**17th ICCRTS**

**“Operationalizing C2 Agility”**

**Title of Paper**

# Modeling trust in ELICIT-WEL to capture the impact of organization structure on the agility of complex networks

**Topic(s)**

Topic 4: Collaboration, Shared Awareness and decision Making
Topic 5: Experimentation, Metrics, and Analysis
Topic 8: Networks and Networking

**Name of Author(s)**

Kevin Chan,  US Army Research Laboratory
Mary Ruddy, Azigo

**Point of Contact**

Kevin Chan
RDRL-CIN-T
2800 Powder Mill Rd.
Adelphi, MD 20783
kevin.s.chan@us.army.mil

## Abstract:

As tactical environments become more complex and dynamic, it has become increasingly important to develop suitable models for them, and to anticipate the effects of organizational and network changes on operational agility and mission effectiveness. Building upon previous work that integrated ELICIT with a wireless emulation test bed, the Wireless Emulation Laboratory (WEL), the ELICIT-WEL system is further enhanced to model the evolution of trust between and among network nodes under varying organizational and network connectivity scenarios. Trust between entities in the organization varies based on perceived willingness and competence within the ELICIT framework. The enhanced integrated emulation platform is then used to conduct a series of agent-based ELICIT experiments whose design is informed by soldier exercises.

## 1. Introduction

Information in command and control environments is readily available and the scope, volume, and diversity are growing continuously. Being able to handle this data correctly, efficiently and securely is essential in maintaining acceptable decision-making performance and situation awareness, not unnecessarily draining communications and human resources, and preventing adversaries from accessing it. Without such services, the effectiveness of organizations is hindered, on every level of tactical operations.

Particularly within the United States Department of Defense (DOD), the DOD Chief Information Officer (CIO) is tasked to ensure that mission-critical information is visible, accessible, and understandable to all authorized users in a trusted environment without regard to location or time. Within this mission, the goal is to continue to look for best ways to manage information flows in a complex world and to leverage available technology. Specifically, the DoD CIO issued a data sharing strategy in 2009 [DoD CIO 2009] to change the data sharing paradigm through the various strata of the military networks from "Process, exploit, disseminate" to "post before process". This involves satisfying several data service goals:

a) *Make data visible* – users and applications can discover the existence of all data assets through databases or search services.
b) *Make data accessible* – data is stored such that users and applications can access it except when limited by policy, regulation or security.
c) *Institutionalize data management* – data approaches are incorporated into the Department processes and practices.
d) *Enable data to be understandable* – users and applications can comprehend the data both structurally and semantically, and readily determine how the data may be used for their needs.
e) *Enable data to be trusted* – users and applications can determine and assess the authority of the source because of the pedigree, security or access control level of each data asset.
f) *Interoperable* – many-to-many exchanges of data between systems allow mediation or translation of data between interfaces.
g) *Be responsive to user needs* – incorporate perspectives of users via continual feed back to ensure satisfaction

We consider two example tactical networks to frame our discussions. One involves a small unit of soldiers supporting a commander responsible for ultimate decisions and the other a coalition network where there are multiple organizations operating with varying objectives and capabilities.

First, Company Intelligence Support Teams (COIST) are company-level intelligence S2 sections responsible for providing intelligence to the commander. Because the commander is required to perform intelligence analysis and fusion on many sources of information (e.g. documents, reports, debriefs, SITREPs) he needs small teams of soldiers (COIST) to gather information in order to understand and effectively make tactical decisions. In [Morgan 2008], COIST are responsible for five functions.

- Manage the company’s lethal and non-lethal targeting
- Supervise the company’s intelligence, surveillance, and reconnaissance (ISR) program
- Manage the patrol prebrief/debrief for the company
- Detainee operations
- Tactical site exploitation

Performance and the quality of decisions in COIST environments can be greatly influenced by how the commander trusts his sources of information relative to the current operating environment. Being able to model and simulate various configurations and operating environments is crucial to the understanding of the capability of COIST in tactical networks. This networking scenario also reinforces the idea that “every soldier is a sensor,” given that every soldier is generating data and in some cases also processing, interpreting or exploiting the data.

Coalition networks are another example of complex networks in a tactical environment that handles a wide range of information flows. Members within the coalition must make decisions based on information from entities with whom they may not be familiar or have complete trust. These networks may be comprised of other military branches, non-governmental agencies, other militaries, or foreign nationals. Given the diversity of entities and necessity to exchange information, it is vital to understand trust relationships, information value and quality when interacting with other coalition members.

In tactical networks such as COIST or coalition networks, the overriding problems involve being able to handle immense amounts of data, to deliver the information to those who need the information to make informed decisions, and to maximize the decision-making performance of these networks. Trust may serve as a means to improving the performance of C2 networks.

This work extends existing work on modeling of trust in an information sharing scenario and it also describes how trust is built into an existing command and control experiment platform. It is important to understand how trust evolves in networked systems and the effect of trust on behavior and network performance. This work is one approach to building a model for how two of these concepts could be realized in a command and control operational scenario. Building a model and being able to experiment with these concepts can provide valuable insights to which parameters can be adapted to maximize mission performance in tactical networks.

## 2. Experimental Laboratory for Investigating Collaboration, Information-sharing and Trust.

The Experimental Laboratory for Investigating Collaboration, Information-sharing and Trust (ELICIT) was created to test some of these concepts and properties. ELICIT is a tool for modeling the behaviors of individuals in various organizational networks.  Sponsored by the Command and Control Research Project, a project within the Office of the Assistant Secretary of Defense (OASD) Networks and Information Integration (NII), ELICIT has an online multi-user software platform for conducting experiments and demonstrations in information-sharing and trust. The ELICIT software platform allows researchers and instructors to precisely model specific Command and Control processes, as well as edge organization processes and to fully instrument all interactions. The original project objective was to enable a series of online experiments to compare the relative efficiency and effectiveness of various organization types, traditional *command and control (C2)* vs. self-organizing, peer-based *edge (E)* organizational forms, in performing tasks that require decision making and collaboration. ELICIT supports configurable task scenarios. The original baseline experiment task is to identify the who, what, where and when of an adversary attack based on information factoids that become known to individuals in a team or group of teams. The independent variable for the baseline experiment is whether a team is organized using traditional Command and Control vs. Edge organization principles.

ELICIT participants can be humans and or configurable software agents. The software agent-based version of ELICIT (abELICIT) supports software agents whose behavior is defined by over 50 variables that can be configured to model various social and cognitive behaviors; and operations and performance delays. The agent behavior was modeled upon and validated against the actual behavior of human participants in ELICIT exercises. To date, ELICIT experiments have been run with both human and software agent participants internationally at both military and civilian institutions. Participating organizations include US Military Academy; Army Research Labs (ARL); Army War College; National Defense University; Naval Post Graduate School; Naval War College; Harvard; Boston University; George Mason University; Johns Hopkins University; Defense Research and Development Canada; York University; Defense Academy of the United Kingdom; Cranfield University; University of Southampton; Portuguese Military Academy; Singapore Armed Forces Centre For Military Experimentation; and Military Polytechnic Academy, Army of Chile. Thus the ELICIT experience base is well suited to the modeling of international military/civilian efforts. ELICIT is unique in that it not only can model complex networks and information flows, it can also be used to assess whether an intelligent agent assigned to a particular part of the network has sufficient situational awareness to effectively execute their assigned task.

Based on input from the ELICIT research community, ELICIT continues to evolve to be a more powerful and flexible research tool. Though originally designed to compare just the edge and traditional C2 organization structures, it is now flexible enough to model other hybrid organizational forms. Manso [Manso and B. Manso 2010] has used ELICIT to model the five organizational structures comprising the North Atlantic Treaty Organization (NATO) Network Enabled Capabilities (NEC) Command and Control (C2) Maturity Model (NEC2M2, SAS-065 2011. The concept of a "maturity model" was first popularized through the very successful "Capability Maturity Model" for software development organizations (CMM-SW) which was created by the Software Engineering Institute (SEI) between 1986 and 1993 (Schlichter, 2011.) SAS-065 leveraged this concept to develop a maturity model for general organizational agility. The N2C2M2 defines five levels of ability to generate synergies across a group of participants. The five levels of operational capability are: Conflicted C2; De-conflicted C2; Coordinated C2; Collaborative C2; and Edge C2. So for example, a level 5 organization has the ability to operate in an edge organizational structure and also in any of the organizational structures represented by the lower levels. The following chart (Manso 2011) highlights some of the organizational capabilities that are characteristic of these five levels.

| | Degree of Shared Awareness | Degree of Shared Understanding | Relative Effectiveness | Efficiency, Given Effectiveness | Agility of the Collective C2 Process |
|---|---|---|---|---|---|
| Edge C2 | Broad, Deep, Tailored and Dynamic | Broad, Deep, Tailored and Dynamic | Tailored and dynamic synergies | Highly efficient | Proactive across a broad range of conditions |
| Collaborative C2 | Significant | Significant | Substantial synergies across collaborative areas/functions | Substantial efficiencies across collaborative areas/functions | Substantial, timely and continuous |
| Coordinated C2 | Limited | Limited | Limited synergies due to coordination | Limited efficiencies due to coordination | Limited to coordinated functions/actions; Slow; Reactive |
| De-conflicted C2 | Focused on the boundaries | None | Avoids costs of negative cross-Impacts | Sub-optimized use of resources | Vulnerable at seams; Rigid from specialization |
| Conflicted C2 | None | None | Negative cross-Impacts | Inefficiency wasted resources | Fragile and vulnerable at the seams |

**Table 1 – Characteristics of five NEC2M2 approaches**

Thus, associated with each level is the ability of an organization to adopt one or more C2 Approaches. Moreover, associated with increased maturity is the ability to adopt a wider range of C2 Approaches that, in turn, cover a large portion of the C2 Approach Space (SAS-050 2006, 2). (see Figure 1).

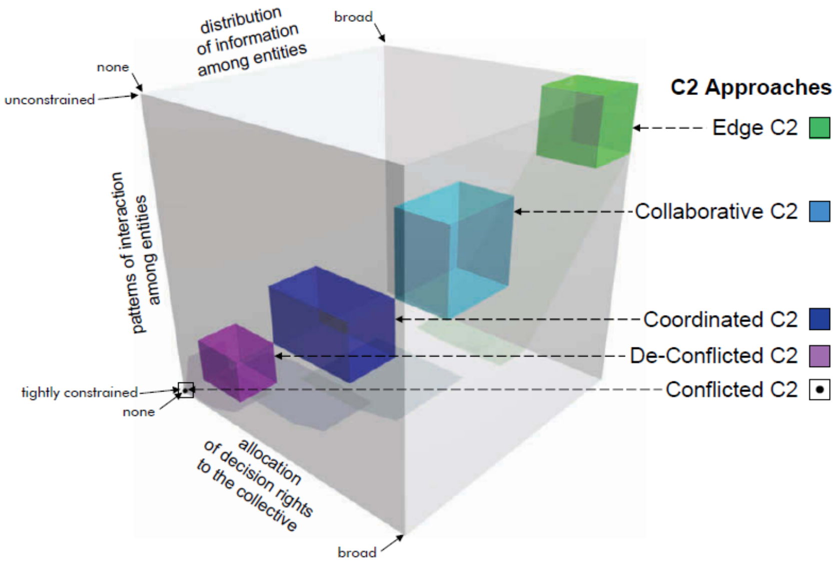


**Figure 1 - Collective C2 Approach Space (SAS-065 2010)**

Higher maturity levels include the ability to adopt C2 approaches located at the ‘upper right’ side of the C2 approach space (e.g., Collaborative and Edge).

A main assumption in the N2C2M2 is that **more network-enabled Collective C2 Approaches achieve higher levels of shared awareness and understanding than less network-enabled ones, as well as increased endeavor effectiveness, efficiency and agility**. This model has been tested in (SAS-065 2010) [Manso and B. Manso 2010] and yielding conclusions that support the model's assumptions.

ELICIT experiments by [Powley, 2009] have shown that team performance is very sensitive to participant trust levels. By enhancing ELICIT software agents to have a richer trust model, we can enable a richer modeling of the NEC C2 maturity model.

### 3. Network Science Collaborative Technology Alliance (CTA):

Past work involving composite networks and ELICIT included adding a communication network component to ELICIT and enabling loss and delays along with other communication network related quality of service parameters. [Chan 2010, 2011]. First, we used ELICIT agent configuration parameters to simulate loss and delays in communications to observe how decision-making performance and shared situational awareness was impacted by various network quality of service (QoS) parameters. It was observed that there was a threshold effect in the delays in communication with regard to shared situation awareness. Additionally, a processing information overload was observed when the connectivity of the organization grew past a particular point. Second, we augmented the capability of the sensemaking agent in ELICIT by integrating ELICIT into United States Army Research Laboratory's (ARL) Wireless Emulation Laboratory (WEL) [Chan 2011]. This enabled ELICIT to be run with an underlying communication network during the execution of the task within the organization. Then this integrated platform was used to perform experiments to acquire corroborating evidence, by configuring more sophisticated delays in WEL to represent delays in the communication network.

In addition to modeling the communication network within this scenario, it is of interest to model aspects from multiple layers of composite networks. In this work, we consider trust as a dimension within the ELICIT scenario to determine its impact on shared situation awareness. In 2009, ARL established a collaborative research alliance to unite research across organizations, technical disciplines, and research areas to address the critical technical challenges of the Army and Network-Centric Warfare (NCW). The Network Science Collaborative Technology Alliance [NSCTA 2012] was formed to explore foundational cross-cutting research on network science, resulting in greatly enhanced human performance for network-enabled warfare and in greatly enhanced speed and precision for complex military operations. One of its research thrusts is the trust cross cutting research initiative (Trust CCRI), which was established to study the composite nature of trust to include the communication, information and social and cognitive network influences of and to trust.

With regard to trust, the basic formulation of a trust relationship is an evaluation of a trustee entity by a trustor entity. The trustor can establish trust in the trustee by collecting evidence of the trustee to determine if the trustee is trustworthy or not. There have been a great number of proposed trust models [Endsley 1995, 1998, Lee 2004, Rempel 1995, Mayer 1995, Cho 2010].

Most of these works define a set of dimensions of which trust is composed. The literature also presents models or flows of the process of trust. What are generally not developed are computational models to show how composite trust dimensions are incorporated. The goal of this paper is to present a computational trust model for an information sharing scenario that we recently developed [Chan 2012] and to implement it into the existing ELICIT platform.

The trust model that we developed consists of two trust dimensions that are applicable to the information sharing scenario. We propose to include the concepts of willingness and competence as trust dimensions. We define competence as the ability of a team member to send pertinent or useful information. We define willingness as the amount of effort a team member is willing to spend on the given entity. We also propose a way that a trustor can use evidence based on the experience the trustor has interacting with the trustee to compute an estimate of its trust in the trustee. The calculations are done using a Bayesian update with conjugate based on prior distributions to model the estimate of trust distribution. In this paper, we define how the trust evidence can be collected within the ELICIT platform.

With regard to competence, a trustor tracks positive and negative evidence to evaluate its competence trust. This dimension measures the amount of new information the trustee node provides to help with the information disambiguation task, which leads to improved situation awareness. In this scenario, we consider positive evidence to be the number of new factoids sent by the trustee and negative evidence to be the number of duplicate factoids sent by the trustee. The evidence is modeled by a binomial distribution and incorporated as likelihood to the Beta distribution for the prior distribution.

| | |
|---|---|
| a. $p_c(\text{trust}) = \dfrac{t^{\alpha-1}(1-t)^{\beta-1}}{B(\alpha,\beta)}$ | c. $E(t) = \dfrac{\alpha+r}{\alpha+r+\beta+s}$ |
| b. $p_c(\text{evidence}\,|\,\text{trust}) = \dbinom{r+s}{r} t^r(1-t)^s$ | d. $\sigma^2(t) = \dfrac{(\alpha+r)(\beta+s)}{(\alpha+r+\beta+s)^2(\alpha+r+\beta+s+1)}$ |

**Table 1. Conjugate prior-posterior beta-binomial distributions. a) Prior competence trust distribution b) Likelihood (evidence) distribution) c) Expected competence trust d) Variance competence uncertainty.**

Willingness is measured by the raw number of factoids sent by the trustee to a trustor in a specified period of time. This will evaluate the relative cognitive or communications bandwidth that the trust is willing to spend on the trustee. The neighbor that sends the most factoids to the trustor will be assigned a willingness trust score of 1 and the neighbor who sends the least will be given a score of 0. The neighbor sending the second most factoids will receive a willingness trust (n-2)/(n-1). If two nodes send the same amount of factoids, then they are given the average of the scores each of the nodes would have received. The willingness scores are used as evidence (likelihood) for a Gaussian-Gaussian conjugate prior-posterior distribution.

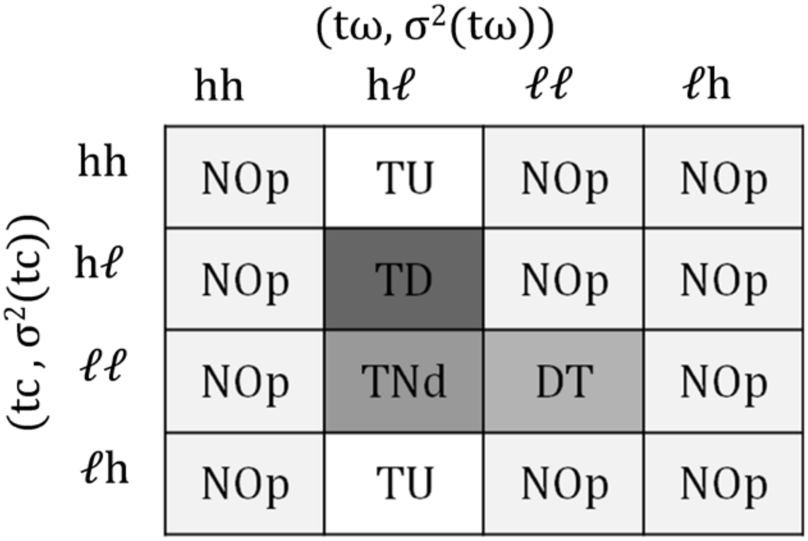
| | |
|---|---|
| a. $p_w(\text{trust}) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(t-\mu_0)^2}{2\sigma^2}}$ | c. $E(t) = \left(\frac{u_0}{\sigma_0^2}+\frac{u}{\sigma_U^2}\right)/\left(\frac{\sigma_0^2+\sigma_U^2}{\sigma_0^2\sigma_U^2}\right)$ |
| b. $p_w(\text{evidence}\,\vert\,\text{trust}) = \frac{1}{\sqrt{2\pi\sigma_U{}^2}} e^{-\frac{(\omega-t)^2}{2\sigma_U^2}}$ | d. $\sigma^2(t) = \left(\frac{\sigma_0^2\sigma_U^2}{\sigma_0^2+\sigma_U^2}\right)$ |

**Table 2. Conjugate prior-posterior Gaussian-Gaussian distributions. a) Prior willingness trust distribution b) Likelihood (evidence) distribution) c) Expected willingness trust d) Variance willingness uncertainty.**

With the expected trust and uncertainty for both willingness and competence, we can assign one of a several trust categories for each trustee. A particular threshold can be set or established to determine whether or not a particular expected trust or uncertainty is “high” or “low”. In terms of modeling, this may represent one’s propensity to trust (some individuals may have a lower/higher threshold for what behavior is acceptable). We have the following trust categories with the following properties of the trustee with regard to trust:

- Trusted Discriminating (TD): both competent and willing
- Trusted Unknown (TU): competent, but willingness is not known with high certainty
- Trusted Nondiscriminating (TNd): willing but competence is uncertain
- Distrust/Untrust (DT): low competence
- No Opinion (NOp): undefined combinations of competence and willingness (other categories / personalities could be defined

The combinations of these trust dimensions and determination of trust categories is illustrated in Figure 2. In each trust evaluation period, a trustor will have some estimate of competence and willingness for each of its neighboring nodes. These estimates will include both an expected value (tc, tω) and a variance ($\sigma^2$(tc), $\sigma^2$(tω)) as described in Tables 1 and 2. Additionally, each node will have a threshold value to assess whether a node has either high (h) or low (ℓ) competence or willingness. Evaluation of the four high/low estimates enables each trustor to assign a particular trust category to each of its neighbors. Given these trust categories or personalities, the trustor may choose to adapt its behavior based on these categories.



$(t\omega, \sigma^2(t\omega))$

| $(tc, \sigma^2(tc))$ | hh | hℓ | ℓℓ | ℓh |
|---|---|---|---|---|
| hh | NOp | TU | NOp | NOp |
| hℓ | NOp | TD | NOp | NOp |
| ℓℓ | NOp | TNd | DT | NOp |
| ℓh | NOp | TU | NOp | NOp |

**Figure 2. Explanation of Trust categories given competence and willingness trust expectation and uncertainty.**

The following ELICIT decision behaviors can be adapted based on trust categories of its neighbors:

- *Sharing behavior*: Nodes may choose to only share with certain trust categories. Alternatively, nodes may give preference to Trusted Discriminating nodes by sharing with them first. With any remaining time it may have, the node will send to nodes with other trust categories. As sending factoids in this scenario and model is one way to gain trust, it may be important for nodes to transmit information to improve other node's trust in them.
- *Processing order*: Understanding of who is providing useful information will enable nodes to give priority or ignore nodes with whom the trustor node is aware of their behavior. In the inbox, a node may sort their unprocessed factoids according to the trust levels of who sent them the factoid. If the path information is available, some combination of senders could be used to determine processing order.
- *Posting behavior*: Nodes can use the websites to post factoids. If a node has particular trust or confidence that other nodes also pull information from the websites, they may post factoids to the websites. Also, if they believe that the websites are more reliable means to get information to other nodes, then this may cause the nodes to post. This formulation has not been completely described for website interactions. These interactions can be considered to be centralized and one-to-many communications. However, competence may be a measure of the redundancy of the factoids posted to the website and willingness a measure of the perceived frequency of nodes pulling from particular websites. Given this trust evaluation, a trustor node could evaluate website interactions along with one-to-one sharing interactions.

These behaviors can be implemented into the agent configuration within ELICIT. Performing appropriate experiments will acquire greater understanding of trust between entities and its impact on gaining shared situation awareness as well as more efficient and accurate decision-making.

## 5. Implementation of trust capability into ELICIT

As part of the current effort, ELICIT was modified so that each participant maintains a matrix of their levels of trust in each of the other participants, using the trust model defined in this paper. This trust implementation also allows baseline trust levels to be individually configurable. A total of nine new agent trust configuration variables were added. These include initialization values for the willingness and competence trust level components, as well as thresholds for these values and the frequency with which trust levels are recalculated.  A sample configuration is provided below.

```
willingness|Willingness trust level|0.5
uncertaintyWillingness|Uncertainty of willingness trust|0.5
competence|Competence trust level|0.5
uncertaintyCompetence|Uncertainty of competence trust|0.05
willingnessThreshold|Willingness trust level threshold|0.5
uncertaintyWillingnessThreshold|Uncertainty of willingness trust
threshold|0.03
competenceThreshold|Competence trust level threshold|0.5
uncertaintyCompetenceThreshold|Uncertainty of competence trust threshold|0.03
recalculateTrustLevelDelay|Time interval to recalculate trust|300000
```

The optional ELICIT agent audit trails were modified so that they would record each time the new trust calculations were made and the results of those calculations.  Thus we are now able to observe the software agents levels of trust awareness at all times in an exercise. This new functionality is available as part of ELICIT v2.6.

## 6. Future capabilities

Now that the ELICIT agents have a sophisticated model of trust, the next phase is for the agent software to be enhanced so that agents can be configured to vary their behavior based on their level of trust of other individual participants.  The next step of the process is to design how agent behavior can vary based on an agent's trust of other entities. Some of the factors being considered include varying what trust levels affect behavior, and identifying how behaviors vary with trust. In designing this new agent behavior we plan to draw on observed behavior in humans performing tasks in ELICIT as well as other trust work done at ARL. In some human ELICIT exercises, persons reciprocate sharing of important information, and want to punish persons who spam the group with redundant information. It may be that participants share more directly with trusted parties.  If one has low trust in a group, but not distrust, it may be that people redundantly share in the hope of finding one competent receiver. We will map out our configurable model and instantiate it in ELICIT.

## 7. Conclusion:

By building upon previously validated models, this resulting model now allows trust to be evaluated as a component of  sharing strategy and for trust to be included in ELICIT's modeling of C2 maturity levels. Implementation and validation of this trust model in ELICIT has not yet been completed. Implementation of the trust model will likely drive further refinement of t the proposed trust models for potential implementation in ELICIT. We expect that this trust model will show an enhanced efficiency in attaining situation awareness / correctness in ELICIT experiments. The agents will be able to process information more quickly and gain an understanding of the performance of the organization to determine with which nodes to interact. The efficiency will be characterized in terms of total communications required to gain particular levels of correctness in the ELICIT task. Additionally, past work has studied the presence of hoarding nodes in ELICIT and measured the impact of these behaviors on overall performance of the organization. Using trust, this may be a countermeasure to mitigate the negative impact of the presence of misbehaving nodes in the organization.

## Bibliography

[Morgan 2008] R. Morgan, “Company Intelligence Support Teams,” Jul-Aug 2008 Armor Magazine, 2008.

[Morgan 2008] R. Morgan Company Command - Building Combat-Ready Teams: Scorpion Reflections,” ARMY Magazine, Volume 58 Number 8, August 2008.

[NSCTA 2012] Network Science CTA Retrieved February 20, 2012, [Online] http://www.ns-cta.org/ns-cta-blog/.

[DOD CIO 2012] Department of Defense Chief Information Officer Retrieved February 20, 2012, from http://dodcio.defense.gov/policy/datastrategy.shtml.

[Powley, 2009] E. Powley, M. Nissen, “Trust-Mistrust as a Design Contingency: Laboratory Experimentation in a Counterterrorism Context,” Proceedings 14th International Command & Control Research & Technology Symposium, Washington, DC, June 2009.

[Powley 2010] E. Powley, M. Nissen, J. Seykora, “Study of Trust as an Organizational Contingency, Part II: Examining Four Dimensions of Trust in ELICIT Experimentation,” proceedings 15th International Command & Control Research & Technology Symposium , June, 2010.

[Lee 2004] J. D. Lee and K. A. See, “Trust in automation: Designing for appropriate reliance,” Human Factors, 2004.

[Manso, 2011] “N2C2M2 Validation using abELICIT Design and Analysis of abELICIT runs and comparison with human runs,” Naval Post Graduate School Center for Edge Power, 2011.

[Manso, 2012] “Measuring Agility in ELICIT Design and Analysis of Experiments”, Naval Post Graduate School Center for Edge Power, 2012.

[Mayer 1995] R. Mayer, J. Davis, and F. Schoorman, “An integrative model of organizational trust,” Academy of Management Review, vol. 20, 1995.

[Rempel 1995] J. Rempel, J. Holmes, and M. Zanna, “Trust in close relationships,” Journal of Personality and Social Psychology, vol. 49, no. 1, 1995.

[Schlichter 2011] ,John, McEver, Jimmie, Hayes, Richard, “Maturity Frameworks for Enterprise Agility in the 21st Century” OPM Experts, Inc. 20110

[Cho 2010] J. Cho, A. Swami, and I. R. Chen, “A survey on trust management for mobile ad hoc networks,” IEEE Comm. Surveys and Tutorials, 2010.