Trustworthiness and IT Suspicion: An Evaluation of the Nomological Network

Joseph B. Lyons, Charlene K. Stokes, Kevin J. Eschleman, Gene M. Alarcon, and **Alex J. Barelka,** Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio

Objective: The authors evaluated the validity of trust in automation and information technology (IT) suspicion by examining their factor structure and relationship with decision confidence.

Background: Research on trust has burgeoned, yet the dimensionality of trust remains elusive. Researchers suggest that trust is a unidimensional construct, whereas others believe it is multidimensional. Additionally, novel constructs, such as IT suspicion, have yet to be distinguished from trust in automation. Research is needed to examine the overlap between these constructs and to determine the dimensionality of trust in automation.

Method: Participants (N = 72) engaged in a computer-based convoy scenario involving an automated decision aid. The aid fused real-time sensor data and provided route recommendations to participants who selected a route based on (a) a map with historical enemy information, (b) sensor inputs, and (c) automation suggestions. Measures for trust in automation and IT suspicion were administered after individuals interacted with the automation.

Results: Results indicated three orthogonal factors: trust, distrust, and IT suspicion. Each variable was explored as a predictor of decision confidence. Distrust and trust evidenced unique influences on decision confidence, albeit at different times. Higher distrust related to less confidence, whereas trust related to greater confidence.

Conclusion: The current study found that trust in automation was best characterized by two orthogonal dimensions (trust and distrust). Both trust and distrust were found to be independent from IT suspicion, and both distrust and trust uniquely predicted decision confidence.

Application: Researchers may consider using separate measures for trust and distrust in future studies.

Keywords: trust in automation, suspicion, trustworthiness, decision confidence

Authors' Note: The authors of this article are U.S. government employees and created the article within the scope of their employment. As a work of the U.S. federal government, the content of the article is in the public domain. Address correspondence to Joseph B. Lyons, Air Force Research Laboratory, 2698 G St., Bldg. 190, Wright-Patterson AFB, OH 45433-7604; e-mail: Joseph.lyons@wpafb.af.mil.

HUMAN FACTORS
Vol. 53, No. 3, June 2011, pp. 219–229.
DOI: 10.1177/0018720811406726.

INTRODUCTION

Research on trust, specifically, trust in automation, has burgeoned in recent years because of the proliferation of automation throughout our society. Automation, herein defined as the "execution by a machine agent of a function that was previously carried out by a human" (Parasuraman & Riley, 1997, p. 231), has become an omnipresent aspect of modern life. The role of automation in daily life is vast, and this trend of placing more and more human activity in the hands of automated tools will continue to grow at exponential rates. This trend is evident within military doctrine, which calls for increased use of automation to supplant the inherent information-processing limitations of humans. Increasingly, the role of humans is to supervise automated tools, monitor automated tool performance, and intervene when needed (Muir, 1994). However, there are sometimes costs associated with automation, and these costs may lead to unintended consequences (Parasuraman & Riley, 1997).

For example, research has shown that highly reliable automation fosters complacency among users (Rovira, McGarry, & Parasuraman, 2007), which, in turn, can lead to catastrophic performance errors. Some high-profile accidents have been blamed on overreliance on automation. Thus, researchers are called to better understand when and how humans will develop "appropriate reliance" on automated tools (Lee & See, 2004). However, measurement of trust in automated systems has proven to be an elusive endeavor. The current study explored the construct validity of an established trust-in-automation scale in relation to a novel scale measuring information technology (IT) suspicion. This study is the first of its kind to simultaneously explore the dimensionality of trust in automation and IT suspicion.

Trust represents an individual's intention to accept vulnerabilities from others with the expectation of positive outcomes (Mayer, Davis, & Schoorman, 1995). Research on interpersonal trust has distinguished trust from its antecedents. Notably, interpersonal trust is believed to be driven by dispositional forces (e.g., one's propensity to trust) and indicators of trustworthiness (e.g., ability, integrity, and benevolence) (Colquitt, Scott, & LePine, 2007; Mayer et al., 1995; Mayer & Davis, 1999). Yet trust is relevant within interpersonal relationships and in interactions with automation (Lee & See, 2004; Madhavan & Wiegmann, 2007; Parasuraman & Riley, 1997). Foundational trust-in-automation research revealed that human perceptions of trust predicted the use of automated aids in supervisory control scenarios above and beyond the actual reliability of the system (Lee & Moray, 1994; Muir & Moray, 1996). This work was critical in demonstrating that the psychological experience of trust was a significant influence on how humans interacted with automated systems. Yet questions still remain regarding appropriate measures of trust in automation.

Within the past decade, researchers have explored measures for gauging trust in automation. Jian, Bisantz, and Drury (2000) tested a series of items related to Sheridan's (1988) taxonomy of trust dimensions (reliability, robustness, familiarity, understandability, explication of intent, usefulness, and dependence) as well as Muir and Moray's (1996) trust dimensions (predictability, dependability, faith, competence, responsibility, and reliability). It should be noted that unlike the interpersonal trust literature, research on trust in automation has not typically distinguished trust from trustworthiness. Notably, the dimensions discussed here largely reflect aspects of trustworthiness. Jian and colleagues found evidence for a unidimensional scale to index perceptions of trustworthiness of the automated system. However, researchers have suggested that trust and distrust are independent constructs. For example, Lewicki, McAllister, and Bies (1998) believe that trust and distrust represent psychological states that involve some degree of certainty about a stimulus in either a positive (i.e., trusting) or negative (i.e., distrusting) fashion.

Furthermore, research on dispositional trust in e-commerce has shown that dispositional forms of trust and distrust are orthogonal (McKnight, Kacmar, & Choudhury, 2004). This perspective raises two important questions regarding the nomological network of trust in automation. First, are trust and distrust of automation orthogonal constructs, or are they merely two ends of a unidimensional trust in automation construct? Second, if trust and distrust are separate factors that represent movement toward certainty with regard to a particular stimulus, what factor could be used to account for uncertainty in a target stimulus? To address the second question, one must look to the concept of suspicion.

When individuals are uncertain about the implications of a particular stimulus, they may become suspicious of that object. Suspicion, therefore, can be defined as the degree of uncertainty one has when interacting with a particular stimulus, in this case, a computer system that includes an automated tool. One possible way to index this uncertainty is to examine perceptions of anomalies within a situation. Research supporting the concept of suspicion has emerged in the interpersonal domain whereby researchers were focused on understanding suspicion and deception within communication. Early work on deception detection identified a dispositional tendency for some individuals to be biased toward suspecting others of trying to deceive them (i.e., generalized communicative suspicion; Levine & McCornack, 1991). This research led to the development of an assessment to determine the extent to which individuals were suspicious of others called the Generalized Communications Suspicion Scale (GCS; Levine & McCornack, 1991).

More recently, research has shown that individuals' scores on the GCS were negatively related to the propensity to trust in two studies (Bond & Lee, 2005); however, factor analytic methods were not incorporated to examine the factor structure of these two constructs. The moderate correlations reported by Bond and Lee (2005; rs = –.50 and –.41) suggest that trust

and suspicion are related but not completely dependent constructs.

In addition to the dispositional aspects of suspicion, McCornack and Levine (1990) discuss state-based suspicion, which is driven by contextual cues suggesting that a stimulus is of questionable veracity. These cues may represent dissonance between one's expected reality and one's perceived reality. Given the proliferation of computers, it is likely that many if not most people in modern societies have preexisting attitudes about using computers. When these computer systems perform in anomalous ways, individuals' expectations may be violated, resulting in tension or, in this case, suspicion. Trustworthiness indicators are also cues used to establish perceptions of a stimulus, yet little is known about the relationship between trustworthiness cues and state-based suspicion, as both are influenced by cues that must be perceived by an individual.

A recent study provides some evidence that trust and suspicion are independent processes. Sinaceur (2010) created conditions in which participants were cued to either trust, distrust, or be suspicious of another person in an interpersonal scenario. The researcher manipulated trustworthiness indicators to induce high and low trustworthiness as well as uncertainty (i.e., suspicion). Participants in the suspicion condition engaged in greater information search tactics relative to the trust and distrust conditions. Furthermore, participants in the suspicion condition evidenced more conscious motive attributions to the actions of the other person in the scenario, which suggests that these participants were more critical of their fellow participants' motives. However, it is unclear how suspicion, specifically, suspicion associated with IT, relates to trust in automation. In the current study, we evaluated these two constructs using factor analytic methods.

Trust in automation was believed to be independent of one's suspicion beliefs regarding the computer system in which the automation resides. In addition to using factor analysis, the authors tested the unique influence of both trust in automation and IT suspicion on decision confidence. Past research has shown that extreme suspicion is negatively related to confidence in one's decisions (Toris & DePaulo, 1985). Furthermore, research has also shown that decision confidence affects reliance on automated tools (Lewandowsky, Mundy, & Tan, 2000). In the current study, an automated tool offered decision support to users during a decision-making scenario, and as such, it represents a more proximal influence on decision confidence relative to IT suspicion. Proximal constructs have a greater impact on behavior and attitudes relative to more distal constructs (Fishbein & Ajzen, 1975); thus, trust in automation was expected to be related to decision confidence, and IT suspicion was not.

In summary, we explored the factor structure of trust in automation and IT suspicion while examining their unique relationships with a relevant outcome for scenarios requiring interactions with automated tools, namely, decision confidence. It was expected that trust in automation and IT suspicion would comprise orthogonal constructs. Furthermore, it was expected that trust in automation (as a more proximal construct) would uniquely predict decision confidence and that IT suspicion (as a more distal construct) would not.

METHOD

Participants

Participants ($N = 72$) from a midwestern Air Force base participated in the study on a volunteer basis with no remuneration. The age distribution of the sample ranged from 18 to 66 (mean = 37). The majority of the sample were male (75%), and most of the sample were government civilians (60%), followed by military (20%) and students (20%). Almost all (98%) of the sample reported moderate to high comfort in operating computers, 91% indicated spending at least 13 hr or more working on a computer during a typical week, and 70% indicated working on a computer at home for at least 5 to 7 hr per week. Thus, the participants in this sample were highly familiar with computers. However, none of the participants had any experience with the computer-based decision-making scenario used in the present study.

TABLE 1: Rotated Factor Loadings for Study Items

	Factor			
Item	Trust	Suspicion	Distrust	Unknown
Trust				
1. The system behaves in an underhanded manner	−.05	−.23	**−.70**	−.18
2. I am suspicious of the system's intent, action, or output	−.18	−.23	**−.75**	−.10
3. I am wary of the system	−.18	−.26	**−.59**	−.23
4. The system's action will have a harmful or injurious outcome	−.26	−.24	**−.70**	.09
5. I am confident in the system	**.84**	.07	.22	.04
6. The system provides security	**.73**	.03	.03	.15
7. The system has integrity	**.71**	.03	.18	.17
8. The system is dependable	**.87**	.08	.05	.18
9. The system is reliable	**.82**	.14	.18	.14
10. I can trust the system	**.78**	.23	.16	.01
11. I am unfamiliar with the system	.11	.03	.39	.41
Suspicion				
1. I have confidence in the integrity of the data stored on this computer	.29	.19	.26	.75
2. I noticed no unusual behaviors	.02	**.65**	.20	.24
3. I was never concerned about my computer working properly	.23	**.71**	.20	.17
4. I noticed no unfamiliar behaviors	.13	**.85**	.03	.02
5. The output of the computer was valid	.12	.52	.37	.49
6. I believe I have full access to all data stored locally on this computer	.29	.33	−.12	.48
7. My computer was acting normally	.13	**.71**	.21	.22
8. The software on this computer operated the way I expected	.22	**.55**	.36	.05
9. I was not suspicious about what my computer was presenting to me	−.15	**.66**	.33	−.07

Note. Items selected for a particular factor are bolded.

Measures

Trust in automation. Trust in automation was measured with the use of an established 11-item scale (Jian et al., 2000). Participants used a 7-point Likert-type scale to rate their agreement with items that asked about reliability, dependability, and other aspects of the automation (the full scale can be found in Table 1).

IT suspicion. IT suspicion was measured with the use of a 9-item scale. Participants used a 7-point Likert-type scale to rate their agreement with items assessing their perception of abnormal activities within the IT system during the experiment. Example items include "I noticed no unusual behaviors," "My computer was acting normally," and "The software on this computer operated the way I expected it to."

Decision confidence. Decision confidence was measured with the use of a 5-item scale created for this study. Following their route choice, participants used a 7-point Likert-type scale to rate the degree to which they were confident in their route choice. Example items included "I feel

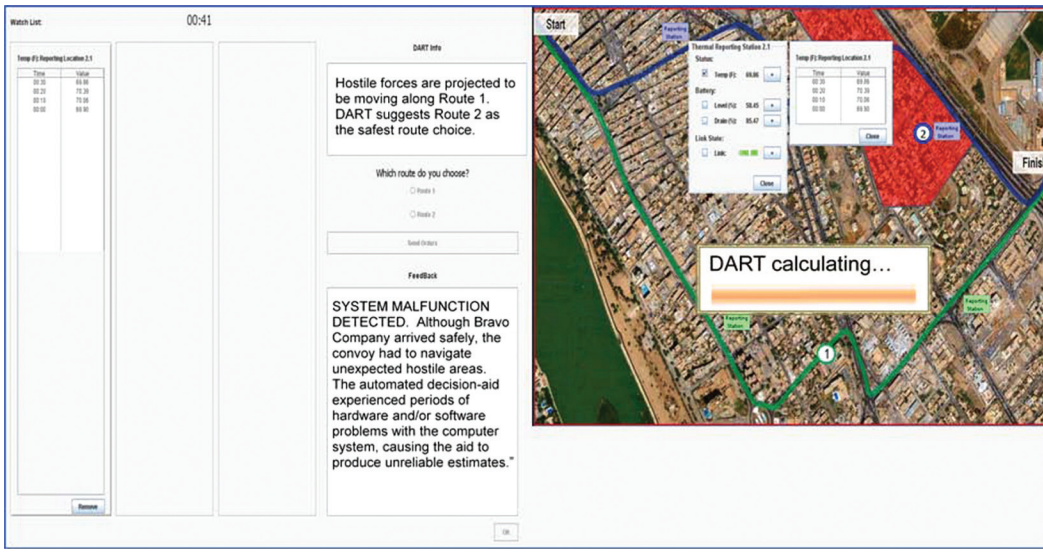

Figure 1. Screenshot of the modified Convoy Leader 2.0 software.

confident about my decision" and "I feel like I made the right choice."

Experimental Task

A modified version of the research platform Convoy Leader (Lyons, Stokes, Garcia, Adams, & Ames, 2009) was used as the experimental platform. Convoy Leader is a computer-based task that simulates a convoy scenario. Participants were asked to select the best possible route based on (a) a map display indicating historical hostile areas; (b) streaming sensor data informing the participant of the thermal, audio, and magnetic activity in four overlapping areas; and (c) an automated-decision aid that generated newly projected hostile areas and a suggested route based on real-time data (see Figure 1 for a screenshot).

Following a training phase including two practice trials, participants completed nine 3-min trials, each of which presented two route options. Vulnerability, a critical assumption within the trust domain, was established by scenarios in which participants were forced to make decisions based on conflicting information. A low-vulnerability route was characterized by agreement between historical hostile areas on the map display and projected hostile areas generated by the automated-decision aid, indicating a safe route. In high-vulnerability routes, the historical hostile areas conflicted with the aid's projected areas, forcing participants to place trust in either the historical map display or the automated aid. Previous research has shown that this type of manipulation influences risk perceptions (Stokes & Lyons, 2009).

Procedure

Experimental sessions were held in a computer laboratory, and participants conducted the experiment at separate stations. After obtaining informed consent, participants completed a background survey, which included demographics (e.g., age, gender) as well as several questions relating to their use of computers at work and at home. Following the background survey, participants completed a short task training phase (approximately 20 min) that included a slide presentation describing the task in detail and two 3-min practice trials to familiarize the participants with the interface. The training was piloted with a few individuals prior to the experiment to ensure that the training provided adequate information for potential participants in terms of ensuring their competence and understanding of the task. At the conclusion of the training phase, participants completed the experimental trials. The nine experimental trials were split into three sessions

(three trials each), and the trust and IT suspicion measures were completed at the end of each session. Decision confidence scales for each trial were averaged for each session.

RESULTS

All scales evidenced acceptable reliability (all coefficient alphas were >.70; Nunnally, 1978). Principal axis factoring with a varimax rotation was used to examine the factor structure of the items. Items were dropped when they did not clearly load onto a single factor (e.g., evidencing high factor loadings on multiple factors). This situation occurred for Item 11 on the trust-in-automation scale and Items 5 and 6 in the suspicion scale. As shown in Table 1, four factors emerged with eigenvalues greater than 1.0. However, the fourth factor was not interpretable with only one item, and thus, Item 1 (from the suspicion scale) and, subsequently, the fourth factor were dropped from further analyses. The three remaining scales were created without the aforementioned items. The first factor accounted for 37% of the variance. The second factor added 16% of the variance, and the third factor added 9% of the variance accounted for. After review of the items, we labeled the factors *trust*, *suspicion*, and *distrust* for Factors 1 through 3, respectively. The suspicion items were reverse coded such that higher scores denote higher levels of suspicion.

As shown in Table 2, trust, suspicion, and distrust were moderately correlated. Specifically, trust was negatively related to both distrust and suspicion, and distrust was positively related to suspicion. Given the correlations between trust, distrust, and suspicion, hierarchical multiple regression analyses were used to ascertain their unique relationships with decision confidence and subsequent changes in decision confidence. As shown in Tables 3 through 5, distrust initially predicted less decision confidence at Time 1, and trust uniquely predicted greater decision confidence at Time 2.

DISCUSSION

In the current study, we examined the construct validity of trust in automation and IT suspicion using factor analytic procedures. To date, no studies have simultaneously examined trust in automation and IT suspicion. The results indicated that trust in automation and IT suspicion represent orthogonal constructs. Trust in automation was best characterized as a two-dimensional construct consisting of trust and distrust. These findings are consistent with Lewicki and colleagues' (1998) proposition that trust and distrust are orthogonal constructs and adds to the growing empirical evidence that suggests that trust and distrust are orthogonal processes (McKnight et al., 2004). Additionally, neuroimaging studies have shown that trust and distrust activate different parts of the brain (Dimoka, 2010), which suggests that trust and distrust may be involved in different cognitive or emotional processing. In fact, researchers have suggested that trust is based on feelings of calmness and security, whereas distrust is associated with fear and worry (McKnight & Chervany, 2001).

Ultimately, a lack of trust in automation does not mean high distrust of that automation. Similar to state affect, whereby positive state affect and negative state affect are actually orthogonal (Watson, Clark, & Tellegen, 1988), trust in automation appears to be best represented by two constructs with either a positive or a negative valence. It may be that trust and distrust represent correspondence to perceptions that are either positive or negative with some degree of certainty (Lewicki et al., 1998).

Attitudes about the trustworthiness (or lack of trustworthiness) of an automated system appear to be independent of the suspicion beliefs targeting the larger IT system that encompasses the automation. Previous researchers have suggested that state-level suspicion is driven by cues in the environment (McCornack & Levine, 1990). Similarly, trustworthiness of an automated system is driven by cues related to the system's performance (Merritt & Ilgen, 2008; Muir, 1994). The current research shows that these cues may be different depending on the target in question, be it an automated tool or, more broadly, an IT system.

The current study also demonstrated that trust in automation and IT suspicion have differential effects on decision confidence. Initial distrust predicted less decision confidence. It may be that negative information weighs more heavily than positive cues when making trust-based decisions

TABLE 2: Descriptive Statistics and Correlations of Study Variables

Variable	*M*	*SD*	1	2	3	4	5	6	7	8	9	10	11	12
1. Suspicion Time 1	4.34	.89	(*.87*)											
2. Suspicion Time 2	4.37	.93	.72**	(*.88*)										
3. Suspicion Time 3	4.46	.94	.67**	.77**	(*.92*)									
4. Distrust Time 1	3.33	1.09	.53**	.29*	.38**	(*.84*)								
5. Distrust Time 2	3.02	1.12	.49**	.45**	.44**	.70**	(*.88*)							
6. Distrust Time 3	3.34	1.24	.51**	.46**	.58**	.72**	.81**	(*.88*)						
7. Trust Time 1	4.37	.92	−.27*	−.06	−.12	−.37**	−.38**	−.32**	(*.92*)					
8. Trust Time 2	4.48	1.10	−.31**	−.26*	−.20	−.36**	−.55**	−.40**	.70**	(*.96*)				
9. Trust Time 3	4.39	1.22	−.33**	−.30**	−.31**	−.40**	−.61**	−.52**	.71**	.91**	(*.96*)			
10. Confidence Time 1	5.48	.81	−.14	−.23	−.27*	−.40**	−.37**	−.37**	.13	.05	.15	(*.86*)		
11. Confidence Time 2	4.98	.89	−.12	−.20	−.21	−.38**	−.34**	−.38**	.29*	.33**	.37**	.60**	(*.87*)	
12. Confidence Time 3	5.13	.90	−.17	−.21	−.11	−.23	−.22	−.27*	.11	.25*	.28*	.47**	.66**	(*.89*)

Note. Cronbach's alphas are in parentheses. Reliabilities for decision confidence represent the average alpha for the three trials within that period.
*$p < .05$. **$p < .01$.

TABLE 3: Multiple Regression Analyses for Suspicion, Distrust, and Trust as Time 1 Predictors and Decision Confidence as the Criteria for Times 1 Through 3

Confidence Time 1	β	R^2
Model 1		.17**
Suspicion Time 1	.10	
Distrust Time 1	−.46**	
Trust Time 1	−.01	
Confidence Time 2	**β**	**R^2 Change**
Model 1		.36**
Decision Confidence 1	.60**	
Model 2		.06†
Decision Confidence 1	.53**	
Suspicion 1	.08	
Distrust 1	−.14	
Trust 1	.19	
Confidence Time 3	**β**	**R^2 Change**
Model 1		.22**
Decision Confidence 1	.47**	
Model 2		.22**
Decision Confidence 1	.09	
Decision Confidence 2	.60**	
Model 3		.02
Decision Confidence 1	.10	
Decision Confidence 2	.66**	
Suspicion 1	−.13	
Distrust 1	.13	
Trust 1	−.09	

†$p < .10$. *$p < .05$. **$p < .01$.

TABLE 4: Multiple Regression Analyses for Suspicion, Distrust, and Trust as Time 2 Predictors and Decision Confidence as the Criteria for Times 2 and 3

Confidence Time 2	β	R^2 Change
Model 1		.39**
Decision Confidence 1	.63**	
Model 2		.09*
Decision Confidence 1	.62**	
Suspicion Time 2	.02	
Distrust Time 2	.02	
Trust Time 2	.31**	
Confidence Time 3	**β**	**R^2 Change**
Model 1		.22**
Decision Confidence 1	.47**	
Model 2		.22**
Decision Confidence 1	.09	
Decision Confidence 2	.60**	
Model 3		.01
Decision Confidence 1	.12	
Decision Confidence 2	.57**	
Suspicion 2	−.01	
Distrust 2	.06	
Trust 2	.09	

*$p < .05$. **$p < .01$.

(Lee & See, 2004), particularly early in the interaction, when trust-based perceptions tend to be influenced by familiarity (Webber, 2008). At Time 2, however, trust appeared to predict greater decision confidence, as expected. Past research has shown that machine characteristics (i.e., indicators of trustworthiness) were predictive of trust later in an interaction but not of initial trust perceptions (Merritt & Ilgen, 2008). In the current study, one's initial distrust may have been driven by participants' lack of familiarity with the system, and this may have subsequently lowered decision confidence perceptions among participants. On the contrary, perceptions of trustworthiness later in the interaction appeared to have a positive influence on participant's decision confidence.

Implications and Future Research

The current findings have important implications for research. First, trust in automation appears to be multidimensional. Researchers exploring the construct of trust in automation might consider separating this construct into positive and negative dimensions. Second, perceptions of suspicion regarding an IT system appear to be different from trust and distrust of an automated decision aid. Trust likely corresponds to positive beliefs of the trustworthiness of a system with some degree of confidence in that belief. In contrast, distrust appears to represent

a lack of trustworthiness. Suspicion, on the other hand, appears to be something else, and it warrants independent assessment in future studies. Finally, it appears that both distrust (initially) and trust influence decision confidence in meaningful ways. Thus, researchers should seek to better understand the factors that foster trust and distrust in automated systems. One way to foster calibrated trustworthiness perceptions of automation is to educate users on the potential limitations of the automation and its algorithmic underpinnings (Dzindolet, Peterson, Pomranky, Pierce, & Beck, 2003).

Future research should focus on three areas. First, researchers should examine the impact of uncertainty perceptions on trust in automation and IT suspicion. The manipulation of uncertainty appeared to be a key element that distinguished between trust, distrust, and suspicion conditions in previous research (Sinaceur, 2010). Future experiments should inject elements of uncertainty and explore whether trust, distrust, and IT suspicion show differential effects on behavior and attitudes.

Second, researchers may consider the role of affective processes when looking at trust and distrust. Past research has shown that affect influences trust perceptions within interpersonal interactions (Dunn & Schweitzer, 2005; Lount, 2010) and in interactions with automation (Stokes et al., 2010). It may be that trust and distrust correspond to positively and negatively affective experiences, as suggested by McKnight and Chervany (2001).

Finally, future research should explore the concept of perceived vulnerability. Past research has shown different effects for trust and distrust under low- and high-risk web perceptions (McKnight et al., 2004). Furthermore, studies have shown that users' reliance on different information sources varies by vulnerability levels such that individuals rely on inputs from computers significantly more often than on inputs from unfamiliar humans in high-vulnerability conditions (Stokes & Lyons, 2009). Thus, vulnerability should be considered when evaluating the differential impacts of trust and distrust.

TABLE 5: Multiple Regression Analyses for Suspicion, Distrust, and Trust as Time 3 Predictors and Decision Confidence as the Criteria for Time 3

Confidence Time 3	β	R^2 Change
Model 1		.22**
Decision Confidence 1	.47**	
Model 2		.22**
Decision Confidence 1	.09	
Decision Confidence 2	.60**	
Model 3		.01
Decision Confidence 1	.12	
Decision Confidence 2	.57**	
Suspicion 3	.07	
Distrust 3	−.02	
Trust 3	.07	

*$p < .05$. **$p < .01$.

Limitations

There are several limitations of current study. Most notably, the current study measured perceptions of trustworthiness rather than actual reliance on the automation. Unlike research in the interpersonal trust domain, the trust-in-automation literature is in need of a valid measure to separate the process of trust (i.e., reliance on an automated system) from its antecedents (i.e., system trustworthiness and dispositional influences). Although this is a limitation of the current study, it is also shared by much of the trust-in-automation literature. A second limitation is the lack of an uncertainty manipulation. Uncertainty appears to be an important factor in understanding the differential influence of suspicion. In the future, researchers should further explore how trust in automation and suspicion differ using scenarios that inject uncertainty into the situation.

Finally, the current study relied on self-report measures. Future studies should examine how trust in automation and suspicion are related to actual behavior (i.e., reliance on automated systems). Despite the use of self-report measures in the current study, past research has established a strong link between self-report measures of trustworthiness and actual reliance on automation (Lee & Moray, 1994; Merritt & Ilgen, 2008; Muir & Moray, 1996). Nonetheless, research is needed to establish a relationship between IT suspicion and behavior.

KEY POINTS

- Trust in automation was best characterized by two dimensions: trust and distrust.
- Both trust and distrust were found to be orthogonal to information technology suspicion.
- Both trust and distrust were found to uniquely predict decision confidence at different time points.

REFERENCES

Bond, G. D., & Lee, A. Y. (2005). The darkest side of trust: Validating the Generalized Communication Suspicion Scale with prison inmates. *Personality and Individual Differences*, *38*, 1429–1438. doi:10.1016/j.paid.2004.09.008

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*, 909–927. doi:10.1037/0021-9010.92.4.909

Dimoka, A. (2010). What does the brain tell us about trust and distrust? Evidence from a functional neuroimaging study. *MIS Quarterly*, *34*, 373–396. Retrieved from http://www.misq.com

Dunn, J. R., & Schweitzer, M. E. (2005). Feeling and believing: The influence of emotion on trust. *Journal of Personality and Social Psychology*, *88*, 736–748. doi:10.1037/0022-3514.88.5.736

Dzindolet, M. T., Peterson, S. A., Pomranky, R. A., Pierce, L. G., & Beck, H. P. (2003). The role of trust in automation reliance. *International Journal of Human-Computer Studies*, *58*, 697–718. doi:10.1016/S1071-5819(03)00038-7

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Jian, J., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an empirically determined scale of trust in automated systems. *International Journal of Cognitive Ergonomics*, *4*, 53–71. doi:10.1207/S15327566IJCE0401_04

Lee, J. D., & Moray, N. (1994). Trust, self-confidence, and operators' adaptation to automation. *International Journal of Human-Computer Studies*, *40*, 153–184. doi:10.1006/ijhc.1994.1007

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, *46*, 50–80. doi:10.1518/hfes.46.1.50_30392

Levine, T. R., & McCornack, S. A. (1991). The dark side of trust: Conceptualizing and measuring types of communicative suspicion. *Communication Quarterly*, *4*, 325–340. doi:10.1080/01463379109369809

Lewandowsky, S., Mundy, M., & Tan, G. P. A. (2000). The dynamics of trust: Comparing humans to automation. *Journal of Experimental Psychology: Applied*, *6*, 104–123. doi:10.1037/1076-898X.6.2.104

Lewicki, R. J., McAllister, D. J., & Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review*, *23*, 438–458. doi:10.1037/1076-898X.6.2.104

Lount, R. B. (2010). The impact of positive mood on trust in interpersonal and intergroup interactions. *Journal of Personality and Social Psychology*, *98*, 420–433. doi:10.1037/a0017344

Lyons, J. B., Stokes, C. K., Garcia, D., Adams, J., & Ames, D. (2009). Trust and decision-making: An empirical platform. *IEEE A&E Systems Magazine*, *24*, 36–41. doi:10.1109/MAES.2009.5317785

Madhavan, P., & Wiegmann, D.A. (2007). Similarities and differences between human-human and human-automation trust: An integrated review. *Theoretical Issues in Ergonomic Science*, *8*, 277–301. doi:10.1080/14639220500337708

Mayer, R. C., & Davis, J. H. (1999). The effects of the performance appraisal system on trust for management: A field quasi-experiment. *Journal of Applied Psychology*, *84*, 123–136. doi:10.1037/0021-9010.84.1.123

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*, 709–734. doi:10.2307/258792

McCornack, S. A., & Levine, T. R. (1990). When lovers become leery: The relationship between suspicion and accuracy in detecting deception. *Communication Monographs*, *57*, 219–230. doi:10.1080/03637759009376197

McKnight, D. H., & Chervany, N. L. (2001, August). While trust is cool and collected, distrust is fiery and frenzied: A model of distrust concepts. In *Proceedings of the American Conference on Information Systems* (pp. 883–888). Retrieved from http://aisel.aisnet.org/amcis2001/171

McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Dispositional trust and distrust: Distinctions in predicting high- and low-risk internet expert advice site perceptions. *E-Service Journal*, *3*, 35–58. doi:10.1353/esj.2005.0004

Merritt, S. M., & Ilgen, D. R. (2008). Not all trust is created equal: Dispositional and history-based trust in human-automation interactions. *Human Factors*, *50*, 194–210. doi:10.1518/001872008X288574

Muir, B. M. (1994). Trust in automation: I. Theoretical issues in the study of trust and human intervention in automated systems. *Cognitive Ergonomics, 37*, 1905–1922. doi: 10.1080/00140139408964957

Muir, B. M., & Moray, N. (1996). Trust in automation: Part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics*, *39*, 429–460. doi:10.1080/00140139608964474

Nunnally, J. C. (1978). *Psychometric theory*. New York, NY: McGraw-Hill.

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, and abuse. *Human Factors*, *39*, 230–253. doi:10.1518/001872008X288547

Rovira, E., McGarry, K., & Parasuraman, R. (2007). Effects of imperfect automation on decision making in a simulated command and control task. *Human Factors*, *49*, 76–87. doi:10.1518/001872007779598082

Sheridan, T. B. (1988). Trustworthiness of command and control systems. In *Proceedings of the IFAC/IFIP/IEA/IFORS Conference on Man Machine Systems* (pp. 427–431). Elmsford, NY: Pergamon.

Sinaceur, M. (2010). Suspending judgment to create value: Suspicion and trust in negotiation. *Journal of Experimental Social Psychology*, *46*, 543–550. doi:10.1016/j.jesp.2009.11.002

Stokes, C. K., & Lyons, J. B. (2009, April). Trust in computer-mediated collaboration. In J. B. Lyons (Chair), *Enhancing and understanding trust in virtual teams*. Symposium conducted at the 24th Annual Conference of the Society for Industrial and Organizational Psychology, New Orleans, LA.

Stokes, C. K., Lyons, J. B., Littlejohn, K., Natarian, J., Case, E., & Speranza, N. (2010). Accounting for the human in cyberspace: Effects of mood on trust in automation. In *Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems* (pp. 180–187). Chicago, IL: IEEE. doi:10.1109/CTS.2010.5478512

Toris, C., & DePaulo, B.M. (1985). Effects of actual deception and suspiciousness of deception on interpersonal perceptions. *Journal of Personality and Social Psychology*, *47*, 1063–1073. doi:10.1037/0022-3514.47.5.1063

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology*, *54*, 1063–1070. doi:10.1037/0022-3514.54.6.1063

Webber, S. S. (2008). Development of cognitive and affective trust in teams. *Small Group Research*, *39*, 746–769. doi:10.1177/1046496408323569

Joseph B. Lyons is the team lead for the Organizational Effectiveness research area within the 711th Human Performance Wing–Sensemaking and Organizational Effectiveness Branch (711th HPW/RHXS) at Wright-Patterson Air Force Base in Dayton, Ohio. He received his PhD in industrial-organizational psychology from Wright State University in Dayton, Ohio, in 2005. Some of his research interests include trust, leadership, stress and emotions, organizational assessment, and organizational change. He is researching the social and other contextual predictors of trust in decision making and team settings.

Charlene K. Stokes is a research psychologist with the Organizational Effectiveness research area within the 711th HPW/RHXS at Wright-Patterson Air Force Base in Dayton, Ohio. She received her PhD in industrial-organizational psychology from Wright State University in Dayton, Ohio, in 2008 and completed a postdoctoral position with 711th HPW/RHXS. Her current research thrusts include trust, emotions, and adaptive performance and understanding how these factors relate to decision making in complex settings. She has published in a variety of journals and other publications, including *Human Factors*, *IEEE A&E Systems Magazine*, *Air Force Journal of Logistics*, and *Encyclopedia of E-Collaboration*.

Kevin J. Eschleman is an associate research psychologist with the Air Force Research Laboratory and a PhD candidate at Wright State University. His research interests include longitudinal data analysis, individual differences, and occupational stress and well-being. His research has been published in top scholarly journals, such as *Journal of Applied Psychology*, *Journal of Occupational Health Psychology*, *Journal of Occupational and Organizational Psychology*, and *International Journal of Stress Management*.

Gene M. Alarcon is a postdoctoral student for the Organizational Effectiveness research area within the 711th Human Performance Wing. He received his PhD in industrial-organizational psychology from Wright State University in 2009. His research interests include stress and emotions, coping, personality, engagement, item response theory, and hierarchical linear modeling.

Alex J. Barelka is the chief of behavioral studies within the 711th HPW/RHXS at Wright-Patterson Air Force Base in Dayton, Ohio. He received his PhD from Michigan State University. His research interests include suspicion metrics, leadership, and social media.

Date received: October 19, 2010
Date accepted: February 22, 2011