The Construct of State-Level Suspicion: A Model and Research Agenda for Automated and Information Technology (IT) Contexts

Philip Bobko, Gettysburg College, Gettysburg, Pennsylvania, Alex J. Barelka, U.S. Air Force, Dayton, Ohio, and Leanne M. Hirshfield, Syracuse University, Syracuse, New York

Objective: The objective was to review and integrate available research about the construct of state-level suspicion as it appears in social science literatures and apply the resulting findings to information technology (IT) contexts.

Background: Although the human factors literature is replete with articles about trust (and distrust) in automation, there is little on the related, but distinct, construct of "suspicion" (in either automated or IT contexts). The construct of suspicion—its precise definition, theoretical correlates, and role in such applications—deserves further study.

Method: Literatures that consider suspicion are reviewed and integrated. Literatures include communication, psychology, human factors, management, marketing, information technology, and brain/neurology. We first develop a generic model of state-level suspicion. Research propositions are then derived within IT contexts.

Results: Fundamental components of suspicion include (a) uncertainty, (b) increased cognitive processing (e.g., generation of alternative explanations for perceived discrepancies), and (c) perceptions of (mal)intent. State suspicion is defined as the simultaneous occurrence of these three components. Our analysis also suggests that trust inhibits suspicion, whereas distrust can be a catalyst of state-level suspicion. Based on a three-stage model of state-level suspicion, associated research propositions and questions are developed. These propositions and questions are intended to help guide future work on the measurement of suspicion (self-report and neurological), as well as the role of the construct of suspicion in models of decision making and detection of deception.

Conclusion: The study of suspicion, including its correlates, antecedents, and consequences, is important. We hope that the social sciences will benefit from our integrated definition and model of state suspicion. The research propositions regarding suspicion in IT contexts should motivate substantial research in human factors and related fields.

Keywords: state suspicion, information technology, distrust

Suspicion is an important, yet relatively uninvestigated, topic in the social sciences, particularly in technology-oriented contexts. For example, suppose a drone operator is monitoring a computer screen that provides a visual representation of what is being seen while the drone is flying in a remote region of the world. If the information gets unusually blurry, does the operator become suspicious and wonder if the satellite transmission is being affected by solar flares or if the transmission is being tracked by the enemy? Further, assuming the transmission is indeed being tracked (and possibly even purposely distorted), what cues might lead the operator to suspect the attacker has, in turn, become suspicious that others are aware of his or her covert activities?

Or imagine an individual who is monitoring electronic transmissions of another computer operator. If the first individual sees an anomaly, does that cause him or her to be suspicious? At what level of perceived malintent do such triggers occur? And what information might lead the first operator to suspect that the second operator knows he or she is being monitored? When suspicion occurs, what is the psychological state of that first operator? What emotional and cognitive responses are associated with the state of suspicion?

Or imagine an analyst (financial, military, etc.) who, during a work-related task, encounters an untrustworthy website that asks for personal login information. At what point does he or she become suspicious and/or follow any pre-defined organizational protocols developed for these malicious situations?

The current review and analysis proceeds in two parts. In the first part, we conduct a literature-based review of the general construct of suspicion—a construct that, although important,
is associated with scant academic research. We develop a definition of state suspicion that involves the simultaneous occurrence of several components (cognitive activity, uncertainty, perceived malintent).

In the second part of our review and analysis, we begin with a three-stage model of state suspicion as it occurs in information technology (IT) contexts. The three stages involve (a) environmental cues that can induce suspicion, (b) individual differences that can influence suspicion (filters, catalysts, inhibitors), and (c) immediate derivatives and outcomes of suspicion. As each stage is described, we provide a listing of research propositions, research questions, and future research needs, which we hope will guide the field.

TOWARD A LITERATURE-BASED DEFINITION OF THE CONSTRUCT OF STATE-LEVEL SUSPICION

The Social Science Literature on Suspicion

We reviewed several social science literatures for published work that provided definitions of the concept of suspicion. Literatures included psychology (personality and social psychology subfields), human factors, management, information science, marketing, IT, and political science (including conflict resolution). We found minimal literature on suspicion. Some of the definitions were about state suspicion (e.g., Fein, 1996; Lyons, Stokes, Eschleman, Alarcon, & Barelka, 2011), some were about more generalized dispositional suspicion (e.g., Buss & Durkee, 1957, or Levine & McCormack, 1991, who had both types), and some articles did not make this distinction. Although we borrow conceptual issues from all this work, we focus our attention on state suspicion, because our resulting model is about the transient state (compare Bond & Lee, 2005) induced by IT interactions.

The minimal work we did find (often in social psychology) was only sometimes useful. For example, some authors discussed suspicion as a central variable in their study without defining it (e.g., Ferrin & Dirks, 2003, in management; Hoffman, 2007, in political science; Vonk, 1998, in social psychology; Yoon, Gurhan-Canli, & Schwarz, 2006, in marketing). If definitions were provided, they were sometimes of questionable use (e.g., Deutsch, 1958, or, in conflict management, Buss & Perry, 1992). (Deutsch [1958] is an oft-cited early researcher in this domain. His definition of suspicion is as follows: “an individual may be said to be suspicious of the occurrence of an event if the disconfirmation of the expectation of the event’s occurrence is preferred to its confirmation and if the expectation of its occurrence leads to behavior which is intended to reduce its negative motivational consequences” [p. 267].)

However, some articles provided more guidance regarding components of the suspicion construct, and they are summarized in Table 1. They led to some convergences in our analysis (see the common attributes of uncertainty, malintent, and cognitive activity earmarked in Table 1), although we note that there was no single, consistent conceptual definition of the construct of suspicion in the prior literature (as previously noted by Levine & McCormack, 1991). We summarize this literature, and the entries in Table 1, by discussing the three common components of suspicion that led to our integrative definition of state suspicion.

The characteristic of uncertainty. The factor of uncertainty appears as a key facet of several definitions of suspicion. In social psychology, Hilton, Fein, and Miller’s (1993) review of the role of suspicion in making inferences suggests that suspicious individuals “suspend their judgments” [italics added] until they are able to determine which alternative is accurate (p. 504). A similar follow-up definition by Fein (1996) was also adopted by Sinaceur (2010) in his studies on suspicion in two-person negotiation scenarios, as well as by Campbell and Kirmani (2000) in their marketing and consumer behavior studies. This suspension of judgment is consistent with the presence of uncertainty. If individuals were more certain (i.e., below some threshold of uncertainty), they might be more prone to making decisions instead of waiting. Also in social psychology, Echebarria-Echabe (2010) studied students’ suspicions when processing persuasive arguments; his definition included an implied
TABLE 1: Definitions of Suspicion From Social Science Literatures

Social psychology
— Hilton, Fein, and Miller (1993) defined suspicion as having two components of “questioning motives” and being in a state of “suspended judgment” (p. 502). Suspicious perceivers “suspend their judgments until they are able to determine” which alternative is accurate (p. 504). It is also noted that suspicion increases cognitive load. Un, CA.
— Fein (1996) defined suspicion as “a dynamic state in which the individual actively entertains multiple, plausibly rival hypotheses about the motive or genuineness of a person’s behavior” (p. 1165). The author also suggested that suspicion implies that the “other” person (i.e., the actor) is hiding something or discrediting the meaning of behavior. Un, CA, MI.
— Sinaceur (2010) adopted Fein’s definition of suspicion in dyadic, negotiation contexts (i.e., consideration of plausible, rival hypotheses about another’s motives). Sinaceur noted that suspicion is more than uncertainty because of the additional cognitions about underlying motives, although the motives can be both positive and negative. Un, CA.
— Echebarria-Echabe (2010) defined suspicion as “the preventive attitude of receptors towards a message because they think that it contains biased or hidden interests and involves some attempt at manipulation” (p. 148). Un, MI.

Marketing (and consumer psychology)
— DeCarlo (2005) defined suspicion (of motives) as a “questioning” (p. 239) of motives that underlie another’s behavior. The role of cognitive arousal was also noted. Un, CA.

Consulting psychology
— Buss and Durkee (1957) defined suspicion as “projection of hostility on to others. This varies from merely being distrustful and wary of people to beliefs that others are being derogatory or are planning harm.” In follow-up work (Buss & Perry, 1992), suspicion and resentment items loaded on the same factor. MI.

Management
— Grant and Hofmann (2011) defined suspicion as “questioning the motives or the sincerity of behavior” (n2, p. 175). Un, MI.

Communication
— Buller and Burgoon (1996) defined suspicion as “a belief, held without sufficient evidence or proof to warrant certainty, that a person’s speech or actions may be duplicitous” (p. 205). Un, MI.
— Levine and McCormack (1991) defined trait suspicion as “a predisposition toward believing that the messages produced by others are deceptive”; state suspicion is “a belief that communication within a specific setting and at a particular time may be deceptive” (p. 328). They also noted that suspicion invokes active information processing. Un, CA, MI.
— Kim and Levine (2011) defined suspicion of deception as “the degree to which a person is uncertain about the honesty of some specific communication content thereby stimulating a construal of motives in an effort to assess potential deceptive intent” (p. 52). Un, CA, MI.

Human factors
— Lyons et al. (2011, p. 220) defined suspicion as “the degree of uncertainty one has when interacting with a particular stimulus,” and they noted that suspicion is associated with tension and cognitive processing. Un, CA.
— Olson (2009, p. 13) defined suspicion as “user perceptions that the direction, duration, and intensity of an IT systems [sic] unexpected behavior will negatively impact their task.” Un, MI.

Note. The commonalities of attributes across these definitions are delineated as follows: Uncertainty (Un), Malintent (MI), and Cognitive Activity (CA).
uncertainty by students (as well as a concern about motives and intent).

In marketing, DeCarlo (2005) studied students’ suspicion of salespersons, which was defined as a “questioning” (p. 239) of the salesperson’s motives; hence uncertainty is again implied. In management, Grant and Hofmann (2011) studied the reception of an ideological message in organizations as a function of the characteristics of the message sender. They hypothesized receiver suspicion as a mediating, explanatory variable for their findings, and they defined suspicion as “questioning the motives or the sincerity of behavior” (p. 175).

A similar definition appears in the communication literature. For example, Buller and Burgoon (1996) defined suspicion as “a belief, held without sufficient evidence or proof to warrant certainty, that a person’s speech or actions may be duplicous” (p. 205), whereas Kim and Levine (2011, p. 52) used the phrase “the degree to which a person is uncertain.” Finally, in human factors, Lyons et al. (2011) defined suspicion as “the degree of uncertainty one has when interacting with a particular stimulus” (p. 220), which, in their study, was a computer system that included an automated tool.

Thus, uncertainty is likely an important component in the definition of suspicion. We emphasize “an” because this factor does not, by itself, define suspicion. For example, one can be uncertain about how to operate a software application (due to inexperience) yet not necessarily be suspicious about it.

The characteristic of (mal)intent. In the literature-based definitions of suspicion, attributions about the intent of an external agent emerged as another important component. For example, in social psychology, Fein (1996, p. 1165) mentioned an attribution about the “genuineness” of a person’s behavior. He also noted that suspicion implies that the other person is hiding something or discrediting the meaning of his or her behavior. Or, in Echebarria-Echabe’s (2010) study of persuasive arguments, suspicion is defined as “the preventive attitude of receptors towards a message because they think that it contains biased or hidden interests and involves some attempt at manipulation” (p. 148).

In management, Grant and Hofmann (2011, n2, p. 175) used the phrase “questioning the motives”; in communication, Buller and Burgoon (1996) mentioned that “a person’s speech or actions may be duplicous” (p. 205).

We also incorporate mal in the notion of intent—thereby giving suspicion a negative cast—because almost every article about suspicion assumed the potential for harm and negative outcomes, particularly in cyber contexts. However, we note that suspicion can be more general, as it can also have a positive cast (e.g., “I suspect my family is planning a surprise birthday party for me”). (Additionally, we note that in positive instances involving suspicion, the uncertainty is enjoyable [e.g., party giving; what song a DJ is going to play next]. Indeed, in management contexts, entrepreneurs might enjoy the uncertainty and risk associated with business ventures, as well as attempts to unpack suspicions about their competitors [see also LeFevre, Matheny, & Kolt, 2003, who discuss occupational stress and the concept of positive stress, or eustress]. However, the negative instances associated with suspicion [e.g., “I suspect that that person might be trying to do me harm and might be acting intentionally deviously”; “I am suspicious of the information being given me by the automated read-out”] are more fundamentally related to the cyber focus of this review.)

The characteristic of cognitive activation. Several literatures suggest another important component of suspicion; that is, a substantial increase in cognitive load when in a state of suspicion (see Bond, 2012, or Patterson, 2009, for some markers of cognitive load, such as inhibition, loss of working memory, reduced processing speed, reduced sensory functioning, excess body movement, or decreased eye blinking). For example, Fein’s (1996) social psychological review and definition of suspicion included the cognitive generation/consideration of multiple plausible, rival hypotheses for observed behavior. He noted research support for such increased cognitive activity (p. 1167). In adopting Fein’s definition in negotiation contexts, Sinaceur (2010) also noted associated increases in cognition.

In the communication literature, Levine and McCormack (1991, p. 328) suggested that suspicion leads individuals to “more actively process” incoming information, and in later work, Kim and Levine (2011, p. 52) noted that suspicion (of being deceived) stimulates individuals...
to engage in “a construal of motives.” In DeCarlo’s (2005) marketing study, he suggested that suspicion increases “sophisticated attributional thought processes” (p. 239). And in the Lyons et al. (2011) study on IT, it is suggested that suspicion is associated with increased cognition (e.g., more information search tactics).

In sum, the construct of suspicion involves uncertainty. This uncertainty may be related to future behavior and/or attributions of possible intent—and often malintent. Being in a state of suspicion also involves increased cognitive activity and load, because the actor (the suspicious person) is actively engaged in collecting data about another’s motives or cognitively generating alternative explanations for the observed behavior (see Campbell & Kirmani, 2000; DeCarlo, 2005; Fein, 1996; Levine & McCor- 
nack, 1991; Lyons et al., 2011). Further, as suggested in the foregoing section, none of these components by itself is sufficient for generating increased (or reduced) states of suspicion. For example, one can be uncertain, yet not suspi-
cious, about tomorrow’s weather. Also, as noted by a reviewer, one can be certain that an external agent is an enemy (certainty about intent), yet still be suspicious because the uncertainty is in regard to possible future behavior on that agent’s part. Thus, it is the simultaneous combination of uncertainty, perceived (mal)intent, and cognitive activity (searching for alternative explanations or new data) that defines state suspicion. (In statistical terminology, this definition implies a three-way interaction among cognitive activity, uncertainty, and malintent.)

State Suspicion in IT Contexts

To place our definition in context, we first note that IT contexts might involve electronic input or collection of data (e.g., cataloging consumer purchases; determining the length of response time on a computer display) or automated throughput/analysis of such data (e.g., encoding, summarization, or interpretation via computer algorithms). IT contexts also might involve output such as decision making (e.g., offering alternative solutions to potential aircraft conflicts; generating potential preferences/rankings of possible troop movements) or electronic implementation of courses of action (e.g., generating automatic replies to customer queries). This summary of contexts is similar to the four purposes of automation noted by Lee and See (2004, citing Parasuraman et al., 2000); that is, information acquisition, information analysis, decision selection, and action implementation. Thus, we define state suspicion in IT contexts as follows:

State suspicion in IT contexts is a person’s simultaneous state of cognitive activity, uncertainty, and perceived malintent about underlying information that is being electronically generated, collated, sent, analyzed, or implemented by an external agent.

The external agent in this definition is intentionally general; the agent could be another person, a collection of individuals (e.g., a business organization or political group), or an inanimate object (e.g., a computer or an information system). For example, in our reading of the trust and automation literature, the concept of agent sometimes referred to (a) the operator of the IT system, (b) the programmer/designer of the IT system, (c) the programmer/developer of the algorithms used in the software, (d) the software itself (without reference to the programmer, as in Bisantz & Seong, 2001), (e) the hardware in the system, (f) the entire IT system (or perhaps linked mini-systems, as in Buhler & Huhns, 2001), or (g) the organization that is using the system (see Bobko, 2012). In our model, we suggest that an individual might have state suspicion about any of these agents.

A PROCESS-BASED MODEL OF STATE SUSPICION

In the application of trust to IT, Gefen, Benbasat, and Pavlou (2008) noted a need for a conceptual framework to guide research. Thus, with our focus on IT suspicion, we also develop a three-stage process model of state-level IT suspicion.

As noted, there is a dearth of literature directly related to the definition, causes, and consequence of suspicion in IT contexts. The field is ripe for future research, and based on our review, analysis, and model (graphically depicted in
(June 2019 - Human Factors)

We present research propositions when the underlying theory appears sufficient to suggest a direction of effect for the underlying variables, and we offer exploratory research questions when the literature is less well specified.

Suspicion Stage I: Cues in the IT Environment

Cues in the environment can act as a trigger of state-level suspicion (over and above baseline levels of trait suspicion, or tendency to be suspicious, noted in Stage II). The Stage I cues include:

- **pattern of negative discrepancies**
- **missing information**
- **system and interface characteristics**

To generate relatively more specific cues, we used literature on decision making and missing information, as well as neurological literature. We also borrowed from the literature on trust in automation because (a) there is minimal literature on IT suspicion and (b) this literature sometimes parallels our analysis of the general suspicion literature. For example, many articles on trust in automation, almost by definition, assume that the external agent does not have to be an individual but could, in fact, be an automated system or other technology component (see Gefen et al., 2008, p. 281, for a similar statement). Second, articles in the literature on trust in automation implicitly note the role of uncertainty (although the focus is uncertainty reduction) in their models (Jarvenpaa & Leidner, 1999; Lee & See, 2004; Lyons et al., 2011; McKnight, Choudhury, & Kaemar, 2002; Xu, Feng, Wu, & Zhao, 2007). Third, Lee and See (2004, p. 76) noted that trust applies in automated situations, in which uncertainty and complexity make an exhaustive evaluation of options impractical. This relates to our notion that suspicion involves a generation of alternatives.

Table 2 summarizes factors that likely apply as Stage I cues to our state-level suspicion process. Note that Table 2 is not employed as a quick point of reference; rather, it is a listing and categorization of potential Stage I factors, and their reference citations, from our review of the literatures on trust in automation and on decision making.

---

Figure 1. Stages of state-level IT suspicion.

<table>
<thead>
<tr>
<th>STAGE I: cues</th>
<th>STAGE II: filters</th>
<th>STAGE III: immediate derivatives and outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing Information</td>
<td>Trust, Distrust, Training/Rewards, Individual Differences</td>
<td>Increased Cognitive Load, Emotional Arousal, Fear, Anxiety, Stress Correlates (sick, heartbeat, etc.)</td>
</tr>
<tr>
<td>Pattern of Negative Discrepancy</td>
<td></td>
<td>Neurological Indicators, Detection of Deception, Secondary Task Performance</td>
</tr>
<tr>
<td>System &amp; Interface Characteristics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1, we offer some formal propositions.
**TABLE 2:** Possible Input Factors at Stage I of the State Suspicion Process (based on Figure 1)

**Missing, incomplete, or clarifying information**
- Capacity to observe performance of the system (Lee & See, 2004)
- Explanation/understandability of the algorithms and operations and their intent; clarity of benefit of automation (Lee & See, 2004; Lyons et al., 2011; Merritt & Ilgen, 2008, citing Muir, 1994; Parasuraman & Riley, 1997)
- Specificity of system information (e.g., information support or specific recommendation; see Parasuraman & Manzey's 2010 review, p. 396, or Metzger, Flanagin, & Medders, 2010)
- Information perceived as missing (Ebenbach & Moore, 2000)
- Structural assurances (e.g., on a website or system confidence information; McKnight, Choudhury, & Kacmar, 2002; Parasuraman & Manzey, 2010, although not supported in Wang & Benbasat, 2008) and branding alliances (Lowry, Vance, Moody, Beckman, & Read, 2008)
- Willingness of persons in an electronic social system to provide personal information (Ridings, Gefen, & Arinze, 2002)
- Whether the information is focused on positive feedback (all systems working) or focused on negatives (warnings); Lee and See (2004) noted that individuals are more cautious in the latter condition

**Pattern of negative discrepancies, reliability, and validity**
- The patterns across time of failures in the system (Bisantz & Seong, 2001); for example, framing effects attributable to initial expectations (Lee & See, 2004)
- Normality of the organizational structure and/or technical situation, or assurances thereof (Li, Hess, & Valacich, 2008)
- Reliability and predictability of software being used (Jarvenpaa & Leidner, 1999, for predictable communication; Lee & See, 2004; Lyons et al., 2011; Parasuraman & Riley, 1997)
- Reliability of hardware being used (Bailey & Scerbo, 2007, citing Lee & Moray, 1992; Merritt & Ilgen, 2008)
- Integrity of the software's algorithms (matching to values of the user, Huhns & Buell, 2002; see also Lee & See's 2004 notion of “value congruence”)
- Reputation of the system or vendor (Li et al., 2008; McKnight et al., 2002)
- Accountability of the operator (see Parasuraman & Manzey's 2010 discussion of work by Mosier and colleagues)
- Accuracy or competence of the software being used (Huhns & Buell, 2002; Lyons et al., 2011; Merritt & Ilgen, 2008, citing Lee & Moray, 1992; Parasuraman & Riley, 1997)

**Environmental cues via user interface**
- Correspondence of visual interface with the actual environment being simulated (Bisantz & Seong, 2001)
- Whether or not the interface is audiovisual, audio only, or text only (Burgoon, Blair, & Strom, 2005); it was found that truth bias was strongest in the audiovisual condition, but type of interface did not influence the accuracy of deception detection
- Use of instant messaging in a running history, static format or only the current communication in a real-time format (Zhou & Zhang, 2007)
- Etiquette (e.g., patience vs. interruption) and politeness of any voice used (Parasuraman & Miller, 2004)
- Timing of responses (Jarvenpaa & Leidner, 1999; Lee & See, 2004; Ridings et al., 2002)
- Use of real pictures, good colors, and provision of a physical address when websites are being used (Lee & See, 2004)
- Ease of use of a website (“site quality” in McKnight et al., 2002; navigability, spelling, grammar in Metzger et al., 2010)
- Use of instructive tone of voice versus informational tone (Cramer, Evers, Kemper, & Wielinga, 2008); the instructive agent was perceived as more competent, although this was moderated by user locus of control
- Matching of the emotion of any system voice with emotion of the user (Nass et al., 2005)

**Miscellany**
- Time constraints (Parasuraman & Riley, 1997)
- Task complexity (Bailey & Scerbo, 2007; Parasuraman & Riley, 1997)
making. In addition, based on our findings in the literature, the missing information category was expanded to include incomplete or clarifying information; the discrepancy category was also enhanced to include reliability and validity.

For example, regarding discrepancies as cues, and consistent with the uncertainty component, state-level suspicion might be increased because of a mismatch between what is being perceived and what one expects. When operating a normally fast computer, a slow session might lead to a perceived discrepancy in expected speed, as well as generation of subsequent explanations (not enough RAM, malware, being monitored, etc.). Indeed, Oliveira, McDonald, and Goodman’s (2007) neurological study supports this notion. They suggested that any discrepancies (positive or negative) between observation and expectation will be associated with increased anterior cingulate cortex activity—an indicator of increased need for cognition and use of external information.

Missing information is another possible environmental cue (via uncertainty and malintent) that increases state suspicion. In their marketing study, Johnson and Levin (1985) noted that missing information is related to a reduction in predicted satisfaction (hence concern) with the potential purchase of a television. They pointed out that missing information is particularly salient when the missing attribute is negatively correlated with other attributes. Indeed, these authors suggested that missing information induces “suspicion” (p. 177, undefined). Other social science literature also supports the idea that missing information causes a devaluation of, or concern about, the focal object (e.g., Ebenhach & Moore, 2000, regarding environmental decisions about waste facility sites; Jagacinski, 1991, regarding personnel selection of hypothetical job candidates).

As an example of system and interface cues (our third category of Stage I variables), we suggest that the correspondence of actual and simulated environments, as well as ease of use of software, may reduce IT-induced suspicion (Bisantz & Seong, 2001; McKnight et al., 2002). Conversely, audio-only or text-only interfaces may increase suspicion relative to audiovisual interfaces (Burgoon, Blair, & Strom, 2005).

The entries in Table 2, and our model in Figure 1, lead to our first two sets of research propositions for Stage I:

**Proposition I.1:** A pattern of negative discrepancies between observed behavior by an external agent and predicted behavior of that agent will increase the observer’s (user’s) state-level suspicion. It also may be that a single discrepancy will have the same effect if the discrepancy is sufficiently large and harmful.

In addition, missing information (external systems not responding completely, visual or audio input is impaired, etc.) will increase the user’s level of state suspicion.

**Proposition I.2:** Regarding cues and the characteristics of IT system or situational attributes, state-level IT suspicion will decrease when

a. there is a good correspondence between the visual interface and the actual environment being simulated (e.g., Bisantz & Seong, 2001),
b. there is a capacity to observe performance of the system (in terms of either reliability or accuracy; e.g., Lee & See, 2004),
c. structural assurances about the system’s integrity and purpose are provided (e.g., McKnight et al., 2002) or when there is an explanation about the system’s capabilities or purpose (e.g., Lyons et al., 2011),
d. system feedback is focused on systems working normally rather than feedback about potential negative events (e.g., Lee & See, 2004),
e. system etiquette or politeness is high (Parasuraman & Miller, 2004),
f. responses are timely (e.g., Jarvenpaa & Leidner, 1999),
g. system-based decisions are presented in a clear manner (Parasuraman & Manzey, 2010),
h. the task is complex (in that complexity reduces monitoring; e.g., Bailey & Scerbo, 2007), and
i. the user generally perceives that the surrounding organization structure is normal (Li et al., 2008).

Conversely, levels of state-level IT suspicion will increase as the foregoing factors become less prevalent or otherwise violate user expectations about the IT system. (Note that Table 2 includes additional specific citations, as well as other possible influential cues.)

We also suggest that Stage I determinants of state-level IT suspicion may be bypassed (directly to Stage III) simply by telling individual users, “Be suspicious.” We consider this possibility in the discussion section, where we note the need for research on the development of training programs.

A few exploratory research questions (offered when the literature is not as well specified) about Stage I can also be generated. We hope they motivate future research as well.

Exploratory Research Question I.1 (multivariate modeling): Mathematical models of the simultaneous operation of the multiple factors in Table 2 should be investigated. For example, consider two system precursors of suspicion from the earlier listings; that is, explanation of system purpose ($X_1$) and physical representation of the simulated environment ($X_2$). If both $X_1$ and $X_2$ are positive, then presumably state suspicion is reduced. However, suppose $X_1$ is positive but $X_2$ is negative. Do these factors cancel each other out in the prediction of suspicion (i.e., an additive model)? Or if either one of the variables is negative, will state suspicion be induced (i.e., an interactive model whereby if any variable is negative, this overrides all positive factors)? And if the cues are all related to suspicion in the same direction, which cues are more salient (more heavily weighted) than others? To increase the interactive complexity, perhaps these models vary as a function of the individual difference moderators (catalysts and inhibitors) in Stage II.

Exploratory Research Question I.2 (negative events and framing): Research should consider how user behaviors are influenced by the pattern of previous successes and failures when interacting with specific IT systems. This notion might involve an application of the literature on cognitive heuristics (e.g., framing and anchoring) in human decision making (Metzger, Flanagan, & Medders, 2010; Tversky & Kahneman, 1981). Such factors occasionally appear in the literature on trust in automation (e.g., Lee & See, 2004, for framing). For example, although the two statements are arithmetically equivalent, does informing a user that a system works 95% of the time have different effects than informing a user that the system fails 5% of the time? Intuitively, the latter frame (and perhaps any negative frame about reliability and accuracy) may induce more suspicion.

Conversely, an argument could be made for the opposite effect; that is, perhaps knowing that failure is occasionally a possibility may lead to less suspicion of the system because failure is a familiar outcome. (This latter possibility is analogous to classic reinforcement theory and the notion that behavior is more difficult to extinguish after variable ratio reinforcement [Reynolds, 1968]. That is, under variable ratio reinforcement, one learns that an event [in this case, a failure/event] occasionally occurs, so behavior [attitude toward the system] does not extinguish even when the data indicate otherwise.)

Exploratory Research Question I.2b (negative events and their magnitude): Research should also consider how the salience or importance of any failure influences the aforementioned processes. For example, if each of the failures that occur 5% of the time are “small” losses, is suspicion reduced due to “minor” failures are familiar? Conversely, there might be some threshold of failure importance beyond which suspicion is aroused, regardless of prior experiences. We expect levels of this threshold to be correlated with individual differences as presented in Stage II. For example, an experienced computer user might
quickly notice, and become suspicious about, a negative event, whereas a novice computer user might more readily blame himself or herself in the presence of IT system failures, even if the system failures are substantial.

**Exploratory Research Question 1.3 (subliminal cues):** We encourage research on the subliminal manipulation of cues listed in Table 2. For example, if a user begins a task in a high state of suspicion, will subliminal messages on the user’s screen (e.g., a subliminal display of the phrase “all is well”) reduce self-reported or physiological or neurological measures of suspicion? Will the user’s behaviors focused on deception detection be reduced? There is support in the general literature for the influence of subliminal messages (see Mlodinow, 2012, for a review). For example, MacCrae, Milne, and Bodenhausen (1994) found that subjects’ use of stereotyping could be manipulated subliminally. To the extent that use of stereotypes is related to reduced cognitive energy, increased cognitive “miser-ing,” and so on, it can be hypothesized that state suspicion could be reduced subliminally. Conversely, it might be possible to increase a user’s cognitive activity and suspicion subliminally.

**Suspicion Stage II: Individual Difference Determinants (Filters, Inhibitors, and Catalysts)**

Individual differences also might play a major role in increasing, or inhibiting, state-level suspicion (e.g., trait-level propensity to be suspicious or generalized distrust may act as catalysts). We discuss the following variables in our analysis and research propositions:

- **A user’s trust in automation**, which decreases the likelihood of suspicion (via cognitive miser process)
- **A user’s lack of trust (or distrust) in automation**, which increases the potential for suspicion
- **Other, correlated individual difference characteristics of the IT user**, such as faith in humanity, fatigue, general propensity to trust, or self-efficacy
- **Training/rewarding** the user to embrace uncertainty and “be suspicious.”

We first discuss the literature on trust and distrust and then consider other individual differences variables that are likely to influence state-level suspicion in IT contexts.

**The role of trust and distrust; related but conceptually distinct concepts.** The most cited article on the construct of interpersonal trust in the management literature is by Mayer, Davis, and Schoorman (1995). Trust is defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trusting irrespective of the ability to monitor or control that other party” (p. 712). Note that there is an expectation involved in the decision to trust someone, that is, a substantial reduction in uncertainty (see also Wang & Benbasat, 2008). In another highly cited article (McAllister, 1995), trust is also linked to reductions in uncertainty. (Although the articles by Mayer and McAllister, and their focus on interpersonal trust, continue to dominate management and applied psychology, other researchers suggest that trust can occur at many levels and with many different types of agents [for example, see Lee & See, 2004]. That is, trust is also considered to occur within or between virtual teams or virtual communities [e.g., Jarvenpaa & Leidner, 1999; Ridings, Gefen, & Arinze, 2002], countries [e.g., Hoffman, 2007], Internet websites [e.g., McKnight, Kacmar, & Choudhury, 2004], automated decision aids [e.g., Huhns & Buell, 2002; Lyons et al., 2011], and new technology [e.g., Li, Hess, & Valacich, 2008].) Indeed, Colquitt, LePine, Piccolo, Zapata, and Rich (2012) empirically found that both of McAllister’s subdimensions of trust were negatively correlated with uncertainty (−.47 and −.55 for affect-based and cognition-based trust, respectively).

Based on the foregoing discussion, we suggest that trust involves a decision to act; in contrast, state suspicion is a cognitive process based in part on uncertainty. If a decision has already been formed, uncertainty is reduced and thus suspicion is reduced. As such, predispositions to trust are predispositions that remove uncertainty.
Thus, predispositions to trust will inhibit increases in state-level suspicion by deemphasizing the perception or incorporation of cues from the IT context.

The existing literature hints at this hypothesis. For example, Lee and See (2004) and McKnight et al. (2002) implied that because trust reduces uncertainty, trust may reduce the likelihood of suspicion. Buller and Burgoon (1996) also implied that trust inhibits suspicion, but via a somewhat different perspective—that is, trust leads to truth bias (a tendency to assume that someone is truthful, regardless of the veracity of his or her statements or actions).

More specifically, if one sees inconsistent behavior from a trusted external agent, one is less likely to attribute malintent to that entity and less likely to engage in cognitive effort that generates alternative explanations for the observed behavior. That is, trust, like stereotypes, economizes cognition (Gilbert & Hixon, 1991; MacCrae et al., 1994; Sherman & Frost, 2000). Indeed, too much trust can lead to complacency (see Ray, Baker, & Plowman, 2011, in management, or Bailey & Scerbo, 2007, and Parasuraman & Manzey, 2010, in trust in automation).

Regarding distrust, there is a minimal amount of literature that explicitly refers to distrust and the notion that distrust also involves a decision. For example, in social psychology, Sinaceur (2010) stated that distrust is a “negative, unilateral judgment” (p. 544). Or, in management, Lewicki, McAllister, and Bies (1998) defined distrust as “confident [italics added] negative expectations regarding another’s conduct” (p. 439). Although distrust thus implies a decision (about intent), we propose that distrust can indeed be a catalyst for state-level suspicion—by focusing one’s cognitive activity on that agent’s uncertain future behavior. Thus, given distrust, the emergence of suspicion is not focused on the (mal)intent of the external agent but is focused on cognitive activity and uncertainty regarding the agent’s unknown behavior (and possible safeguards against that behavior).

For completeness, we note that the ambivalent feeling of neither trust nor distrust could lead to both kinds of cognitive engagement associated with state-level suspicion: activity focused on uncertainty about the agent’s motives and the agent’s possible future actions. In sum, our Stage II propositions about the role of trust and distrust are as follows:

**Proposition II.1:** In the face of anomalies in the system, relatively high levels of user trust act as an inhibitor to increases in state suspicion. In contrast, distrust leads to cognitive engagement associated with suspicion, but only for cognitive activity regarding possible alternative future actions of the external agent, and not the direction of the (mal)intent. Further, individual users who neither trust nor distrust external agents will, in the face of anomalies, engage in both types of cognitive activity associated with state suspicion: cognitive activity focused on the agent’s possible intent and cognitive activity focused on the agent’s possible future actions.

**Other individual differences antecedents of state-level suspicion.** Given our definition of suspicion, we hypothesize several other individual differences variables (creativity, need for cognition, cognitive capacity/intelligence) that are likely to be empirically correlated with levels of state suspicion.

First, it is suggested that creative individuals are better able to be suspicious. Griffin and Moorhead (2010) defined creativity as the “ability to generate new ideas or to conceive of new perspectives on existing ideas” (p. 210), and tests of creativity even include the “alternative uses test” (see Lissitz & Willhoft, 1985). Thus, given that state suspicion involves generating alternative explanations, we suggest that the capacity to be suspicious is conceptually linked to individual levels of creativity.

Second, work by Echebarria-Echabe (2010) suggests that the “need for cognition” may increase levels of suspicion, because individuals who have high levels of need for cognition are “more willing to engage in systematic processing” (p. 156). For example, Cacioppo and Petty (1982) developed a need-for-cognition scale that includes items such as “I would prefer complex to simple problems.” We hypothesize that the need for cognition will be positively related to
increased levels of suspicion due to the cognitive activity component of suspicion. In contrast, individuals low on need for cognition may be motivated to take things at face value. Such a notion (related to the concept of cognitive miser) appears in the social psychology (Priester & Petty, 1995) and human factors (Parasuraman & Manzey, 2010, citing Wickens & Hollands, 2000) literatures.

Third, in regard to task performance in suspicious contexts (e.g., the detection of deception; the capacity to be suspicious yet function on secondary tasks), we hypothesize that individuals who are high on measures of cognitive capacity are more capable of performing in environments that require increased state suspicion. Given the aforementioned cognitive nature of suspicion (coding/acquisition of information in the context of uncertainty; generating alternative explanations), suspicious individuals are cognitively busy. Thus, we suggest that individuals who are relatively high on measures of cognitive capacity will be better able to function on other tasks while engaging in suspicious thoughts. We also suggest that individuals who are relatively high on measures of cognitive capacity will be better able to be suspicious. We make this suggestion with caution, however, particularly when detection of deception is the outcome measure. As a reviewer reminded us, reviews of the empirical literature indicate that detection accuracy by individuals is often close to chance levels (Bond, 2012; Kim & Levine, 2011).

As noted earlier, there was little mention of the construct of suspicion in the human factors literature (exceptions being Lyons et al., 2011, and Parasuraman & Riley, 1997). However, we borrow from the extensive literature on trust in automation to suggest yet other individual differences factors in Stage II of our model. That literature suggests the following:

- Experience and familiarity with the technology (Lee & See, 2004; Lyons et al., 2011; see also Potosky & Bobko, 1998, or Potosky, 2007, for scales that assess computing experience)
- Faith in humanity (Li et al., 2008)
- Tendency to take a trusting stance and general levels of trust (Li et al., 2008; Ridings et al., 2002)
- Conformity, inclination to use stereotypes, general negative affect, and cynicism (Bobko, 2012; Gefen et al., 2008)
- Self-efficacy and competence (“user accuracy”; Parasuraman & Miller, 2004; Parasuraman & Riley, 1997)
- Cost–benefit calculation by the user (Li et al., 2008; Wang & Benbasat, 2008)
- Workload and fatigue (Parasuraman & Riley, 1997).

For example, to the extent that faith in humanity or self-efficacy regarding technology are positively related to trust propensity, then these factors are likely to influence suspicion at Stage II (see also Parasuraman & Riley, 1997). Other dispositions that might be associated with reduced state-level suspicion, all else being equal, include conformity or tendency to use stereotypes (Bobko, 2012) or other personality traits (Gefen et al., 2008). Still other characteristics of the user might be more situation specific and include perceptions of individual workload (Parasuraman & Riley, 1997) or familiarity with the particular technology (Lee & See, 2004). We offer the following propositions regarding Stage II in our model:

**Proposition II.2a:** Individual differences across users will influence levels of IT state-level suspicion. Specifically, levels of suspicion will be increased when the user

- a. lacks familiarity with similar systems,
- b. has had some unexpected negative experiences with similar systems,
- c. lacks faith in humanity,
- d. tends to take cynical stances,
- e. lacks self-efficacy and perceived individual competence,
- f. has a minimal routine workload, and
- g. has a high need for cognition.

Conversely, inhibitors to increased levels of IT state-level suspicion include

- a. positive experiences and familiarity with similar systems,
- b. faith in humanity,
c. tendency to take a trusting stance and general disposition to trust,
d. self-efficacy and perceived personal competence, and
e. high workload and/or fatigue.

Proposition II.2b: Individual differences across users, specifically cognitive capacity and creativity, will also influence the capacity to be suspicious. More specifically, cognitive capacity will increase the ability to be suspicious and engage in secondary tasks. Further, we tentatively suggest that both cognitive capacity and creativity might be associated with increased success in detection of deception.

Proposition II.3: The individual differences in Proposition II and the situational characteristics in Proposition I will combine in an interactive manner (see, e.g., Bobko, 2001, for a discussion of interactions) to predict levels of state suspicion. For example, consider the individual differences variable of “experience with similar systems” and the situational characteristic of “correspondence between visual interface and simulated environment.” The state-level suspicion of highly experienced (e.g., expert) operators will be increased by relatively small discrepancies between interfaces and simulated environments. In contrast, inexperienced users will require larger discrepancies before their state-level suspicion is increased.

Suspicion Stage III: Immediate Derivatives and Outcomes

Our definition and analysis of state-level IT suspicion suggested that when one is in a suspicious state (Stage III), cognitive activity or load is increased. During this stage, the user’s cognitive activity is a central (but, as noted, not sufficient) component of state-level suspicion. Such cognitive activity occurs because the suspicious observer is engaged in looking for alternative “pieces” of information and/or generating alternative explanations for observed behavior. In an empirical confirmation of this increased cognitive processing, Vonk (1998) demonstrated that suspicious subjects took longer to read textual stimuli than less suspicious subjects (see also Buller & Burgoon, 1996). Recent neurologically based studies also indicate that suspicion involves substantial cognition (see Dimoka, 2010). Conversely, Parasuraman and Manzey (2010, citing Weiner) noted the link between complacency (and lower cognitive load) and a lack of suspicion.

We suggest that state suspicion at Stage III is also associated with emotional reactions— but they would be reactions of anxiety and fear (given the uncertainty component), whereas distrust might be associated with reactions of anger (about a negative event and its causal agent). We note these immediate outcomes in our model in Figure 1.

Indeed, Huddy and Feldman’s (2011) analysis of reactions to the events of 9/11 suggest that in negative situations, anxiety was linked to uncertainty, whereas anger was linked to certainty. In yet another context (political doves vs. hawks), a similar suggestion was made in Mahoney’s (2011) analysis of the Cuban missile crisis in the 1960s. Mahoney states that the hawks’ view of the crisis was “predictable” and “controllable,” whereas the doves’ view of the crisis was, among other things, “unpredictable.” The doves thus felt “enormous anxiety throughout, while the hawks felt virtually none” (p. 204).

Our research propositions for immediate, psychological consequences of Stage III are the following:

Proposition III.1: As individual users become more suspicious, their cognitive load will increase (and markers of cognitive load such as working memory or speed of processing will decrease). Further, as state suspicion increases, the (mal)intent and uncertainty facets will result in increased emotional facets (characterized by fear and anxiety rather than by anger).

In regard to hypotheses about neurological indicators of state-level suspicion, Watabe, Ban, and Yamamoto (2011) noted that it is difficult to identify specific decision-making processes
based upon differential brain activation, given the interconnectedness of the influence of brain regions. Nonetheless, we draw some tentative research propositions about the identification and measurement of IT-induced state-level suspicion.

It was noted earlier that one potential cause of state-level suspicion was a discrepancy between what one expects and what one observes. Such a discrepancy could lead to cognitive activity dedicated to searching for explanations of the discrepancy, causing increased uncertainty, decreased trust, and so on. Oliveira et al. (2007) conducted two EEG studies based on the assumption that the anterior cingulated cortex (ACC) in the brain is involved in error detection or evaluation of poor performance (see also Hajcak, McDonald, & Simons, 2004). Note that error recognition and performance evaluation are two representations of increased cognitive activity. Further, Oliveira et al. found that ACC activity occurs for unexpected rewards as well as increases in rewards. This converges with our “uncertainty” facet of suspicion (whether positive or negative). Oliveira et al. also suggested that the ACC acts as a system that signals an increased need for cognitive control, an updating of one’s internal models, and increased use of external information. These processes all directly reflect the increased active cognition facet of our definition of state-level suspicion. Thus, we suggest,

**Proposition III.2**: Increased levels of IT suspicion will be associated with increased anterior cingulate cortex activity.

Regarding emotion and the neurological literature, Hajcak et al. (2004) found that if an individual’s uncertainty was perceived to have potentially negative consequences (which reflects our focus on malintent in IT contexts), then anxiety would be increased due to the interaction of potential negativity and hyper-arousal (cognitive activity). This links with our suggestion that suspicion will be associated with increased anxiety (rather than, say, increased anger). However, one moderator to the aforementioned hypothesis might involve mood of the IT user. That is, Hajcak et al. (2004) found that negative affect or mood increased error-related negativity while reducing an error positivity measure. In other words, participants who were relatively high in negative affectivity noticed errors more strongly, but they were also less likely to process those errors cognitively and/or update any mental models about what was happening.

Stickney (2009; citing Schwartz, 2000) also noted that mood influences decision-making strategy; that is, a sad mood leads to more attention to detail and less reliance on preexisting strategies, whereas a positive mood is linked to greater use of heuristics. This implies that negative mood is more strongly related to suspicion than is positive mood, given the process of generating alternative explanations when suspicion. Thus, we suggest,

**Proposition III.3**: Individuals who are experiencing a negative mood (due to long-term trait or shorter-term situational reasons) are more likely to become suspicious than are individuals who are experiencing a positive mood (due to long-term trait or shorter-term situational reasons).

Going a step further, we note that other researchers (e.g., Marsland, Cohen, Rabin, & Manuck, 2006) stated that negative affect is associated with right-sided prefrontal brain activity and positive affect is associated with left-sided prefrontal activity. Interestingly, this converges with recent work in the management literature (Waldman, Balthazard, & Peterson, 2011) on the link between neuroscience and “inspirational leadership.” These authors noted that right frontal brain dysfunction is associated with difficulties in dealing with uncertainty. Given that uncertainty is a facet of suspicion, we might suggest that researchers also look for associations between right-sided prefrontal activity and increased levels of suspicion. However, another facet of suspicion is increased cognitive activity, which would increase activation in both sides of the brain. Hence we refrain from any specific propositions in this regard.

Researchers conducting “theory of mind” (Premack & Woodruff, 1978) studies have found
that the anterior paracingulate cortex is activated when participants are deciding whether or not to cooperate with, or trust, someone else (e.g., Gallagher & Frith, 2003). That is, higher brain activation in the anterior paracingulate cortex has been associated with the cognitively demanding process by which a person infers whether or not another person is trustworthy. Such activation is consistent with the findings of Dimoka (2010), Gefen et al. (2008), and Krueger et al. (2007). However, Dimoka also found that subjects who were given ambiguous information (i.e., subjects in the condition of no trusting information and no distrusting information) were also prone to increases in anterior paracingulate cortex activity. We suggest this is because the ambiguous information could breed suspicion, which, in turn, would lead to increased cognitive activity. This more general link between cognitive activity and anterior paracingulate cortex activity (whether via a decision process about trust or due to informational ambiguity) is consistent with the theory of mind. Thus, we suggest,

Proposition III.4: Increases in paracingulate cortex activity will be associated with (a) individuals in the process of making decisions about trust (or distrust) or (b) individuals who are receiving ambiguous information. Conversely, decreases in paracingulate cortex activity will be associated with individuals who have made decisions about trust (or distrust), because these individuals invoke cognitive structures and heuristics to quickly and efficiently process future information.

Regarding more distal outcomes, to the extent that state-level suspicion induces fear and anxiety, then suspicion will be associated with indicators of arousal such as increased blood pressure and electrodermal activity. If the suspicion, and associated stress, is sustained across time, then long-term outcomes might be increased susceptibility to colds or even increased likelihood of coronary heart disease (Friedman & Ulmer, 1984; Myers, 2010).

We also suggest that an increase in state-level suspicion might be associated with an increased ability to correctly detect deception. Consistent with our propositions about individual differences, it is further tentatively hypothesized that detection of deception is also enhanced by increased levels of individual cognitive capacity and/or creativity (because these individual differences factors enhance one’s ability to generate alternative possibilities and be suspicious). Note also that the foregoing suggestions assume that there is some deception to be detected. This leads to the following:

Exploratory Research Question III.1 (warranted suspicion): Are there appropriate levels of suspicion, and what is the nature of the relationship between levels of suspicion and successful detection of deception? Presumably, such a relationship is curvilinear (McCornack & Levine, 1990). That is, as suspicion increases, detection of suspicious events increases, but at a particular point generalized suspicion is unwarranted (Parasuraman & Riley, 1997, discuss the use, abuse, misuse of automated systems and the phrase unwarranted suspicion). If some individuals are predisposed to be suspicious (e.g., possibly even paranoid), then they are predisposed to spend cognitive energy generating alternative possibilities. Will this expenditure of cognitive resources then reduce their capacity to sometimes “see the obvious”? 

SUMMARY

One purpose of the current article was to present a multidisciplinary review of the (minimal) research on suspicion, with a specific focus on IT-induced state-level suspicion. The few existing articles from each of several social science domains were considered and inconsistencies/consistencies were noted. The integrative definition of suspicion has the key components of uncertainty, cognitive activity, and (mal)intent. In particular, we defined IT state-level suspicion as a person’s simultaneous state of cognitive activity, uncertainty, and perceived malintent about underlying information that is being electronically generated, collated, sent, analyzed, or implemented by an external agent.
A three-stage heuristic model of suspicion was developed, aided by other, related literatures regarding the concepts of trust (in general) and trust in automation (in particular). This led to several research propositions and exploratory questions about the concept of IT-induced state-level suspicion at each of the three stages. We believe that attention to a common definition of suspicion, and research on the propositions/questions in this article, will assist both academicians and practitioners who desire to embrace the notion of suspicion in technologically enhanced contexts.

Other efforts might readily follow beyond those listed in this review. For example, use of a theoretically based, uniform definition of state-level suspicion by social scientists in other disciplines could lead to a more reliable and valid measure of suspicion. Self-report items could be developed (particularly about the interactive facets of uncertainty, cognition, and intent), as well as physiological and neurological measures. To further assess construct validity, the self-report measures could be triangulated with neurological measures (paralleling Hancock et al.’s 2011 call for assessments of measurement convergence in the human-robot interaction literature).

Measurement items also might be categorized as assessing the ability to be suspicious (e.g., capacity to generate alternative explanations, to recognize relevant cues, or to accurately detect deception) or the motivation to be suspicious (i.e., attentiveness to cues across time). These two types of criteria match the usual “can do” and “will do” distinction in studies on job performance in management and applied psychology (e.g., Borman, White, Pulakos, & Oppler, 1991).

Given this uniformly accepted definition or measure of suspicion, the nomological net of correlates discussed earlier could be empirically investigated to further enhance the understanding of suspicion. Several possible correlates were noted in our discussion of Stage II (e.g., cognitive capacity, creativity, need for cognition, disposition to trust, cynicism). As suggested by others (Bond & Lee, 2005; Levine & McCormack, 1991), it is also useful to distinguish between trait and state suspicion. That is, it may be that some individuals are predisposed to be suspicious (as with the suggested correlate faith in humanity).

On the other hand, our focus has been on suspicion as a transient state that is dependent on IT-induced situational factors. For example, we noted a variety of system or machine characteristics that could influence levels of state suspicion. Benbasat, Gefen, and Pavlou (2008) noted a variety of moderators of user trust in IT systems, which also might apply to research on IT suspicion (e.g., moderators such as gender and culture). Indeed, one of the primary dimensions of globally based culture is labeled uncertainty avoidance (Hofstede & Bond, 1988, p. 11), which involves relative discomfort in unstructured, unknown, or surprising situations. Thus, individuals from such cultures may be less likely to engage in suspicious behaviors, as they have a desire to avoid the uncertainty component in our definition of suspicion.

Further, if suspicion can indeed be influenced, and if suspicion is both an ability (can do) and attitude (will do), suspicion might be trained via programs involving attitude formation and training. Attitudes are considered to have three components—cognitive, affective, and behavioral intent (e.g., Griffin & Moorhead, 2010)—and the first two attitudinal components mirror the active cognition facet of suspicion and the arousal/anxiety outcomes discussed earlier.

Suspicion training also might be informed by the IT literature. For example, it has been suggested that operator performance is readily influenced or enhanced by requiring the operator to occasionally shift from automated to manual modes (e.g., Chen, Barnes, & Harper-Sciarini, 2010; Lee & See, 2004; Parasuraman & Manzey, 2010, citing work by Gopher and by Metzger). Therefore, the active cognition component of suspicion may be enhanced by having users occasionally switch modes (of information acquisition or responding) rather than succumb to complacency via continued use of a single channel.

As another example, the U.S. Army has adopted a program, based on positive psychology, that builds soldier resilience by training those individuals to avoid worst-case-scenario thinking (see Cornum, Matthews, & Seligman,
The definition of state suspicion is the simultaneous occurrence of (a) uncertainty, (b) increased cognitive processing (e.g., generation of alternative explanations for perceived discrepancies), and (c) perceptions of malintent.

The potential for research on suspicion (and IT suspicion) as a psychological construct: Interim report (Air Force Research Laboratory, 711th Human Performance Wing, ICER Contract No. FA8650-09-D-6939). Dayton, OH: Wright-Patterson Air Force Base.


ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. Air Force Office of Scientific Research (AFOSR). Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the AFOSR. We thank the action editor, two reviewers, and Heather Odle-Dusseau for helpful comments on an earlier draft of this article.

KEY POINTS

- There is little in the human factors literature on the important topic of suspicion.
- We develop a definition and integrative model of IT-induced state-level suspicion based upon work in communication, psychology, human factors, management, marketing, information technology, and neuropsychology.
- The definition of state suspicion is the simultaneous occurrence of (a) uncertainty, (b) increased cognitive processing (e.g., generation of alternative explanations for perceived discrepancies), and (c) perceptions of malintent.
- Research propositions within IT contexts are derived at each of the three stages in our model of suspicion.

REFERENCES


In sum, the potential for research on suspicion, and IT state suspicion, is vast, and this work has important implications. We hope the integrative review, definition, three-stage model, and propositions presented in this paper assist future researchers in this domain. We look forward to the results that such research will bring.


Philip Bobko is professor of management and psychology at Gettysburg College. He has served as editor of the *Journal of Applied Psychology* and associate editor of the *Academy of Management Journal*. He received his PhD in economic and social statistics from Cornell University.

Alex J. Barelka is a leader in the Trust and Organization Science Team at the Air Force 711th Human Performance Wing. He has published in the *Journal of Applied Psychology, Human Factors*, and *Journal of Computer Information Systems*. He received his PhD in management from Michigan State University in 2007.

Leanne M. Hirshfield is an associate research professor in the Newhouse School of Public Communications at Syracuse University. She received her PhD in computer science from Tufts University.

*Date received: August 4, 2012  
Date accepted: June 11, 2013*