AFRL-RH-WP-TM-2010-0003

Cyber Disrupt and Deny (Cyber D&D)

Dennis J. Riechman

Air Force Research Laboratory
Sensemaking & Organizational Effectiveness Branch

May 2010

Final Technical Memo June 2007 to May 2010

Approved for public release; distribution is unlimited.

Air Force Research Laboratory
711th Human Performance Wing
Human Effectiveness Directorate
Anticipate & Influence Behavior Division
Sensemaking & Organizational Effectiveness Branch
Wright-Patterson AFB OH 45433-7604

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th Air Base Wing Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RH-WP-TR-2010-0003 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//SIGNED//
DENNIS J. RIECHMAN
Work Unit Manager
Sensemaking & Organizational
Effectiveness Branch

//SIGNED//
GLENN W. HARSHBERGER
Anticipate & Influence Behavior Division
Human Effectiveness Directorate
711th Human Performance Wing
Air Force Research Laboratory

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
May 2010	Final Technical Memo	June 2007-May 2010

4. TITLE AND SUBTITLE

Cyber Disrupt and Deny (Cyber D&D)

5a. CONTRACT NUMBER
In-House

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62202F

6. AUTHOR(S)

Dennis J. Riechman

5d. PROJECT NUMBER
7184

5e. TASK NUMBER
X0

5f. WORK UNIT NUMBER
7184X01W

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Sensemaking & Organizational Effectiveness Branch

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Materiel Command
Air Force Research Laboratory
711th Human Performance Wing
Human Effectiveness Directorate
Anticipate & Influence Behavior Division
Sensemaking & Organizational Effectiveness Branch
Wright-Patterson AFB OH 45433-7604

10. SPONSOR/MONITOR'S ACRONYM(S)

711 HPW/RHXS

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

AFRL-RH-WP-TM-2010-0003

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

88ABW cleared on 26 May 2010, 88ABW-2010-2887

14. ABSTRACT

The purpose of this research effort was to study cyber deception and evaluate information technology (IT) suspicion within a human operator. Researchers focused on examining how and under what conditions subtle manipulations cause individuals to become suspicious. This project attempted to develop measures to assess the effects of IT and other cyber tools on human operators. A full description of the effort can be found in "Development of IT Suspicion as a Construct and Subsequent Measure" by Captain Matthew Olson, USAF (AFIT/GEM/ENV/09-M15, ADA50246).

15. SUBJECT TERMS

Trust, Construct, Information Technology, Suspicion

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
Unclassified					Dennis J. Riechman
a. REPORT	b. ABSTRACT	c. THIS PAGE	SAR	10	19b. TELEPHONE NUMBER *(include area code)*
U	U	U			NA

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. 239.18

THIS PAGE LEFT INTENTIONALLY BLANK

SUMMARY

This report summarizes the research effort titled "Cyber Disrupt and Deny" (Cyber D&D), which started on June 12, 2007 and concluded on March 31, 2010. The report references the collaborative research effort between the Air Force Research Laboratory's Information Directorate (AFRL/RI), Human Effectiveness Directorate (711HPW/RH) and the Air Force Institute of Technology (AFIT). AFIT's published contribution is a thesis titled "Development of IT Suspicion as a Construct and Subsequent Measure" by Captain Matthew Olson, USAF (AFIT/GEM/ENV/09-M15, ADA502469). This cumulative research effort was accomplished in-house in conjunction with the Air Force Institute of Technology for Anticipate and Influence Behavior Division (711HPW/RHX) of the Human Effectiveness Directorate. This technical memo substitutes for the technical report to close out work unit 7184X01W in HWIS and DTIC, since the above referenced thesis was published by AFIT.

The purpose of this effort was to study cyber deception and evaluate information technology (IT) suspicion within a human operator. Researchers focused on examining how and under what conditions subtle manipulations cause individuals to become suspicious. This project attempted to develop measures to assess the effects of IT and other cyber tools on human operators.

The original intent of the work unit was to encompass both cyber disruption and denial on the human operator. This research vector was narrowed in scope due to a changing management mission focus. Funding was zero-out for Fiscal Year 2009 and Fiscal Year 2010 and oversight was advanced to the Air Force Office of Scientific Research (AFOSR) to sustain funding. AFOSR provided minimal funding to continue the research effort and leverage this with other AFOSR "Cyber D&D" research efforts. AFRL/RI and AFOSR concentrated their resources on the destroy task of the original intent.

This project developed a baseline with an extensive literature review on suspicion, specifically IT suspicion, which was followed with a definition of the experimental design. The target was to characterize the capacity of IT suspicion to develop in an operator. After establishing the construct, the IT suspicion study was constructed and performed under the guidance of AFIT.

For the intent of this report, this research focus was narrowed to cyber disruption by manipulating the IT system and measuring its effects by evaluating the index of suspicion for human operators.

BACKGROUND

Information Technology (IT) has played an essential role and been the primary channel for communication and data storage operations in the modernized world to include the workforce within the United States Air Force (USAF). IT is used in almost every piece of combat equipment in today's Air Force. New technology and our airmen's dependency on cyberspace has enhanced at a staggering rate over the past decades. The number of internet applications has grown dramatically in the last few years with examples ranging from wiki's, banking, blogs, and social networking sites. More people are using information systems and they are becoming easier to operate with more interactive interfaces. Now more than ever, adversaries of the United States are trying to infiltrate IT systems. Recent examples include the Google computer system that was hacked in 2009. Identifying information and collecting knowledge that can predict how effectively and securely people will interact with IT could be important for almost any job and a valuable insight to Air Force senior leadership and those responsible for Air Force cyber network security.

Military deception (MILDEC) is a core Information Operations capability. Joint Publication 3-13.4, Military Deception, dated 13 July 2006, describes MILDEC as "supporting, and related information capabilities must be planned and integrated to support the commander's campaign and/or operation. Collectively, these capabilities target adversary decision makers to affect their information systems and decision-making processes." However, suspicion is notably absent from joint doctrine. MILDEC is focused on desired behaviors in addition to affecting the adversary's thinking and decision making processes. Suspicion may or may not be a valuable asset in cyber defense.

Developing an assessment for measuring IT suspicion provides that kind of foundational knowledge. Even with the advancements in technology and ever increasing consumer demand for these technology advances, there is little established in the scientific community about suspicion and how that interacts with IT systems. The fact of the lack of research is unexpected since the point at which individuals might realize they are being manipulated can be a dynamic research area. The concept of trust in an information system provides a viable research vector to investigate. Another area is to explore a human operator's index of suspicion regarding the information gathered from an information system. This research delved into the cognitive, attitudinal and behavioral constructs set within the reference of IT and will provide helpful results into the user-IT interface. Suspicion in the conceptual definition is a common thread of research; however, there are few examples in the research literature that focus mainly on the domain of IT suspicion. The examples that do exist center on generic communication-related suspicion and not directly on IT systems. The small number of research studies on suspicion added to the inconsistent validation of those studies creates a deficiency in the suspicion literature. There is a rich potential of research discoveries that have the potential to aid the war fighter.

There are several methods to test a level of suspicion in a computer operator. Workflow disruption can consisted of altering human interface devices such a computer monitor display, keyboard and mouse actions, and other functions such as refresh rates, and data information. By manipulating the monitor parameters, the mouse can be made too sensitive to use or too slow to be effective. By remapping the keys of a keyboard in response to certain actions, such as typing a certain word, or entering a password prompt, an operator can begin to question the integrity of the IT system. These interfaces will be the target for direct disruptive actions.

The dynamics of the IT system interface has created some unique challenges to it because the interface is between a human and a non-human. Conducting a research study needs to differentiate the two. For instance in a research effort by Stricker et al (1967) they revealed that there is a difference between suspicion of method and suspicion in the research purpose. Therefore, a subject may not be suspicious of the IT system but as a research subject, they may be suspicious of the purpose of the experiment. The experimental design must account for this unique interface. Another challenge in measuring IT suspicion is the fact that the generation of the suspicion is an IT system, which is not a person but a series of inputs and codes generated by people who design IT systems. IT is not an individual, but a system (13).

This task was an effort to develop a measure for suspicion that specifically identifies IT suspicion. A construct of IT suspicion was developed to quantify the index of suspicion. The suspicion measure consists of both state and trait measures. IT suspicion can be portioned into an enduring trait characteristic and an induced state characteristic with multiple focuses of the suspicion. The human operator can be suspicious of the IT system and/or the data within the IT system. There are numerous implications to this research area that can protect Air Force infrastructures and IT systems.

METHODS

To go about defining and developing a viable and reliable measurement for suspicion for the Cyber D&D work unit, the research and development approach was to break down the process into four stages.

First, there was a comprehensive literature search for cyber influence and suspicion of information systems. The review looked at leading edge research and current practices on the new cyber domain. Naturally, the focus was on the relationship between the user-IT interface which also included suspicion, trust and locus of control. The literature review provided little conceptual definitions for suspicion and even less for IT suspicion. Therefore, a testable and proven definition of IT suspicion did not emerge for the extensive literature search. This search provided the best foundation to begin the construction of an IT suspicion construct.

Second, the Anticipate and Influence Behavior Division established an alliance with AFIT's Department of Systems and Engineering Management and AFRL's Information System Research Branch to leverage expertise and resources in order maximize the research effort. This working group matured several research vector ideas for research into future efforts.

Third, this research effort was to develop a hypothesis and theory and conduct experiments regarding cyber suspicion. In accordance to this partnership, AFIT student Captain Matthew Olson studied this topic, created a pilot study and published a thesis on this topic. The focus of the "Development of IT Suspicion as a Construct and Subsequent Measure" thesis was the experiment and measure testing user suspicion of IT. This was completed to evaluate the effectiveness of disruptive capabilities. The research objective was conducted in four phases: to define a construct for IT suspicion, to create a subjective measure for this construct, to select lab settings to administer the construct measure, and to complete a pilot study of the measure to guide future research.

The first phase defined the construct for IT suspicion. Since the literature review generated very little conceptual definitions for IT, suspicion did not emerge from the extensive literature search. Therefore, a construct of suspicion with regards to IT suspicion was created. This construct for the effective manipulation of IT became the definitive measure for suspicion.

The second phase of this experiment is the subjective measure of the suspicion construct. This was accomplished by disrupting the workflow of the human operators and promoting inefficiencies within the information system the interface. The measure collected from three parts to create an IT suspicion measure. Abstracted from the AFIT thesis, the measure consisted of three parts; the trait measure from suspicion's nomological net, the trait suspicion measure for establishing the baseline and lastly the state suspicion measure. These individual measurements resulted in the IT suspicion construct. The trait IT suspicion measure was administered with a disposition to trust and a locus of control which was done in order to establish a trait IT baseline (p. 21). The trait suspicion measure was a manipulation exercise on a laptop computer intended to induce suspicion. The state suspicion measurement was analyzed from a survey of those participants in the experiment.

The third phase within the AFIT research was to administer the experiment using AFIT Department of Systems and Engineering Management graduate students. Some key technologies and methodologies used were develop human factor metrics and measures to

evaluate psychological effects of operators; study using survey and experimentation to validate most efficient non-lethal cyber tools. In this instance, the subjects completed a couple of simple computer tasks on a computer that secretly was manipulated. The computer mouse's controls were altered: the left and right mouse buttons were reversed, the mouse's double click speed was increased, and the mouse pointer was altered. The tasks consisted of creating a folder on the computer and creating a word document and excel spreadsheet to put in the folder.

The final phase of the AFIT project was to analyze the pilot study to guide further research from the measurements that assessed the psychological effects of cyber tool employment on human operators. The results from the study and discussion on potential future research vectors gathered from this research are elaborated on in a later section.

The fourth and final stage of this research effort was to publish the results of the manipulation and cyber disruption experiment and extrapolate the results to other fields. The effort then proposed further research in the IT suspicion domain of the comprehensive contract.

RESULTS

The goal of this research effort was to uncover suspicion and frustration tolerance levels and to develop measures to evaluate the psychological effects of cyber tool employment on human operators. Suspicion was measured using a subjective scale to assess trait-based and state suspicion. The results stem from the survey and subsequent experiment conducted on the AFIT campus. The methodology used a psychometric analysis using both factor analysis and reliability analysis. These results show that state and trait dimensions load on different factors, which provides an initial confirmation that suspicion is composed of both state and trait components.

The thesis study resulted from respondents from the Air Force Institute of Technology in the IT suspicion survey. Table 15 from the AFIT thesis packages the results from the 20 person study involving AFIT graduate students.

Table 15. Inter-Measure Correlations

Measure	Revised trait general suspicion	Trait data suspcion	Revised state general suspicion	Revised locus of control	Revised disposition to trust
Revised trait general suspicion	α=.796				
Trait data suspicion	0.412	α=.774			
Revised state general suspicion	0.227	-0.044	α=.916		
Revised LOC	0.064	0.323	-0.576**	α=.706	
Revised disposition to trust	0.167	0.279	-0.169	0.222	α=.911

N=20 ** denotes correlation is significant at $p<0.01$ level.

CONCLUSION

The strategic vision for Cyber D&D was redefined and limited in scope during the research effort. The amended scope of Cyber D&D narrowed and resulted in an AFIT thesis while AFOSR and AFRL/RI assumed the Cyber destroy aspect of the research vector. The aspect of IT denial was put on hold while this effort focused on the spectrum of IT disruption. Suspicion in IT was studied successfully and a suspicion construct was developed.

The experiment design yielded noteworthy data to support a baseline for future IT suspicion studies. The developed measure consisted of three parts: trait measure, trait suspicion measure, and state suspicion measure. The results showed that you can reliably assess trait and state suspicion metrics. However, with small sample size, further testing would be needed to help the validity of these scales. Another limitation is that there are other factors that may contribute to IT suspicion such as existing knowledge of IT systems. Regardless, IT suspicion measurement will support future research projects.

DISCUSSION

This research effort studied IT suspicion and created a measurement construct. IT suspicion as a whole may be too broad to classify and may require a more focused research vector, but this effort provided a foundation for further research. The development of an IT suspicion construct can have many benefits for the Air Force. The scales themselves could be used in on-going research on trust to further explore the convergence or divergence of these suspicion constructs. It is noteworthy that the trust scale had a very low correlation with the suspicion scales, thus suggesting that they are orthogonal constructs. These scales should be included in ongoing research on trust to further explore these relationships.

Another potential application is for IT suspicion surveys that can be administered for recruits to pre-screen them for a career that best suits their index of suspicion. A survey can fit airmen into jobs that will best protect the Air Force. For example, an airman with low suspicion index would be a poor fit for a job in the Communications Group since one would need to have a high level of suspicion while working with IT. Also, an IT suspicion survey can be used determine a part of a computer system is causing suspicion or uncertainty to users, thus paving the way for system improvements.

The generation of the IT suspicion measurement will support future research projects as a focus to study the continuous construct of cyber disruption. Future efforts into cyber destroy and deny undertaking s will potentially benefit Air Force offices that are heavily invested in information systems such as the CNO —cyber network office—and can have significant applications to their mission.

Future research efforts can have a wide range of applications because IT is used in almost every job in the Air Force. A measureable construct will aid in future research. Understanding how a human operator trust or has suspicion for the IT system, the Air Force can maintain a higher level of operational readiness and network security.