IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 18, 2019, accepted February 8, 2019, date of publication February 25, 2019, date of current version April 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2901258

Operator Suspicion and Human-Machine Team Performance Under Mission Scenarios of Unmanned Ground Vehicle Operation

CHRIS GAY[1], BARRY HOROWITZ[2], JOHN J. ELSHAW[1], PHILIP BOBKO[3], AND INKI KIM[2], (Member, IEEE)

[1]Department of Systems Engineering and Management, Air Force Institute of Technology, Dayton, OH 45433-7765, USA
[2]Department of Systems and Information Engineering, University of Virginia, Charlottesville, VA 22904-4747, USA
[3]Management and Psychology, Gettysburg College, Gettysburg, PA 17325, USA

Corresponding author: Inki Kim (ik3r@virginia.edu)

This work was supported in part by the Center for Complex Systems and Enterprises, Stevens Institute of Technology, and in part by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004. SERC is a federally funded University Affiliated Research Center managed by the Stevens Institute of Technology.

ABSTRACT Emergent cyber-attack threats against cyber-physical systems can create potentially catastrophic impacts. The operators must intervene at the right moment when suspected attacks occur, without over-reliance on systems to detect the cyber-attacks. However, military operators are normally trained to trust, rather than suspect systems. We applied suspicion theory to explore how operators detect and respond to cyber-attacks against an unmanned ground vehicle (UGV) system in the operational context of a human–machine team (HMT). We investigated the relationships between the operator suspicion and HMT performance by conducting human-in-the-loop experiments on eight mission scenarios with 32 air-force officers. The experiment yielded a significant, negative relationship between operator suspicion and HMT performance (quantified both in terms of the desirability of decision response and the time to respond). Notably, operator suspicion increased with the combined effects of cyber-attacks and a sentinel alert but not with the alert alone. This finding was particularly meaningful for ‘‘false-negative’’ scenarios, in which no sentinel alert was sent despite cyber-attacks having occurred. Although the operators did not receive an alert, the operators grew more suspicious, seeking more information; it took longer for the operators to respond, and their decision responses were highly divergent (17.2% came with less-desirable responses, and 21.9% were considered instances of over-reliance). In contrast, in ‘‘false-positive’’ scenarios, 95.3% of the operator responses were highly desirable. This experiment has implications for the role of a sentinel alert in engineering trustworthy HMT systems so that the operators can quickly transition through state-suspicion to the most desirable decision.

INDEX TERMS Suspicion, trust, human machine team, cyber security, human-in-the-loop simulation, unmanned ground vehicle control.

I. INTRODUCTION

A considerable effort is ongoing to prevent, detect and mitigate cyber-attacks on the Department of Defense networks and information technology (IT) systems; in contrast, the effort to address these concerns in cyber-physical system (CPS), such as unmanned vehicle systems, pales in comparison. These systems represent an intrinsic vulnerability and allow adversaries to attempt cyber-attacks with the malicious intention of undermining military assets. As an example, Iranian cyber capabilities were believed to have forced down the Central Intelligence Agency operated RQ-170 Sentinel drone while operating near the Iranian border in 2011 [1], causing concern over the potential compromise of highly sensitive surveillance capabilities. This incident sparked much research directed towards the hardware and software security of unmanned vehicle systems [2], [3]. However, research addressing the human dimensions of

The associate editor coordinating the review of this manuscript and approving it for publication was Miltiadis Lytras.

cyber-attack detection and response in the mission operation context remains sparse and represents an emergent area of research needed to fully address cyber-attacks against CPS.

Our research took an operator-centric approach towards exploring the human dimensions of cyber-attack detection and responses through a scenario-based, human-in-the-loop experiment with Air Force personnel as operators of an unmanned vehicle system in a military context. In prior work, we took a systems-oriented approach to the problem by considering the interaction of a Human-Machine Team (HMT) [4], [5] responding to cyber-attacks and defining a framework of performance measurement [6].

In this work, HMT is defined as a team of an operator and Sentinel, an automated cyber-attack detection aid. For machine design, the operators' biases associated with suspicion in their responses to cyber-attacks shed light on the development of an adaptive sentinel. For human operators, the findings on the relationship between HMT performance and level of suspicion have implications for the selection, evaluation and training of appropriate personnel.

II. BACKGROUND

A challenge in designing for high-performance HMT is a lack of theory to help understand how humans interact with machines in work contexts. A recent paradigm in human-machine automation considers autonomy as a variable, rather than a fixed parameter, which can be distributed between human and artificial agents to achieve an optimal performance at work [7]. An ultimate vision for human-machine teamwork is to "race with machines" [8], not against ones, by continuously redefining human roles under new work processes. The promise of complementary engagement of human and machine abilities for enhanced performance has seen some positive examples [9], [10]. Yet, it is difficult to fully accomplish this vision without knowing the constraints of the human, the machine, and the environment [11].

In military operations, mission complexity is outpacing the ability to manage disruptions, which calls for systemic approaches that span technology, human, and mission space [12]. At a minimum, any framework that addresses this complexity should enable the evaluation of human-machine interactions with regard to the nature of problem and solution sets [13], [14], under the situational constraints of mission context. The traditional framework of Level of Automation (LOA) and its alternatives [15]–[17], are confined to the concept of function allocation, not reflecting situational constraints.

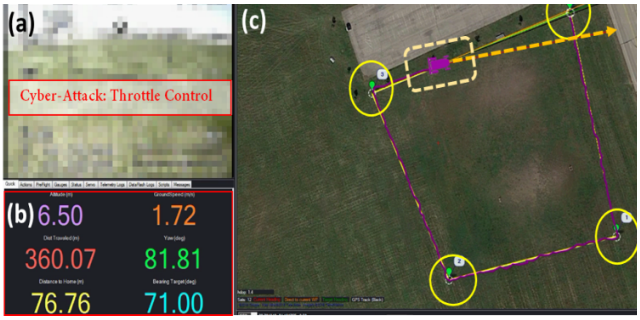
So far, many unmanned systems [18] have attained assurance by counting on human supervision as the last resort. Some systems attempt to augment human cognitive abilities on particular tasks, such as spatial detection [19] and path planning [20]. The cognitive support in HMT [4], [21], [22], focuses on team cognition and mental workload. In particular, human-machine collaboration for emergency management has gained attention, with a focus on risk management and resiliency [23], [24]. Under emergency situations, HMTs are forced to make decisions within tight time schedules often with incomplete information, while the new situational complexity is likely to overload team cognitive resources [25]. In military unmanned systems, a failure to first-respond to the emergency situations can result in catastrophic damages, and there are growing concerns over the potential of cyber threats to impede the timely responses [26].

There are methods proposed to help analyze and guide cognitive responses of human supervisor under cyberattacks (see [27], for instance), but they do not fully consider the dynamic interdependence of human, machine, and situational context. The Instance-based Learning (IBL) model for cyber situation awareness [28] predicted security analysts' recognition of cyberattacks based on the situational attributes and on their similarity to the past instances (to be retrieved from memory). Another example of analyzing cyber situation awareness in [29], proposed a distribution-based simulation model to identify cyber-behaviors and their cognitive aspects based on browser log data. In a hybrid approach, the work in [30] proposed a decision-support scheme to assist in response selection against cyber threats by combining qualitative expert assessment, event history, and multi-criteria decision analysis [31]. Although these works presented formal models and methods to represent performance in cognitive aspects, they focused exclusively on humans, rather than on the dynamics of the human-machine team.

The dynamics associated with the analysis of HMT performance can be internal (i.e., between human and machine), or external (i.e., situation-specific relations between the team and work-related factors). Regarding internal dynamics, the concept of "trust" is key to successful emergency responses – i.e., how trust is formed, developed and confirmed with the automated agents [32]. The literature on operator trust abounds [33]–[36], including when the autonomous systems are under potential cyber-attacks [37]. A wide array of factors has been identified that influence the level of trust in human-automation interaction [38]. Not only formation, but the confirmation of trust becomes critical particularly when an unmanned system is under cyberattack. To the contrary, relatively little attention has been paid to understand the external dynamics of the HMT. Such investigations are not straightforward because it is not always feasible to keep the situational factors transparent to the supervisor or the machine [39]. For example, in which task-related conditions can the HMT performance be weakened (or strengthened)? Are there particular cognitive states of the human supervisor that can help improve HMT performance? What are the effective ways for the machine to support the supervisor under cyberattacks?

This paper determined the construct of suspicion to be particularly useful for investigating HMT performance in response to cyberattacks. In recent work, the theory of suspicion [40] defines state-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''. This work also describes the sequential structure of state-suspicion development across three stages.

Stage 1 refers to perceptual cues and indications from the task environment that can trigger suspicious states in the mind of the operators. For example, missing information, patterns of negative discrepancy, or other system and interface characteristics can serve to provoke different levels of suspicion. In UGV control, an operator and Sentinel collaborate in a team for detection and response to cyber-attacks, and the Sentinel alert messages, or their lack, on a control interface can serve as stage-1 cues to initiate operator suspicion. Therefore, this research manipulated the sentinel alert messages to stimulate state suspicion. For example, the Sentinel alert message popped up in the mission video window that read ''Cyber-attack: Throttle Control,'' and it remained visible for thirty seconds, see Figure 1. Not only the display of alert, but the lack of alert when the vehicle was maneuvering abnormally could also trigger suspicion from the interface.



Altitude (m) 6.50
GroundSpeed (m/s) 1.72
Dist Traveled (m) 360.07
Yaw (deg) 81.81
Distance to Home (m) 76.76
Bearing Target (deg) 71.00

FIGURE 1. **A Mission Scenario on a UGV Control Interface. (a) Ego-Centric view of the UGV with a sentinel alert, (b) numerical indicators of the UGV control parameters, (c) Bird's-Eye view with way-points (Circled) and the UGV's location and direction (dotted lines).**

Stage 2 of the suspicion model identifies individual levels of trust, distrust, training and other personal traits that can affect state-level suspicion [41], [42]. Especially, an operator's trait-level attributes, including creativity, cognitive demand and capacity, and propensity to trust [43], can form an internal condition to the arousal of state-suspicion [40]. This research incorporated a set of pre-test surveys prior to the experiment about operator self-ratings of intelligence scores, creativity, general attitude towards complex problems, and propensity to trust.

Finally, stage 3 refers to behavioral, cognitive and emotional outcomes of becoming suspicious. In particular, the State-Suspicion Index (SSI) [40] has been developed to quantify the level of suspicion through a 20-item questionnaire that assesses the suspicion components of uncertainty, mal-intent, and cognitive load, as well as overall suspicion. To reflect the operational context of UGV missions, the original SSI was adapted to a 13-item questionnaire in collaboration with one of those authors.

III. METHODS

This research primarily revolves around the relationship between level of operator suspicion and human-machine team (HMT) performance in the mission operation context of an unmanned ground vehicle (UGV). The definition of key variables and their measurements, and experimental process are described in this section.

A. RESEARCH HYPOTHESES, VARIABLES, AND MEASUREMENTS

This research primarily revolves around the relationship between level of operator suspicion and human-machine team (HMT) performance in the mission operation context of an unmanned ground vehicle (UGV). To answer how suspicion effects HMT performance in a human-in-the-loop simulation, this research paired a UGV operator with a sentinel for automated cyber-attack detection. Guided by suspicion theory, a set of visual cues in the sentinel alarm and control environment was simulated for anomalous system events under different mission scenarios. On completing each mission scenario, HMT performance, as well as suspicion level, was quantified. HMT performance was evaluated on the two general criteria of speed and accuracy [44], for the detection and selection of responses to suspected cyber-attacks. To elaborate on the research question, the following hypotheses were set.

- H_1: Sentinel alert has significant effects on operator suspicion.
- H_2: Operator suspicion is positively related to HMT performance.
- H_3: Cyber-attack (yes/no)/Sentinel alert (alert/no alert) combinations have significant effects on operator suspicion.
- H_4: Operator suspicion is positively related to operator response time (i.e. response times are delayed when operators are more suspicious).

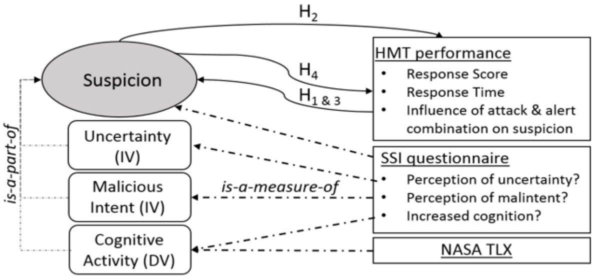


FIGURE 2. **Overview of experimental variables, relationships among them, and methods of measurement.**

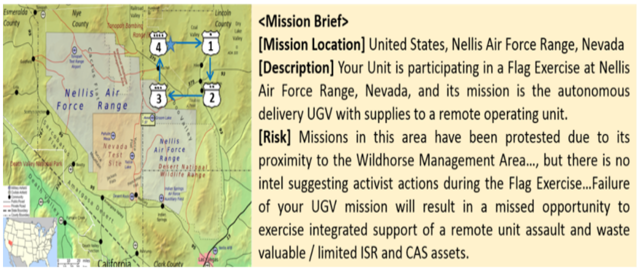
Figure 2 depicts how these four hypotheses associate the operator's suspicion with the responses to cyber-attacks on unmanned systems. Based on suspicion theory, operator suspicion is presumed to be a latent variable that has three components, ''Uncertainty'', ''Malicious Intent'', and ''Cognitive Activity.'' The experimental levels, either high or low, of both uncertainty and malicious intent were manipulated as independent variables (IV) through each mission scenario, while cognitive activity was measured as a dependent variable (DV) at the end of each mission run. For the estimation of cognitive activity, NASA-TLX [45], [46] and the related items in the State-Suspicion Index (SSI) questionnaire were used. The two-levels for each one of the IVs were verified based on the responses to the corresponding items in the SSI questionnaire, which helped confirm if different mission scenarios effectively set different levels of perceptions as intended. The 13-item SSI questionnaire determined the overall level of suspicion (by linear combination of its components).

The performance measures of response time and score were recorded while the mission videos dynamically played back anomalous system events, including cyber-attacks and sentinel alert messages. The time to respond to such events was recorded using an interactive polling software (TurningPoint, TurningTechnologies, Ltd.) during the experiment, and the performance score was determined post-experiment based on rubrics. Each mission scenario has its own unique score rubric defined by subject matter experts. The operator's response selections from a given set of decision trees were logged in the software and were then evaluated against the rubric. Furthermore, the four-way combinations of cyber-attacks (attacks vs. no attacks) and sentinel alert messages (alert vs. no alert) enabled us to analyze operator suspicion under different circumstances.

B. EXPERIMENTAL PROCEDURES, DESIGN, AND SETTING

The human-in-the-loop experiments were designed and conducted in three phases. In phase 1, we obtained consent from thirty-two military operators (IRB: FWR20160115H) and collected personal information, including demographic and personality-related questionnaires. Phase 2 familiarized participants with the experimental tasks through instruction and demonstrations, so that an acceptable level of fluency was ensured in the operational context. In phase 3, participants were presented, in a random order, a series of eight mission scenarios, each with a pair of mission briefing and mission videos. Once the mission briefing was done, the participant responded to events on the mission videos that occurred during each mission scenario while response selection and response times were recorded simultaneously. On completion of each mission scenario, participants' perceptions of uncertainty, malicious intent, and cognitive workload during the mission were obtained via the NASA TLX and SSI questionnaires.

To the operator, a mission scenario was characterized by the combination of mission briefings, illustrated in Figure 3, and mission videos. The mission briefings described mission type, mission context, and descriptive profiles for the operation of the unmanned ground vehicle system (UGVS). The mission type was either training or operational missions for transport and re-supply. The mission context was set in the U.S. or Middle Eastern locations, with the corresponding estimated frequencies of cyber-attacks in the past. For the machine-side, a mission profile configured the UGV behaviors: when a profile was deployed, the UGVS autonomously ran it and generated mission views for playback to use in the simulation experiments. Overall, both verbal and visual elements of mission scenarios were constructed to indirectly manipulate the operator's state-suspicion by forming the two independent variables (IVs), "uncertainty" and "malicious intent", into a two-level full-factorial design.



<Mission Brief>

[Mission Location] United States, Nellis Air Force Range, Nevada

[Description] Your Unit is participating in a Flag Exercise at Nellis Air Force Range, Nevada, and its mission is the autonomous delivery UGV with supplies to a remote operating unit.

[Risk] Missions in this area have been protested due to its proximity to the Wildhorse Management Area..., but there is no intel suggesting activist actions during the Flag Exercise...Failure of your UGV mission will result in a missed opportunity to exercise integrated support of a remote unit assault and waste valuable / limited ISR and CAS assets.

FIGURE 3. Illustration of a mission briefing (part).

After being oriented to the mission briefing, the participants were tasked to record the UGV speed every thirty seconds while monitoring the mission video as well as instrument readouts for anomalous events from the UGV mission. On detecting anomalous events, the participants were instructed to select the most appropriate response from a decision tree that was provided as a guide to standardize the range of possible operator responses (see Table 1). These tasks were closely aligned with typical unmanned vehicle system operator tasks. At the conclusion of each mission scenario, the operator completed two questionnaires: (i) the NASA TLX questionnaire which quantifies the operator's self-assessment of cognitive workload on six dimensions, with each dimension rated on a 0-100 scale, and (ii) the 13-item SSI questionnaire which was developed specifically for this research and evaluated (on a 7-point Likert scale) the operator's perception of uncertainty, malicious intent, cognitive activation, and overall suspicion. The 13 items measuring suspicion were then aggregated to form an overall quantitative measure of operator suspicion. Cronbach's alpha [47] for the 13 items was .88, indicating acceptable internal consistency of the measure. Participants were thirty-two Air Force officers from the Air Force Institute of Technology (AFIT), with each experiment taking 2- 2 1/2 hours to complete. Since many current operations associated with unmanned vehicle missions occur in an office environment, the experimental took place in such a space.

IV. RESULTS

The experiment yielded significant outcomes on the relationship between operator suspicion and HMT performance. The overall level of suspicion derived from the 13-item SSI questionnaire had a significant ($p < 0.001$) Pearson-correlation with the response score ($\rho = -0.251$), as well as with the response time ($\rho = 0.379$). As was expected with the suspicion theory, the subgroups of the SSI questionnaire items that correspond to perception of uncertainty, malicious intent, and cognitive activation also showed a strong, significant correlation with overall suspicion ($p < 0.001$). Correlations were estimated to be $\rho = 0.803$, $\rho = 0.905$, and $\rho = 0.828$, respectively. In addition, there were predictable relationships among the HMT performance metrics. The response score was negatively correlated with response time ($\rho = -0.225$), as well as with the standard deviation of its own score ($\rho = -0.354$), implying that less-desirable decision responses tend to accompany slow and inconsistent responses.

Contrary to H_1, which proposed Sentinel alerts are related to operator suspicion, the result of the one-way ANOVA was not significant ($F_1, 254 = 0.688$, $p = 0.408$); hence Sentinel alerts alone did not create operator suspicion. The variability within each group of the sentinel alert being activated versus not activated, outweighed that of the between-group ($MSE_{Within-group} = 1.009$, $MSE_{Between-group} = 0.694$). It contrasts, for the factor of cyber-attack (or not), a second one-way ANOVA showed a significantly different level of suspicion ($F_1, 254 = 18.393$, $p < 0.001$); i.e., a higher level of suspicion was observed when attacks occurred. These results that Sentinel alerts are not an independent factor of suspicion despite their visual saliency on a display, while cyber-attacks did significantly arouse suspicion, imply a complicated cognitive structure of judgment based on uncertainty of perceptual information [48], [49]. Of particular statistical concern with this uncertainty, is a shared-variance structure of an individual operator's suspicion, which might be determined by combined effects of the Sentinel alert and cyber-attack scenarios.

To resolve these combined effects, a Hierarchical Linear Model (HLM) was applied. The HLM is capable of accounting for the shared variance structure in a nested data with hierarchical levels of variables, by using a complex form of Ordinary Least Squares (OLS) regressions [50]. This HLM method can effectively compensate for the known risks [51]; a risk of ignoring the between-scenario effects on suspicion (as was seen in the first one-way ANOVA of the previous paragraph), as well as ignoring the individual propensity to trust the Sentinel alert (as seen in the second one-way ANOVA of the previous paragraph).

In general, the final outcome of HLM takes on a form of simple regression, where a dependent variable Y_{ij} is predicted by using an i^{th}-level variable X_{ij} that is nested within a higher-level variable, j.

$$Yij = \beta_{0j} + \beta_{1j}X_{ij} + \varepsilon_{ij} \tag{1}$$

In HLM, this low-level model (1) further incorporates the higher-level models of equations (2) and (3) below, for each of the coefficients, β_{0j} and β_{1j}, in terms of the interim variable Qj of the j^{th}-level variable, and the random effects, U_{0j} and U_{1j}, that are adjusted for Q_j. The statistical significance of β_{1j} can be tested to determine if the combined levels i and j influence the dependent variable Y_{ij}.

$$\beta_{0j} = \gamma_{00} + \gamma_{01}Q_j + U_{0j} \tag{2}$$

$$\beta_{1j} = \gamma^{10} + \gamma_{11}Q_j + U_{1j} \tag{3}$$

Finally, the overall model in (4) incorporates both the i^{th}-level and the j^{th}-level predictors X_{ij} and Q_j, respectively, by combining (2) and (3) into (1).

$$Y_{ij} = \gamma_{00} + \gamma_{10}X_{ij} + \gamma_{01}Q_j + \gamma_{11}Q_jX_{ij} + U_{1j}X_{ij} + U_{0j} + \varepsilon_{ij} \tag{4}$$

In order to apply HLM, the dependent variables as summarized in Figure 2 for state-suspicion, HMT performance, and cognitive workload, respectively, were structured for each combination of the level-i of Sentinel alert ($i = 0$ if no alert; $i = 1$ if an alert message was shown on a display) and the level j of cyber-attacks ($j = 0$ if no attacks; $j = 1$ if any attacks occurred in an experimental scenario). Table 1 summarizes the mean and the standard deviation for each combination of the nested levels. Such orthogonal dichotomies of True/False (of cyber-attacks) and Positive/Negative (of sentinel alarm) on a 2-by-2 contingency table allows us to further analyze the experimental results around the classic framework of signal detection theory [52].

TABLE 1. Descriptive statistics for cyber-attack/ sentinel alert combinations (mean± SD).

Dependence Variable	**(a) TP** Attack Yes / Alert Yes	**(b) TN** Attack No / Alert No	**(c) FP** Attack No / Alert Yes	**(d) FN** Attack Yes/ Alert No
Suspicion; (7-Likert)	4.38± 0.97	3.97± 0.96	3.90± 0.96	4.52± 1.00
Score; (0-100)	90.8± 18.1	94.8±12.1	92.7±15.7	81.2±27.7
Time (Sec)	14.91± 16.45	1.00± 2.56	4.61± 3.69	13.48± 12.79
NASA-TLX; (Rating 0-25)	22.1±14.1	16.6± 11.4	16.2± 9.8	23.5± 13.8

Since cyber-attacks are by nature malicious events and require consideration of multiple solutions for the observed behavior, H_2 hypothesized that operator suspicion is positively related with HMT performance, suggesting a suspicious operator would score better on the tasks. This hypothesis was the opposite of the experimental results. The linear coefficient of the HLM analysis was significant when modeled after (1) ($\beta_{10} = -5.63, p < 0.001$), and the direction of the relationship was negative, meaning increased operator suspicion had a significantly negative relationship to HMT performance as depicted in Figure 5.

Additionally, H_4 proposed operator suspicion is positively related to operator task response time, which meant higher suspicion is associated with a longer task response time. The linear coefficient of the HLM analysis supported H_4; i.e., the relationship is statistically significant and in a positive direction ($\beta_{10} = 6.95, p < 0.001$). This linear relationship is depicted in Figure 4.

Finally, the four cyber-attack and Sentinel alert combinations were tested in the experiment and analyzed by using the HLM as summarized in Table 2. The two combinations without cyber-attacks, both (b) True Negative (TN) and (c) False Positive (FP), had a significant ($p < 0.05$) negative impact

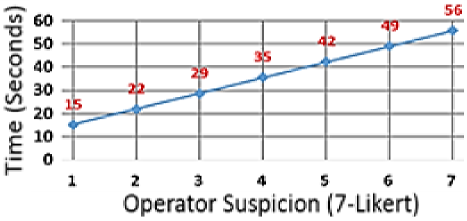


FIGURE 4. Time as a function of operator suspicion.

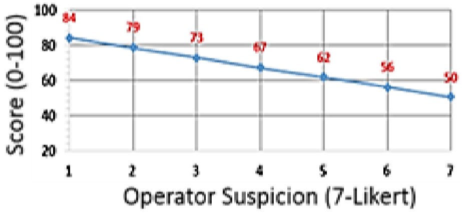


FIGURE 5. Performance score as a function of operator suspicion.

TABLE 2. Combined effects on operator suspicion.

Sentinel Alert	Cyber-Attacks: Yes	Cyber-Attacks: No
Yes	**(a) True Positive (TP)** Increases suspicion ↑ ($\beta_{10} = +0.255$, $p = 0.047$)	**(c) False Positive (FP)** Decreases suspicion ↓ ($\beta_{10} = -0.394$, $p = 0.002$)
No	**(d) False Negative (FN)** Increases suspicion ↑ ($\beta_{10} = +0.440$, $p = 0.001$)	**(b) True Negative (TN)** Decreases suspicion ↓ ($\beta_{10} = -0.301$, $p = 0.019$)

TABLE 3. Frequency analysis of cyber-attack/sentinel alert combinations.

	(a) True Positive	(b) True Negative	(c) False Positive	(d) False Negative
Decision Responses on a Decision Tree				
0- No response	-	51	1	1
1- Continue Mission	2	4	46	6
2- Take action; Sentinel fixes the problem; continue	54	5	11	14
3- Take action; Operator fixes the problem; continue	5	4	6	38
4- Take action; Call backup; continue	-	-	-	2
5- Abort; recovery; backup	2	-	-	2
6- Abort; recovery; no backup	1	-	-	1
Subtotal (N)	64	64	64	64
Suspicion (SSI Total range of 1-7) *Higher indicates more suspicious				
Low (SSI Total: 1 – 3)	5	10	12	1
Medium (SSI Total: 3 – 5)	40	43	41	40
High (SSI Total: 5 – 7)	19	11	11	23
Subtotal (N)	64	64	64	64
HMT Performance (Score range 0-100) *Evaluated by desirability				
Low (Score: 0 – 50)	3	-	1	11
Medium (Score: 50 – 75)	4	5	2	3
High (Score: 75 – 100)	57	59	61	50
Subtotal (N)	64	64	64	64
Response Time (Time range 1-60 sec)				
Fast (Time: 0 – 5)	24	60	43	19
Medium (Time: 5 – 10)	16	2	15	18
Slow (Time: 10 – 60)	24	2	6	27
Subtotal (N)	64	64	64	64

on operator suspicion, meaning that operator suspicion was lowered on both cases. In contrast, the two combinations containing cyber-attacks, (a) True Positive (TP) and (d) False Negative (FN), had a significantly ($p < 0.05$) positive impact on operator suspicion by increasing operator suspicion. These results are consistent with the finding for H_1 that Sentinel alerts alone do not always create suspicion.

The combined effects of Table 2 warrant further discussion. Table 3 presents a frequency analysis of HMT actions for each combination (a)-(d) in terms of the four dependent variables: operator decision selections, suspicion, HMT performance score evaluated in terms of the desirability of the decision response to a given mission scenario, and response time. As previously noted, all operators in the experiment responded to suspicious events by referring to a pre-defined tree of decision responses, and the frequencies associated with those response options are summarized in the first section of Table 3. The HMT actions in the combinations of (a) True Positive (TP) and (b) True Negative (TN) are predictable based on the findings of other hypotheses and will not require further discussion. The more interesting behaviors are from situations (c) False Positive (FP) that represent scenarios in which no cyber-attacks occurred, but the Sentinel sent an alert to the operator anyway, and (d) False Negative (FN) that represent scenarios in which cyber-attacks occurred, but the Sentinel failed to send an alert.

In FP scenarios, 71.8% of responses (i.e., 46 out of 64) were judged desirable for the mission context by subject matter experts: when the operators received the Sentinel alert, most of them collected information available from the system to tell if a cyber-attack was in effect and decided to over-ride the Sentinel alert by continuing the mission without taking additional action. This quick search-and-override decision resulted in a relatively higher HMT performance, and faster response times compared with other combinations as summarized in Table 3. Furthermore, there were no “call for backup” or “abort” actions, which may have come with high cost in mission operation. Overall, these responses in False Positive (FP) scenarios are generally desirable.

In contrast, the HMT actions in False Negative (FN) scenarios were considerably less desirable to the mission context. Regardless of the fact that the operators did not receive a Sentinel alert to prompt information search, they grew more suspicious when cyber-attacks occurred, and it took longer for them to respond, yielding lower HMT performance scores. Of 64 responses, 38 chose to develop their own solutions, 2 called for backup, and 14 even allowed the Sentinel to act, which can be considered instances of *over-reliance* on the Sentinel although it did not detect the attack [53]. Another issue that emerged in this operational context is the frequency of missed detections. The operators completely missed the cyber-attack 7 times (the responses with codes 0 or 1). Overall, the HMT behaviors around the FN scenarios were potentially more damaging to mission outcomes.

V. DISCUSSIONS AND CONCLUSION

Sentinel Alert, Suspicion, and Information-Seeking Behavior

The analysis of recent cyberattacks on cyber-physical infrastructures reveals that adversaries promptly adapt their attack strategies to mitigation actions [54]. This makes early detection and recognition of incoming cyberattacks even more critical to effective mitigation. So far, much research has focused on engineering cyberattack detection aids [55], while not necessarily considering their cognitive effects on the human or human-machine collaboration in mission contexts.

The finding that Sentinel alerts did not necessarily arouse operator suspicion (i.e., rejection of H_1) has implications for vigilant human-machine integration. Perhaps, rather than the Sentinel alert, visual cues of unexpected system behaviors in mission environment are more likely to determine suspicion.

In fact, our finding could be related to the perceived risk that might have been triggered by a Sentinel alert. In the decision science literature [56]–[58], a positive correlation of perceived risk and information-seeking behavior is widely observed in decision under uncertainty. For instance, when a consumer has to choose a service that does not allow feature-by-feature comparison, information-seeking behavior is a common strategy to reduce perceived risk. In particular, information search triggered by perceived risk is more likely to be thorough if decision-makers have less knowledge about their choice and its consequences [59], leading to increased search time. The operators not knowing the true system states on cyberattacks, Sentinel alert could have triggered perceived risk, which then initiated wider information search to resolve suspicion.

In this regard, operator suspicion is a state of suspended or postponed decision-making, and it significantly lengthened mission time as observed both in (a) TP and (d) FN of Table 1. This strong linear relationship of suspicion and time is depicted in Figure 4. The negative correlation of suspicion and performance score also suggests it is wider information-seeking behavior, rather than more elaborated response selection, which actually lengthened the mission time. If the increased mission times were due to more effort investigated into response selection, the operator would have obtained a better score.

Yet, one cannot rule out the possibility that the scenarios which evoked suspicion were inherently more difficult to respond to, and thus increased mission time. Besides, causal relations among alert, state-suspicion and information-seeking behavior are not fully established. The current results do not allow us to conclude how state-suspicion is aroused, modulated, and resolved in the context of HMT collaboration.

VI. CONCLUSION

The novel application of suspicion theory to UGV operations in a military context demonstrated the potential of that theory – particularly in relation to understanding the operation of a human-machine (sentinel) team. We suggest that operator suspicion needs to be managed in order for a HMT to achieve the best results in regard to detection of cyber-attacks, and subsequent responses, when unmanned vehicle systems incur those cyber-attacks. This research provides an understanding of suspicion effects on HMT performance and offers insights about moving quickly (or not) from a position of state-suspicion to making a decision.

A Sentinel alert on cyber-attack symbolizes the roles that automation can play in responding to cyberattacks, and sheds lights on how HMT design can help exploit operator suspicion. As systems developers consider the balance of false-positive and false-negative errors in the design of cyber-attack detection aids, the results of this experiment suggest erring on the side of false positives as more desirable. In addition, the Sentinel design that was used in the experiment did not provide operators with any indication of the need for a more or less immediate response to the attack that was detected. Providing such information could potentially help operators in managing the undesirable delays that were experienced during the experiments. Satisfying such a need could be difficult as it places requirements on the Sentinel to develop more detailed assessments of the attacks that it detects and may also require access to additional data sources that would serve this purpose.

ACKNOWLEDGEMENT

Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Department of Defense.

REFERENCES

[1] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks—An approach to the risk assessment," in *Proc. 5th Int. Conf. Cyber Conflict (CYCON)*, Jun. 2013, pp. 1–23.

[2] B. M. Horowitz and K. M. Pierce, "The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems," *Syst. Eng.*, vol. 16, no. 4, pp. 401–412, 2013.

[3] R. A. Jones and B. M. Horowitz, "A system-aware cyber security architecture," *Syst. Eng.*, vol. 15, no. 2, pp. 225–240, 2012.

[4] M. A. Neerincx *et al.*, "The mission execution crew assistant: Improving human-machine team resilience for long duration missions," in *Proc. 59th Int. Astron. Congr. (IAC)*, Sep. 2008, pp. 7910–7921.

[5] J. M. Hoc, "From human-machine interaction to human-machine cooperation," *Ergonomics*, vol. 43, no. 7, pp. 833–843, Jul. 2000.

[6] C. Gay, B. Horowitz, J. Elshaw, P. Bobko, and I. Kim, "Operator suspicion and decision responses to cyber-attacks on unmanned ground vehicle systems," *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 61, no. 1, pp. 226–230, Sep. 2017.

[7] S. A. Mostafa, M. S. Ahmad, and A. Mustapha, "Adjustable autonomy: A systematic literature review," *Artif. Intell. Rev.*. vol. 51, no. 2, pp. 149–186, 2019.

[8] K. Kelly, *The Inevitable: Understanding the 12 Technological Forces that Will Shape our Future*. New York City, NY: Viking Press, 2017.

[9] A. Birk and M. Pfingsthorn, "A hmi supporting adjustable autonomy of rescue robots," in *Robot Soccer World Cup*. Berlin, Heidelberg: Springer, 2005, pp. 255–266.

[10] K. Petersen and O. V. Stryk, "Towards a general communication concept for human supervision of autonomous robot teams," in *Proc. 4th Int. Conf. Adv. Comput.-Hum. Interact. (ACHI)*, 2011, pp. 228–235.

[11] N. B. Sarter, D. D. Woods, and C. E. Billings, "Automation surprises," in *Handbook of Human Factors Ergonomics*, 2nd ed. New York, NY, USA: Wiley, 1997, pp. 1926–1943.

[12] *A World in Motion: Systems Engineering Vision 2025*, INCOSE, San Diego, CA, USA, 2014.

[13] J. M. Bradshaw *et al.*, "Adjustable autonomy and human-agent teamwork in practice: An interim report on space applications," in *Agent Autonomy*. Boston, MA, USA: Springer, 2003, pp. 243–280.

[14] A. Alzahrani, V. Callaghan, and M. Gardner, "Towards adjustable autonomy in adaptive course sequencing," in *Proc. 9th Int. Conf. Intell. Environments*, 2013, pp. 466–477.

[15] T. B. Sheridan, *Telerobotics, Automation, and Human Supervisory Control*. Cambridge, MA, USA: MIT Press, 1992.

[16] J. E. Allen, C. I. Guinn, and E. Horvtz, "Mixed-initiative interaction," *IEEE Intell. Syst. their Appl.*, vol. 14, no. 5, pp. 14–23, Sep. 1999.

[17] T. Fong, C. Thorpe, and C. Baur, "Collaborative control: A robot-centric model for vehicle teleoperation," School Comput. Sci., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU-RI-TR-01-34, 2001.

[18] M. L. De Brun *et al.*, "Mixed-initiative adjustable autonomy for human/unmanned system teaming," in *Proc. AUVSI Unmanned Syst. North Amer. Conf.*, 2008, pp. 732–746.

[19] J. Y. C. Chen and M. J. Barnes, "Supervisory control of robots using RoboLeader," *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 54, no. 19, pp. 1483–1487, Sep. 2010.

[20] J. Wang and M. Lewis, "Assessing cooperation in human control of heterogeneous robots," in *Proc. 3rd ACM/IEEE Int. Conf. Hum. Robot Interact.*, Mar. 2008, pp. 9–16.

[21] E. Salas, M. A. Rosen, C. S. Burke, D. Nicholson, and W. R. Howse, "Markers for enhancing team cognition in complex environments: The power of team performance diagnosis," *Aviation, Space, Environ. Med.*, vol. 78, no. 5, pp. B77–B85, May 2007.

[22] P. Millot and M.-P. Pacaux-Lemoine, "A common work space for a mutual enrichment of human-machine cooperation and team-situation awareness," *IFAC Proc. Volumes*, vol. 46, no. 15, pp. 387–394, 2013.

[23] S. Zieba, P. Polet, and F. Vanderhaegen, "Using adjustable autonomy and human–machine cooperation to make a human–machine system resilient—Application to a ground robotic system," *Inf. Sci.*, vol. 181, no. 3, pp. 379–397, Feb. 2011.

[24] L. A. M. Bush, A. J. Wang, and B. C. Williams, "Risk-based sensing in support of adjustable autonomy," in *Proc. IEEE Aerosp. Conf.*, Mar. 2012, pp. 1–18.

[25] L. Carver and M. Turoff, "The human and computer as a team in emergency management information systems," *Commun. ACM*, vol. 50, no. 3, pp. 33–38, Mar. 2007.

[26] G. Loukas, D. Gan, and T. Vuong, "A review of cyber threats and defence approaches in emergency management," *Future Internet*, vol. 5, no. 2, pp. 205–236, Jun. 2013.

[27] L. Rothrock and S. Narayanan, *Human-in-the-Loop Simulations*. London, U.K.: Springer, 2011.

[28] V. Dutt, Y.-S. Ahn, and C. Gonzalez, "Cyber situation awareness: Modeling the security analyst in a cyber-attack scenario through instance-based learning," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*, 2011, pp. 280–292.

[29] D. Robinson and G. Cybenko, "A cyber-based behavioral model," *J. Defense Model. Simul., Appl., Methodol., Technol.*, vol. 9, no. 3, pp. 195–203, Jul. 2012.

[30] M. R. Grimaila and A. Badiru, "A hybrid dynamic decision making methodology for defensive information technology contingency measure selection in the presence of cyber threats," *Oper. Res.*, vol. 13, no. 1, pp. 67–88, Apr. 2013.

[31] A. B. Badiru, P. S. Pulat, and M. Kang, "DDM: Decision support system for hierarchical dynamic decision making," *Decis. Support Syst.*, vol. 10, no. 1, pp. 1–18, Jul. 1993.

[32] K. E. Schaefer, E. R. Straub, J. Y. C. Chen, J. Putney, and A. W. Evans, III, "Communicating intent to develop shared situation awareness and engender trust in human-agent teams," *Cogn. Syst. Res.*, vol. 46, pp. 26–39, Dec. 2017.

[33] J. D. Lee and K. A. See, "Trust in automation: Designing for appropriate reliance," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 46, no. 1, pp. 50–80, Mar. 2004.

[34] D. H. McKnight, V. Choudhury, and C. Kacmar, "The impact of initial consumer trust on intentions to transact with a web site: A trust building model," *J. Strategic Inf. Syst.*, vol. 11, nos. 3–4, pp. 297–323, Dec. 2002.

[35] E. T. Chancey, J. P. Bliss, A. B. Proaps, and P. Madhavan, "The role of trust as a mediator between system characteristics and response behaviors," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 57, no. 6, pp. 947–958, Apr. 2015.

[36] J. Xu, K. Le, A. Deitermann, and E. Montague, "How different types of users develop trust in technology: A qualitative analysis of the antecedents of active and passive user trust in a shared technology," *Appl. Ergonom.*, vol. 45, no. 6, pp. 1495–1503, Nov. 2014.

[37] F. Boroomand *et al.*, "Cyber security for smart grid: A human-automation interaction framework," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT Eur.)*, Oct. 2010, pp. 1–6.

[38] K. E. Schaefer, J. Y. Chen, J. L. Szalma, and P. A. Hancock, "A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 58, no. 3, pp. 377–400, Mar. 2016.

[39] A. R. Selkowitz, S. G. Lakhmani, and J. Y. C. Chen, "Using agent transparency to support situation awareness of the autonomous squad member," *Cogn. Syst. Res.*, vol. 46, pp. 13–25, Dec. 2017.

[40] P. Bobko, A. J. Barelka, L. M. Hirshfield, and J. B. Lyons, "Invited article: The construct of suspicion and how it can benefit theories and models in organizational science," *J. Bus. Psychol.*, vol. 29, no. 3, pp. 335–342, Sep. 2014.

[41] D. B. Buller and J. K. Burgoon, "Interpersonal deception theory," *Commun. Theory*, vol. 6, no. 3, pp. 203–242, Aug. 1996.

[42] J. L. Hilton, S. Fein, and D. T. Miller, "Suspicion and dispositional inference," *Pers. Social Psychol. Bull.*, vol. 19, no. 5, pp. 501–512, Oct. 1993.

[43] J. Mayer and T. Mussweiler, "Suspicious spirits, flexible minds: When distrust enhances creativity," *J. Pers. Social Psychol.*, vol. 101, no. 6, p. 1262, Dec. 2011.

[44] I. Kim and J. H. Jo, "Performance comparisons between thumb-based and finger-based input on a small touch-screen under realistic variability," *Int. J. Hum.-Comput. Interact.*, vol. 31, no. 11, pp. 746–760, Jun. 2015.

[45] S. G. Hart and L. E. Staveland, "Development of NASA-TLX (Task load index): Results of empirical and theoretical research," *Adv. Psychol.*, vol. 52, pp. 139–183, Jan. 1988.

[46] S. G. Hart, "NASA-task load index (NASA-TLX); 20 years later," *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 50, no. 9, pp. 904–908, Oct. 2006.

[47] J. R. A. Santos, "Cronbach's alpha: A tool for assessing the reliability of scales," *J. Extension*, vol. 37, no. 2, pp. 1–5, 1999.

[48] D. E. Bell, H. Raiffa, and A. Tversky, "Descriptive, normative, and prescriptive interactions in decision making," in *Descriptive, Normative, and Prescriptive Interactions in Decision Making*, vol. 1. New York, NY, USA: Cambridge Univ. Press, 1988, pp. 9–32.

[49] R. W. Cooksey, *Judgment Analysis: Theory, Methods, and Applications*. New York, NY, USA: Academic, 1996.

[50] S. W. Raudenbush and A. S. Bryk, *Hierarchical Linear Models: Applications and Data Analysis Methods*, vol. 1. London, U.K.: Sage, 2002.

[51] H. Woltman, A. Feldstain, J. C. MacKay, and M. Rocchi, "An introduction to hierarchical linear modeling," *Tuts. Quant. Methods Psychol.*, vol. 8, no. 1, pp. 52–69, 2012.

[52] T. Harlow, "Deputy praised for not sweving in deer crash," *Star Tribune*, Oct. 2017.

[53] K. Drnec, A. R. Marathe, J. R. Lukos, and J. S. Metcalfe, "From trust in automation to decision neuroscience: Applying cognitive neuroscience methods to understand and improve interaction decisions involved in human automation interaction," *Frontiers Hum. Neurosci.*, vol. 10, p. 290, Jun. 2016.

[54] R. Lee, M. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington, DC, USA: E-ISAC, 2016.

[55] P. Nader, P. Honeine, and P. Beauseroy, "Detection of cyberattacks in a water distribution system using machine learning techniques," in *Proc. 6th Int. Conf. Digit. Inf. Process. Commun. (ICDIPC)*, Apr. 2016, pp. 25–30.

[56] K. E. Crocker, "The influence of the amount and type of information on individuals' perception of legal services," *J. Acad. Marketing Sci.*, vol. 14, no. 4, pp. 18–27, Dec. 1986.

[57] R. J. Lutz and P. J. Reilly, "An exploration of the effects of perceived social and performance risk on consumer information acquisition," in *Advances in Consumer Research*, S. Ward and P. Wright, Eds. Ann Abor, MI, USA: Association for Consumer Research, 1974, pp. 393–405.

[58] D. L. Davis, J. P. Guiltinan, and W. H. Jones, "Service characteristics, consumer search, and the classification of retail services," *J. Retailing*, vol. 55, no. 3, p. 3, 1979.

[59] K. Mitra, M. C. Reiss, and L. M. Capella, "An examination of perceived risk, information search and behavioral intentions in search, experience and credence services," *J. Services Marketing*, vol. 13, no. 3, pp. 208–228, 1999.

CHRIS GAY received the Ph.D. degree in systems and information engineering from the University of Virginia, in 2017. He is currently an Assistant Professor of systems engineering and management with the Air Force Institute of Technology, Dayton, OH. He is also an active duty Air Force Officer. His research interests include human response to cyber-attacks and project management of complex systems.

BARRY HOROWITZ has been a Professor of systems and information engineering with the University of Virginia, since 2001, he was the Department Chair, from 2009 to 2017. He has served and led studies for the National Academy of Engineering, the Defense Science Board, and the Army Science Board, focused on system aware cybersecurity.

JOHN J. ELSHAW received the Ph.D. degree in management with a focus on organizational behavior and human resource management from Purdue University. He is currently pursuing the degree with the United States Air Force Squadron Officer School, Air Command and Staff College. He is currently an Assistant Professor of systems engineering with the Department of Systems Engineering and Management, Air Force Institute of Technology.

PHILIP BOBKO received the Ph.D. degree in economic and social statistics from Cornell University. He is currently a Professor (Emeritus) of management and psychology with the Gettysburg College. His research interests, journal articles, and books are in statistics, management, and applied psychology. He has served as an Editor for the *Journal of Applied Psychology*.

INKI KIM (M'16) received the Ph.D. degree in industrial engineering from Pennsylvania State University. He is currently an Assistant Professor of systems and information engineering with the University of Virginia. His research interests include human behavior and performance modeling and simulation-based training. He has been a member of the Human Factors and Ergonomics Society (HFES).