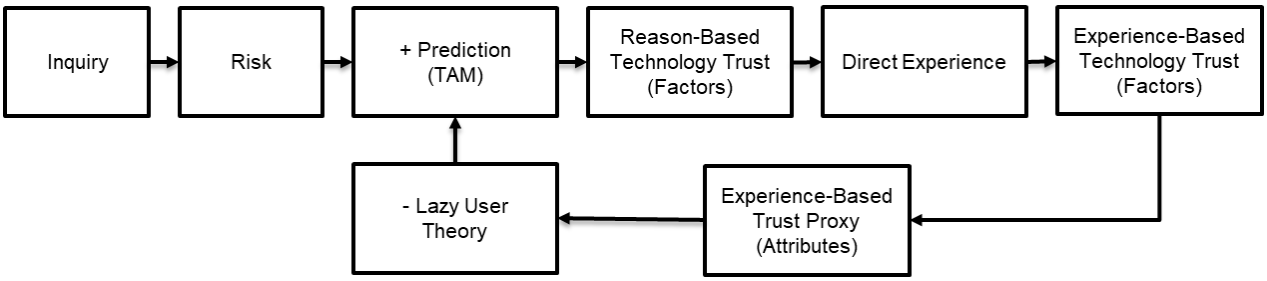

Figure 2-5. Conceptual Framework for Methodology Leading to Technology Trust

Experiment Methodology

This experiment investigates the formation of trust in technology and how it influences the adoption of autonomous systems for use in high-risk military applications. The formation of trust in technology is governed by two constructs: reason-based trust and experience-based trust. Existing literature presents the case for increased accuracy in technology selection through the development of experience-based trust. However, the development of experience-based trust is

financially burdensome and takes much longer to form. In most military scenarios, developing experience-based trust presents high levels of risk for physical injury and harm.

Introduction

This experiment is designed to identify trust metrics and how they influence the formation of reason-based trust in autonomous systems used in high-risk military applications. The desired outcome of this work is the identification of attributes that can replace some of the burden required to develop experience-based trust. This research does not intend to demonstrate the validity of the theories behind technology acceptance. Rather, this work investigates potential causal relationships between the manipulation of information and its effect on trust in technologies.

The experiment is conducted in two-phases. Phase one is a group-administered experimental survey that employs manipulations of multiple theories of technology acceptance in order to collect data on reason-based trust in autonomous systems. Phase Two consists of administering the same survey following extensive field testing and experimentation of the phase one systems to provide external validity.

Metrics

The goal of this work is to study the influence of trust metrics on the acceptance of autonomous systems in high-risk applications. However, the complexity of modern technology makes it difficult to establish generalizable metrics that can function as a proxy for experience-based trust. One area of research relevant to establishing such metrics involves the use of anthropomorphism, the attribution of human traits to nonhuman entities, to increase a trustor's ability to accept and utilize technology. Waytz et al. (2014) discuss the need for humanlike mental models to consider technology as a trustworthy teammate. There are reported cases (Pak et al., 2012) where the tendency to anthropomorphize technology leads to situations in which humans give a higher degree of trust to a technology than is warranted. The inverse of this situation also exists in the development of a lack of trust in a human teammate caused by the introduction of technology with more capability and reliability. The work conducted by Waytz et al. (2014) includes a study that found test subjects were quicker to forgive a trustee's mistakes and stay calm in high-stress situations when the trustee was a technology with humanlike attributes. This work provides a foundation for the establishment of our technology trust metrics.

HAL Score

In this work we hypothesize that statistically significant differences will result in technology trust by anthropomorphizing an experience-based proxy. This hypothesis is based on leading theory used to increase cognition in students enrolled in a college-level computer architecture course. Over a period of ten years, the author of this paper provided instruction to university year-three engineering students on the topics of digital design and computer architecture. The predominant challenge reported by students in end-of-year course evaluations was difficulty synthesizing the highly complex components of a computer into a usable system. Based on student feedback, a method for reducing complexity was developed by anthropomorphizing the components of a computer. This theory provided students with the context needed to understand how the pieces of a computer function together to create a whole system. The work resulted in increased student comprehension and an ability to describe a computer from the elemental circuits up to the most advanced concepts of computer engineering such as compilers and operating systems.

To develop the measurement system needed for an experience-based technology trust proxy, we introduce the anthropomorphic technology categories of *hardware*, *algorithms*, and *links* (HAL) as illustrated in Figure 3-1.

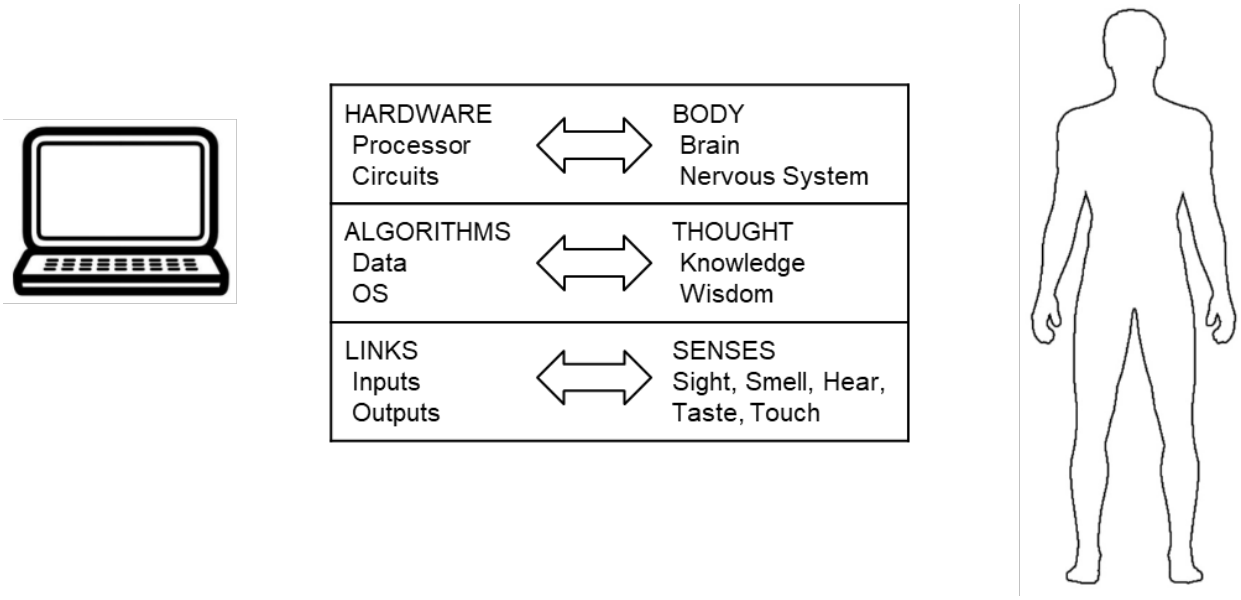

Figure 3-1. Anthropomorphic Technology Trust Metrics

In order to increase the familiarity for military end-users, the metrics are established through the HAL scoring system. The values of each HAL subsystem initially range from 0 to 100 and lead to an equally weighted maximum score of 300. This scoring system is identical to the Physical Fitness Test (PFT) employed by the United States Marine Corps. The PFT scores three physical fitness tests each scored from 0 to 100. The individual tests are pull-ups, crunches, and a 3-mile run that result in a maximum combined score of 300. Future research intends to identify weights for the HAL score that accurately reflect the overall impact on trust. For the purposes of this experiment we integrate the HAL score as a proxy for experience-based trust as shown in Figure 3-2.

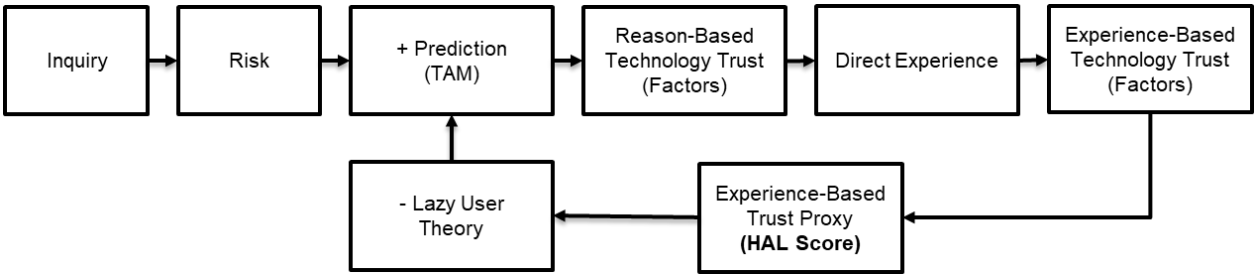

Figure 3-1. HAL Score Experimental Model

Data Analysis Plan

This study will employ Repeated Measures ANOVA. The variables in this study create a mixed design scenario. The first manipulated variable, metric, is a between-subjects factor and applies a treatment between two groups. The second manipulated variable, System Control, is a within-subjects factor, and each subject receives all three treatments of low (autonomous), medium (remote-control), and high (tethered control).

There are validity concerns due to fixed-effects seen in a repeated measure study. The participants may weight the system control variable based solely on whether or not they like the

accompanying technology. To correct for such effects, techniques such as multilevel modelling may be employed in place of repeated measures analysis.

Success in this research is realized through statistically significant results leading to a new theory on the causal relationship between anthropomorphic trust metrics and the intent to use an autonomous system.

Proposed Schedule

Date	Process
Mar–April 2019	Data Collection
April–May 2019	Data Analysis
May 2019	Initial Findings
July–Aug 2019	Field Testing
Sep 2019	External Validity Data Analysis
October 2019	Final Report

Conclusion

The topic of trust in technology is increasingly important to the DoD as outlined in the Defense Science Board Study on Autonomy (David &Nielsen, 2016) that states, "There is a need to build trust in autonomous systems while also improving the trustworthiness of autonomous capabilities. These are enablers that align RDT&E processes to more rapidly deliver autonomous capabilities to DoD missions."

This work involves the introduction of novel ideas to existing theories that relate to the formation of trust. This research focuses on the impact of trust toward the adoption of autonomous systems. We have established that trust involves a user assuming some level of risk. The only literature available on technology trust involves situations that expose users to insignificant levels of risk. We posit that our research conducted on technology used in high-risk military application will reveal causality not identified in previous trust research.

References

Adams, B. D., & Webb, R. D. (2002). Trust in small military teams. In *7th international command and control technology symposium* (pp. 1–20).

Boon, S. D., Holmes, J. G., Hinde, R. A., & Groebel, J. (1991). *Cooperation and prosocial behavior*. Cambridge University Press Cambridge.

Castelfranchi, C., & Falcone, R. (2010). *Trust Theory: A socio-cognitive and computational model*. John Wiley & Sons.

Cho, J.-H., Chan, K., & Adali, S. (2015). A survey on trust modeling. *ACM Computing Surveys (CSUR)*, *48*(2), 28.

David, R. A., & Nielsen, P. (2016). *Defense science board summer study on autonomy*. Defense Science Board Washington United States.

Devitt, S. K. (2018). Trustworthiness of autonomous systems. In *Foundations of Trusted Autonomy* (pp. 161–184). Springer.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51–90.

Hoff, K. A., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*(3), 407–434.

Kramer, R. M., & Tyler, T. R. (1996). *Trust in organizations: Frontiers of theory and research*. SAGE.

Lankton, N. K., McKnight, D. H., & Tripp, J. (2015). Technology, humanness, and trust: Rethinking trust in technology. *Journal of the Association for Information Systems*, *16*(10), 880.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359.

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems (TMIS)*, *2*(2), 12.

Pak, R., Fink, N., Price, M., Bass, B., & Sturre, L. (2012). Decision support aids with anthropomorphic characteristics influence trust and performance in younger and older adults. *Ergonomics*, *55*(9), 1059–1072.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of Personality and Social Psychology*, *49*(1), 95.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404.

Schaefer, K. E. (2016). A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems. *Human Factors*, 24.

Tétard, F., & Collan, M. (2009). Lazy user theory: A dynamic model to understand user selection of products and services. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1–9). IEEE.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315.

Waytz, A., Heafner, J., & Epley, N. (2014). The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle. *Journal of Experimental Social Psychology*, *52*, 113–117.

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net