International Journal of Cyber Society and Education
Pages 127-148, Vol. 5, No. 2, December 2012
doi: 10.7903/ijcse.1101

ON THE OFFENSE: USING CYBER WEAPONS TO INFLUENCE COGNITIVE BEHAVIOR

Preethi Vinayak Ponangi
Wright State University
3640 Colonel Glenn Highway, Dayton, OHIO, USA – 45435
vinayakponangi@gmail.com

Phani Kidambi
Wright State University
3640 Colonel Glenn Highway, Dayton, OHIO, USA – 45435
phani.kidambi@wright.edu

Dhananjai Rao
Miami University
Oxford, OHIO, USA – 45056
dmadhava@djrao.com

Narasimha Edala
Wright State University
3640 Colonel Glenn Highway, Dayton, OHIO, USA – 45435
nedala@gmail.com

Mary Fendley
Wright State University
3640 Colonel Glenn Highway, Dayton, OHIO, USA – 45435
mary.fendley@wright.edu

Michael W. Haas
Air Force Research Laboratory
2510 Fifth St., Building 840, Wright-Patterson AFB, OHIO, USA – 45433
Michael.Haas@wpafb.af.mil

S. Narayanan
Wright State University
3640 Colonel Glenn Highway, Dayton, OHIO, USA – 45435
s.narayanan@wright.edu

ABSTRACT

There is an increasing recognition that cyber warfare is an important area of development for targeting and weaponeering, with far-reaching effects in national defense and economic security. The ability to conduct effective operations in cyberspace relies on a robust situational awareness of events occurring in both the physical and information domains, with an understanding of how they affect the cognitive domain of friendly, neutral, and adversary population sets. The dynamic nature of the battlefield complicates efforts to understand shifting adversary motivations and intentions. There are very few approaches, to date, that systematically evaluate the effects of the repertoire of cyber weapons on the cognitive, perceptual, and behavioral characteristics of the adversary. In this paper, we describe a software environment called Cognitive Cyber Weapon Selection Tool (CCWST) that simulates a scenario involving cyber weaponry.

This tool provides the capabilities to test weapons which may induce behavioral state changes in the adversaries. CCWST provides the required situational awareness to the Cyber Information Operations (IO) planner to conduct intelligent weapon selection during weapon activation in order to induce the desired behavioral change in the perception of the adversary. Weapons designed to induce the cognitive state changes of deception, distraction, distrust and confusion were then tested empirically to evaluate the capabilities and expected cognitive state changes induced by these weapons. The results demonstrated that CCWST is a powerful environment within which to test and evaluate the impact of cyber weapons on influencing cognitive behavioral states during information processing.

Keywords: Cyber Warfare, Cognitive Warfare, Cognitive Cyber Weapon Selection Tool, Distraction, Deception, Confusion, Deceit

INTRODUCTION

Either driven by political, personal or monetary motives, computer hackers create havoc in cyber space by stalling online activities using tactics which are difficult to anticipate and defend. A recent threat to information and network security was witnessed in a series of attacks by the hacker group "AnonOps" in retaliation for Julian Assange's case of Swedish extradition. This group attracted thousands of individuals through Twitter, Facebook, online forums, chat groups etc.; one could download software from their website that could turn any normal Windows or Macintosh Computer into a weapon to launch a full scale Distributed Denial of Service (DDOS) attack (Georgina & Pelofsky, 2010). Their targets were Visa and MasterCard, the world's most reputed credit card payment companies. Attack on these corporate websites has raised new questions about credit and personal information and online safety.

According to a report by the Internet Crime Complaint Center (ICCC), there were almost 336,655 complaints submitted to ICCC and a total dollar loss of $559.7 million for the year 2009. There is, therefore, a critical need to defend cyber-attacks, which have become an expensive menace for online businesses. According to the CSI Computer Crime and Security Survey (2008), as we move towards a business-oriented web, it is imperative to develop and estimate possible future cyber attacks. In the Department of Defense, cyber warfare is an important area of development for targeting and weaponeering, with far-reaching effects in national defense and economic security (Hutchinson & Warren, 2001).

Cyber attackers have a wide plethora of weapons to choose from, and the intensity and effect of an attack generally depends on the motives of the attacker. Every system is inherently susceptible to vulnerabilities, and the knack of a hacker often lies in identifying and exploiting these vulnerabilities effectively. In a real-world cyber warfare scenario, the attacker has the "swift attack" advantage. The unsuspecting cyber administrator is often caught by surprise, and the attack generally doesn't last for more than a couple of minutes, which makes it hard to track down the attacker or to initiate incident response.

The priorities of hackers have changed significantly, from the intention to exploit computer vulnerabilities to exploiting humans and their operation constraints and vulnerabilities. For example, although it might be very difficult to actually gain control of a user's system by accessing open ports in a highly protected system, it is fairly easy to trick him/her to compromise their personal information or their passwords by masquerading as an authentic source.

Although deception and psychological operations are being used as a part of Department of Defense tactics, there are very few approaches that systematically evaluate the effects of the repertoire of cyber weapons on the cognitive, perceptual, and behavioral characteristics of either friendly or adversary forces (Rowe, 2006). Effort has been invested to better understand adversarial intent and motives by attracting hackers to specific systems called "honeypots" (Provos, 2004). There have been efforts in the form of "red teams," which simulate the cyber warfare environment and observe cyber terrorist behavior in a cyber-warfare simulated setup (Wood & Duggan, 2002). However, research of this kind has often focused on compromising vulnerabilities of hardware and software technologies. There has been no effort to understand the cognitive vulnerabilities associated with cyber-attacks. There is little knowledge in terms of the psychological effects caused by these weapons and using these weapons for the purpose of a cyber attack. A test bed is needed to evaluate and map cyber weapons to their respective cognitive characteristics within a real-time cyber attack scenario and to observe user reactions under those cognitive states.

This research explored and mapped the possible perceptual changes to their respective cognitive weapons when used in a particular use-case scenario in information processing. The Cognitive Cyber Weapon Selection Tool (CCWST) tool was developed to simulate a cyber- warfare scenario, where the cyber administrator can deploy and activate certain cognitive weapons at will on the adversary's computer. The objective was to monitor and evaluate the performance of the cognitive weapons and to observe if the desired cognitive changes were present in the adversaries. The overall architecture of CCWST, related research on cyber weaponry, and an empirical evaluation using the tool are described in this paper.

LITERATURE REVIEW

The increasing pervasiveness of information in American society and in various functional areas has triggered Department of Defense (DOD) to make Information Warfare a separate part of its warfare division.

According to Mollander, Riddile, and Wilson (1996) "Information Warfare (IW) represents a rapidly evolving and, as yet, imprecisely defined field of growing interest for defense planners and policy-makers." There is no formal definition for the term "Information Warfare." Information Warfare is often referred to as a collection of different techniques used as a part of Information Operations. Cyber-terrorism according to Lewis (2003) is "The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."

"Malware" includes tools that are used with the intent of gaining access to the user's systems so as to monitor and extract personal information from the users' computers. Designing firewall and anti-malware software has become a herculean task for the anti-malware designers, owing to the various versions of the same virus which surface on the internet (Carvey, 2005; Cuadra, 2007; Jha & Christodorescu, 2004; Heron, 2008).

A prominent reason for cyber-attacks being so highly successful is that these attacks target the "weakest link" in the cyberspace: the unsuspecting user (Karvonen, 2001). Such deception could be used in both offensive and defensive ways, according to Rowe (2004). "Deception is a two agent psychological phenomenon. When used offensively, the attacker might try to fool our information systems into giving away secrets or destroying themselves, or it could be used defensively where a computer pretends by exaggerated processing delays to succumb to denial-of-service" (Rowe, 2004). Cyber adversaries have long since used deception as a means to attack network systems and in the opinion of Rowe (2004) it is only appropriate to return in kind. As the deception should be believable, it is extremely important to use the appropriate context sensitive deception technique on the attacker.

There are very few approaches to date that systematically evaluate the effects of the repertoire of cyber weapons on the cognitive, perceptual, and behavioral characteristics of either friendly or adversary forces (Rowe, 2006). While isolated studies on defensive deception planning for cyber-attacks have led to experimentation test beds (Rowe, Custy, & Duong, 2007), there is a need for a computerized system that can serve as both a

repository of knowledge on the spectrum of cyber weaponry and their effects tied to the state-of-the-art research literature on cognition, human performance, decision making, and behavioral science (Pew & Mavor, 1998).

Cyber Warfare Models

Several models have been proposed to predict and observe cyber-attack scenarios. Such literature could be broadly classified into four areas of research. The four categories which contribute to research literature in the area of cyber warfare are red team efforts, simulations, test beds and honeypots.

Red team efforts have been developed to assess and identify critical vulnerabilities in a system by observing attackers and defenders within a cyber environment (Wood & Duggan, 2000; Benzel, Braden, Faber, Mirkovic, Schwab, Sollins, & Wroclawski, 2009).

Using simulation to model and predict adversarial intentions through automatic agents is another area of research in cyber warfare literature that generates simulated data, which could then be used to generate multiple cyber-attack scenarios (Chaturvedi, Gupta, Mehta, & Yue, 2002; Kotenko, 2005; Vejandla, Dasgupta, Kaushal, & Nino, 2010; Kuhl, Kistner, Costantini, & Sudit, 2007).

Evaluating internet attacks in an experimental environment needs a near - equivalent simulation of the entire internet, and modeling and simulating such a network is not an easy task (Floyd & Paxson, 2001). Several test beds have been developed since the advent of cyber warfare attacks (Floyd & Paxson, 2001; Davis, Tate, Okhravi, Grier, Overbye, & Nicol, 2006; Benzel, Braden, Kim, Neuman, Joseph, Sklower, Ostrenga, Schwab, 2007; Van Leeuwen, Urias, Eldridge, Villamarin, & Olsberg, 2010) and are often driven by specific objectives.

According to a definition by Spintzer (2004), a honeypot is defined as "an information system resource whose value lies in unauthorized or illicit use of that resource." The idea of a honeypot is to attract cyber attackers to compromise a particular pre-selected system and generate logs and monitor system information for later anaylsis in order to gain insight into cyber attacker patterns. Some of the advantages of honeypots include distracting attackers from valuable information, generating warnings in the instance of a compromise, and enabling detailed analysis of hacker exploitation of system vulnerabilities (Provos, 2004). Since setting up a honeypot is often a time consuming and expensive process, Provos (2004) proposed a virtual honeypot framework which simulates the modeled behaviors or an attacker. These behaviors are often collected by studying

previous honeypot data.

Although several of these models have been used for research in the areas of system vulnerabilities and attack types, there isn't any research in the field of cognitive cyber weapons which is capable of inducing alterations in the cognitive thought process of an adversary. This research specifically aims at answering this question by developing a relevant test bed and evaluating the effects of such cognitive weapons through an experiment.

ARCHITECTURAL FRAMEWORK

The CCWST Framework is based upon a distributed software platform that has the ability to manage and monitor multiple computers at any given time. Given the issues of scalability and maintainability for a distributed set up, it was essential to design a robust framework which was extensible and easy to use in information-processing scenarios. In the CCWST framework, it was assumed that there would be a central operator or a group of central operators to monitor and deploy weapons to an adversarial computer with an intention to induce behavioral, cognitive and psychological changes in an adversary.

Two critical functionalities are built into the framework: the ability to monitor and control the adversarial computer for both reconnaissance and warfare operations and to catalog a large arsenal of context-specific weapons that can alter information on specific software suites generally used by an adversary. There are two major components of the CCWST: Keyhole and Genie. Keyhole acts as the "eyes" for the cyber operator, who can constantly monitor adversarial moments, and Genie is a cyber-weapon arsenal from which the operator chooses, so as to deploy relevant cyber weapons onto an adversary's computer. The two components together bridge the gulfs of execution and evaluation between the CUAs (Computers under Attack) and the operator. Figure 1 illustrates the CCWST framework. The framework assumed that the CUAs were already compromised and hence the complexities involved in intruding adversary systems were not accounted for as a part of this research.

The CCWST is a distributed system with various semi-autonomous subcomponents, operating asynchronously on various computers. The independent subcomponents interact with each other via network interconnects using customized application-layer protocols. The underlying interconnect is a standard wired communication channel that supported conventional access to network resources, including the Internet. The customized,

application-layer protocols enabled various subsystems to coordinate their activities with each other to achieve the desired functionality.

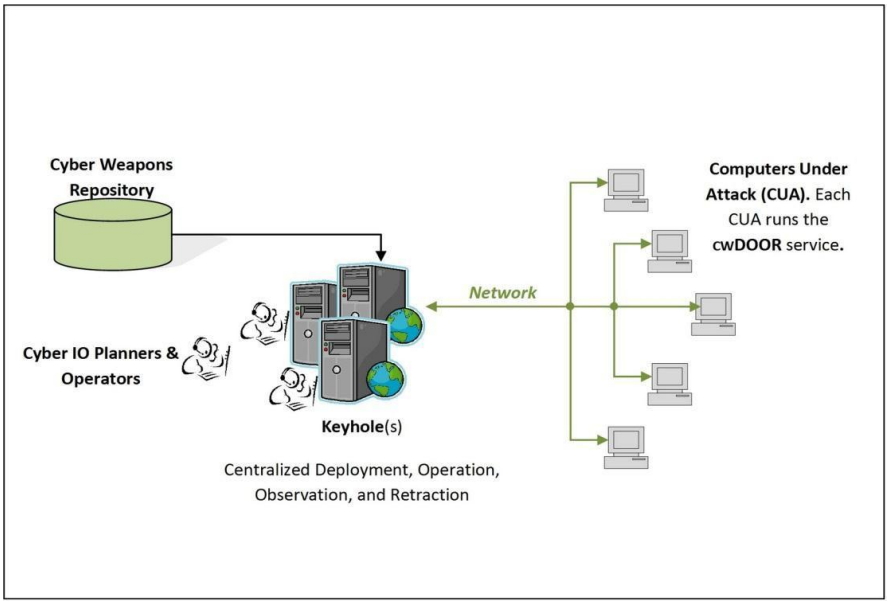

Figure 1 High-Level Overview of the CCWST Software System Illustrating the Major Subsystems

Keyhole

Keyhole gives the sensory stimulus to monitor and trigger actions on CUAs. It provides the Cyber operator the capability to observe, deploy and manage cyber weapons on CUAs. It is a non-obtrusive subsystem that masquerades as a windows system process to monitor adversary activities, and it relays this information back to the Keyhole on the operator's computer. The distributed, asynchronous nature of CCWST required the system to be partitioned into several independent software subsystems. A functional analysis of the overall system yielded an effective delineation into the following three subsystems: Cyber Weapons; Keyhole Graphical User Interface; and Cyber Weapons Deployment, Operation, Observation, and Retraction (cwDOOR) Service

1. Cyber Weapons

In the context of this research, the term "Cyber Weapon" is used to refer to a well-defined unit of software that is capable of potentially impacting and inducing changes

in the cognitive, perceptual, and behavioral aspects of an adversary. As an integral part of CCWST, we developed a variety of weapons that target different classes of software, such as browsers, word processors, spreadsheets, and general-purpose editors. In the following subsection, we primarily focus on the generic life cycle and operations that pertain to all cyber weapons used by CCWST.

2. Keyhole GUI

The Keyhole software subsystem has been designed to provide a user-friendly and intuitive Graphical User Interface (GUI) for a cyber IO planner to perform various tasks associated with impacting the behavior of an individual or a team of adversaries. Keyhole has the ability to deploy, activate, de-activate and retract weapons on and from the adversarial computers using the Keyhole Graphical User Interface. It lists all the computers under attack on the left-hand pane, as well as the state of the weapons on these computers. The central screen relays screenshots of the computers under attack at regular intervals. This provides robust situational awareness to the administrator of Keyhole, giving him/her the time to activate weapons based on adversary specific actions.

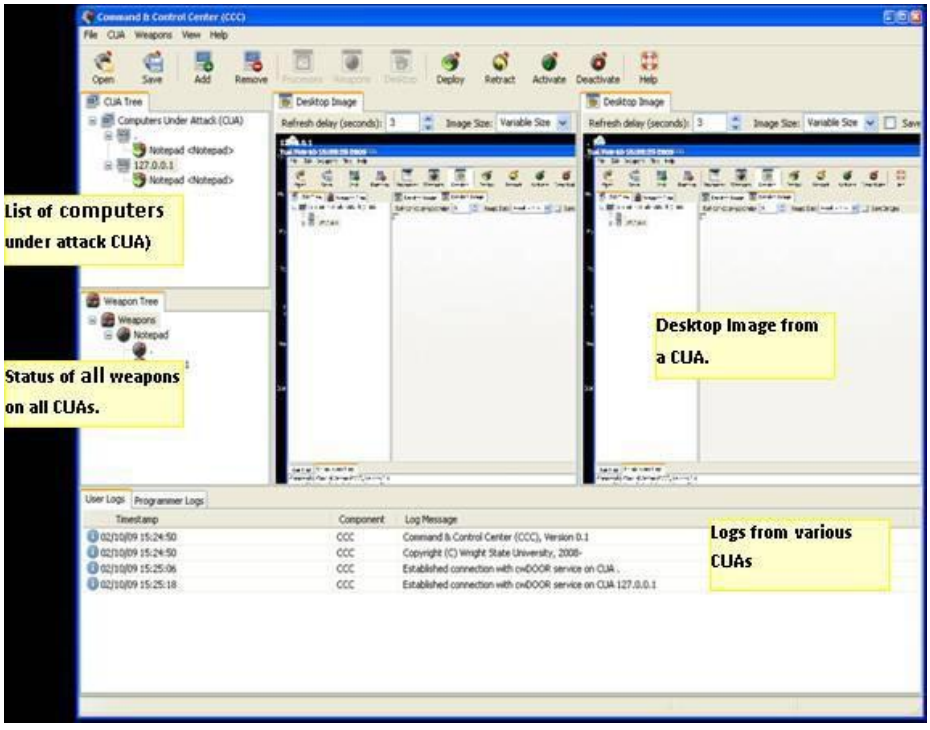

Figure 2 Snapshot of the Keyhole GUI

3. cwDOOR Service

cwDOOR Service is an acronym for Cyber Weapons Deployment, Operation, Observation, and Retraction Service. The primary functionality of the cwDOOR service is to act as a backdoor on each Computer under Attack (CUA).

Genie

Genie is the suite of client-side plug-ins (weapons) that execute on the target computer, presumably on command. The Keyhole daemon model encompasses two customized Genie modules that operate in the context of the user's IE browser (IEGenie) and Microsoft Excel (ExcelGenie). Office Genie is the cyber weapon designed to spy and invokes content attacks in Microsoft Office applications. Office acts as a terminal window for the adversary to compile, author, and exchange information. The three Genies together manipulate environments where adversaries presumably consume, analyze, and author information.

IEGenie manipulates the web pages and document object model for targeted content attack on the CUA. The hyperlinking structure on the web makes it easy to follow information trails for the users, but it also poses a unique challenge to tools such as IE Genie that are designed for content attacks. IE Genie is implemented as a single-cell, finite state automaton that uses a custom XML grammar to define and execute actions in the browser's context to memorize and tailor deception over a prolonged session spread across different web pages. ExcelGenie manipulates content and metadata associated with Excel spreadsheets on the adversary’s computer. The changes can be manifested either upon opening a worksheet, can create an illusion of data, or upon publishing the worksheet can permanently alter the data. OfficeGenie is similar to ExcelGenie in that it alters the content of the documents opened or generated by the adversary, but it also alters content in either Microsoft Word or Microsoft Outlook, thereby covering both the publishing and communication fronts of the adversary.

COGNITIVE OR BEHAVIOURAL CHANGES

The next step was to identify the behavioral changes that could be caused by CCWST so as to disrupt adversaries in a cyber-warfare scenario. These behavioral changes had to be decided by the Keyhole operator in real time, based on predictive reconnaissance data constantly relayed to the operator through Keyhole. We identified the following as potential behavioral changes that could be induced as a disruption in the adversary’s

thought process:

- **Deception:** To deceive the adversary by displaying non-existent or incorrect data on the adversary's screen.
- **Distraction:** To distract the adversary and delay his/her objective in the form of tempting pop-ups.
- **Distrust:** Create distrust in the adversary by causing situations where the adversary would mistrust the information provided by the system.
- **Confusion:** Create situations where the adversary would be confused by the information presented through a CCWST compromised system.

Rowe (2004) suggests that cyber offense would allow understanding of the nature and intent of the attack by causing a distraction on decoy information. However, this type of offensive attack would be possible only if the cyber operator has a constant situational awareness feed from the adversarial system so that his behavioral, cognitive and perceptual characteristics can be assessed accurately.

A scenario was selected where deploying Genie weapons could impact a specific task in the way intended by the Keyhole operator. A typical information retrieval situation was considered as a good test environment for empirical evaluation of CCWST. A scenario where two users would choose an airfare ticket was selected for evaluating the effectiveness of the CCWST weapon suite. Teams of two participants were asked to plan and finalize a travel itinerary (for a 1-day trip to occur in 6 months) consisting of airline travel and lodging information from Columbus, Ohio to Cincinnati, Ohio.

The users were permitted to use only Internet Explorer, their email clients, and Microsoft Excel for documenting the details of the itinerary. Table 1 gives the name of the weapon, the classification of the functionality of the weapon and a brief description of the weapon's capability to induce behavioral changes.

Most methods of evaluation require some kind of an interaction with the user, but in the case of the CCWST, the objective of testing the user would be lost without providing a significant amount of detail regarding the software and its purpose. Therefore, an alternative approach had to be adopted to test and evaluate a surreptitious software program like the CCWST. We identified a set of metrics that could be closely correlated to user behavior. The following metrics were identified to be good indicators of user behavior and useful predictors of change in the cognitive thought processes of the user. The metrics are listed as follows:

- Number of Emails exchanged: The total volume of e-mails exchanged by the individuals in a group for a particular task. This was considered to be the sum of the number of emails sent and received by any one individual of a group.
- Number of Repetitions: The number of times the individuals revisit and repeat searches for a given task.
- Time to Complete a Task: The total time taken by both the individuals in a group to collaboratively complete a task.
- Confidence Rating: The level of confidence of the individual participant after each task in the experiment. The participants were asked to rate their level of confidence after each task in the experiment on a scale of one to ten.
- Error Rate: The number of errors committed by an individual during completion of the task.

Table 1 Proposed Cyber Weapons

Proposed Cyber Weapon	Classification	Brief Description
Genie – Air Fare Changer	Social Psychology & Incorrect Information	This cyber weapon changes air faces published on various websites to different values causing adversaries to get confused as they will be viewing different costs for the same air routes.
Genie – Air Fare Deceiver	Incorrect & Phantom Information	This cyber weapon introduces a new (but non-existing) air route with attractive pricing options to attempt and deceive the adversaries in choosing this non-existing air route.
Genie - Adware	Incorrect Information & Visual Perception	The cyber weapon will attempt to distract the user by placing advertisements and notices in various web pages with attractive slogans to distract the adversaries.
Keyhole – Message Box	Incorrect Information	This cyber weapon pops us additional messages on the adversaries' computer causing them to get distracted.

Table 2 Metrics to Measure Cognitive State

Cognitive State	Confidence	Error Rate	Expected Response Time	Repetition to Validate
Confusion	Lower	Higher	Higher	Yes
Deception	Normal	Higher	Normal	Normal
Distraction	Normal	Higher	Higher	Normal
Distrust	Lower	Higher	Higher	Yes

Table 2 shows the relationship of each metric with the cognitive state of the individual completing the task. Work by De Paulo, Charlton, Cooper, Lindsay, and Muhlenbruck (1997) showed a correlation in confidence with perception of truthfulness; people are confident in their judgments when they decide that a message is truthful, regardless of whether it actually is or not. Therefore, we posit that a state of distrust or confusion on the part of the operator is associated with a lower confidence level. Research has shown that humans have difficulty recognizing false information, so in response, they automatically consider alternative meanings of the stimulus (Schul, Mayo, & Burnstein, 2004). This results in a higher error rate and response time, along with a lower confidence level. Humans also follow regular routines when they feel no need to distrust information; this behavior changes when they are experiencing distrust (Schul, Mayo, & Burnstein, 2008). We use the metric of increased repetitions from the normal state to indicate this status. A state of confusion indicates that an operator does not know how to interpret a given stimuli (Hess, 2003), so their actions in this study would reflect this state by having a lower confidence level, higher error rates, and longer response time, and they would frequently repeat exposure to the stimuli to validate their assumptions. Distraction has been widely studied in the area of driving and safety, and one metric used is the amount of time spent looking at a stimulus not relevant to completion of the primary task (Martinelli, Medellin, & Akuraju, 2008); this would lead to a higher response time and possibly a higher error rate within this study.

EMPIRICAL EVALUATION

Participants

Twenty participants between the ages of 18 and 46 were tested in this experiment. To be considered for the study, the participants were required to have normal or corrected-to-normal acuity; fairly comprehensive knowledge about Windows-based applications, including Microsoft Excel; the ability to search and retrieve information from the Internet; and familiarity with operating a mouse and a keyboard. Out of the 20 participants, 12 were male and 8 were female. One participant was below 20 years of age, one participant was above 40 years of age, and the rest of the participants were between the ages of 20 and 40.

Apparatus

A total of five computers were used for the experiment. Four of these computers, with minimum components of an Intel Core 2 CPU and 1 GB RAM, were set up at four different subject stations, and a computer which monitored all these stations was set up at a "control" station. The "Keyhole" software, which monitors and facilitates the deployment, activation, de-activation and retraction of cyber weapons, was installed on the computer at the control station, which contained an Intel Core 2 Duo CPU and 3 GB of RAM. Cyber weapons were deployed on the subjects' computers in the Experiment Group prior to the experiment. There were no cyber weapons deployed on the subjects' computers in the Control Group. Internet Explorer 7 was the standard browser used on all the computers at the subject stations in the experiment.

Procedure

The experiment was a "between subject design," with two levels of the Group (Non-Weapon and Weapon) as the independent variable. A participant was considered to be in the Non-Weapon (NW) Group if the participant performed the experiment on a computer which had no cyber weapons installed. A participant was considered to be in the Weapon (W) Group if the participants had cyber weapons installed on their computers.

RESULTS

The tasks conducted, the hypothesis for each task, the statistical results, and the summary have all been illustrated in Tables 3, 4, 5, and 6 for Distraction, Confusion, Deception and Distrust.

The results from the confusion scenario were found to be consistent with the hypothesis predicted. Hence, we can conclude that the total number of repetitions for the Weapon (W) group were greater than the total number of repetitions of the No Weapon (NW) group. This suggests that the participants of the W group needed a greater number of repetitions to confirm their values and repeated each task a greater number of times when compared to the NW group.

The user confidence was shown to be greater in the NW group when compared to the confidence of participants in the W group. This indicates that for the scenario related to confusion, the user confidence was lower when weapons were activated on the participants' computers in the W group when compared to the NW group.

The results from the deception scenario were found to be consistent with the variance in the metrics that the research team developed to identify a user who was potentially deceived. The results from the distrust scenario were found to be consistent with the variance in the metrics that the research team developed to identify a user who was potentially experiencing distrust in the system.

The results from scenario of distraction were not consistent with the hypothesis predicted. This might have been because although individuals took almost the same time to arrive at a consensus, there was lot of variability present depending on the subjects performing the tasks in the W group. All the participants would just ignore the pop-ups which intended to create distraction. All the participants in the W group closed all the pop-up windows and proceeded with their tasks, thus avoiding any distractions.

Table 3 Distraction Results Summary

Task	Hypothesis	Result	Summary
Experiment group was working on a specific task; several pop-up windows would appear on the screen at once, which opened several deal sites.	The time taken to complete a task in the distraction scenario would be higher in the W group when compared to the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicated a p-value of 1.94 for a one-tail two- sample t-test assuming unequal variances.	There was no significant difference between the time taken to complete tasks related to distraction in the Weapon (W) Group or the No Weapon (NW) group.
The Keyhole administrator would activate a weapon which opened a pop-up on the participant's screen that would claim to offer a better deal for the same flight that the user was searching for. If the participant chose to look at this better deal, he or she would be re-directed to a page of that particular deal site. But on looking up the specified itinerary, he or she would find out that the claim of that pop-up was actually untrue.			

Table 4 Confusion Results Summary

Task	Hypothesis	Result	Summary
The participants were asked to identify the cheapest airline ticket from Columbus to Cincinnati at http://www.travelocity.com. In the Experiment group, when the participant visited the Travelocity website, he or she was re-directed to http://www.orbitz.com. However, after repeating this task a couple of times, the participant was directed to Travelocity again.	The number of emails exchanged between the participants of the W group is greater than the number of emails exchanged in the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicated a p-value of 0.048 for a one-tail two- sample t-test assuming unequal variances.	The mean of the total number of emails exchanged in the Weapon (W) group is greater than that of the No Weapon (NW) group
When the participant searched for flights from Columbus to Cincinnati, he or she would be redirected to a search page which listed flights from Dayton to Cincinnati instead.	The number of repetitions is higher in the W group when compared to the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 5.57E-08 for a one- tail two-sample t-test assuming unequal variances.	The mean of total number of repetitions for the Weapon (W) group were greater than the mean of total number of repetitions of the No Weapon (NW) group.
	The time taken to complete a task is higher in the W group when compared to the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 0.404 for a one- tail two-sample t-test assuming unequal variances.	The mean of the total time taken to complete the tasks in the Weapon (W) group is greater than that of the No Weapon (NW) group.
	The confidence measure of W group is lesser when compared to the NW group.	A two-sample t-test for a confidence level of 95% (α= 0.05) indicate a p-value of 0.008 (<0.05) for a one-tail two-sample t-test assuming unequal variances.	The user confidence was greater in the group where weapons were not used when compared to the confidence of participants in the group where cyber weapons were used.

Table 5 Deception Results Summary

Task	Hypothesis	Result	Summary
The participants were asked to visit http://www.orbitz.com and search for flights from Columbus to Cincinnati. The objective of this task was to find the cheapest flight and document the details of the itinerary in the Microsoft Excel document provided. However, the price on the "Orbitz" website was changed to a pre-determined value that was lower than the actual price by the Keyhole administrator without the knowledge of the participants in the Experiment group. It was hypothesized that this would result in different prices being documented for the same flight by the participants of the Control group and the Experiment group.	The total number of emails exchanged within W group and total number of emails exchanged within NW group are equal.	A two-sample t-test for a confidence level of 95% (α= 0.05) indicate a p-value of 0.745 (>0.05) for a two-tail two-sample t-test assuming unequal variances.	There is no sufficient evidence to prove that the means of user confidence rating are different for the Weapon (W) Group and No Weapon (NW) Group.
The task was similar to the previous task but in this case the price was changed again on http://www.expedia.com for Experiment Group to deceive the participant into thinking that it was the actual price on the website.	The total number of repetitions within W group and total number of repetitions within NW group are equal.	A two-sample t-test for a confidence level of 95% (α= 0.05) indicate a p-value of 0.035 (<0.05) for a two-tail two-sample t-test assuming unequal variances.	The means of number or repetitions are different for the Weapon (W) and No Weapon (NW) group.

Table 5 Deception Results Summary (Cont.)

Task	Hypothesis	Result	Summary
	The task completion time between W and NW group is equal.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 0.53 (>0.05) for a two-tail two-sample t-test assuming unequal variances.	There is no sufficient evidence to prove that the means of the number of emails exchanged for the No Weapon (NW) and Weapon (W) groups are different.
	The confidence measure of participants is equal for W group and NW group.	A two-sample t-test for a confidence level of 95% (α= 0.05) indicate a p-value of 0.09 (>0.05) for a two-tail two-sample t-test assuming unequal variances.	There is no sufficient evidence to prove that the means of the total time taken to complete the tasks are not equal for the No Weapon (NW) group and the Weapon (W) group.

Table 6 Distrust Results Summary

Task	Hypothesis	Result	Summary
This scenario involved asking the participants of each group to e-mail the attachment of the final Excel document, which was modified after achieving all the tasks in the experiment. The participants were then asked to tally their document against their partner's to see if all the values matched the document. The Keyhole Administrator would activate the ExcelGenie weapon on one of the participants' computer in the Experiment Group. This would change one of the airfare to an extremely large number on the computer where ExcelGenie was activated. This would trigger the chain of emails between the individuals of the Experiment group caused by the mismatch in the airfare values.	The total number of emails exchanged within the team of participants of the W group is greater than the number of emails exchanged within the team of participants of the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 0.055 for a one-tail two- sample t-test assuming unequal variances.	The mean of the number of repetitions for the Weapon Group (W) was greater when compared to the mean of the number of repetitions of the No Weapon (NW) Group.

Table 6 Distrust Results Summary (Cont.)

Task	Hypothesis	Result	Summary
	The total number of repetitions within the team of participants of the W group is greater than the number of repetitions within the team of participants of the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 4.73E-07 for a one-tail two- sample t-test assuming unequal variances.	The mean of the number of emails exchanged within the Weapon (W) group is greater than the mean of the number of emails exchanged in the No Weapon (NW) group.
	The total time to complete the task within the team of participants of the W group is greater than the time taken to complete the task for the NW group.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 0.47 for a one-tail two- sample t-est assuming unequal variances.	There was no sufficient evidence to prove that the mean of the total time taken to complete tasks related to the distrust scenario is higher in the Weapon (W) group when compared to the No Weapon (NW) group.
	The confidence measure for the W group is greater than the NW group for the distrust scenario.	A two-sample t-test for 95% confidence (α=0.05) indicate a p-value of 0.024 for a one-tail two- sample t-test assuming unequal variances.	The mean of participant's confidence in the performance of a particular task was greater in the No Weapon (NW) group when compared to the Weapon (W) group.

SUMMARY

This paper outlined the architectural components of CCWST, a tool that can be used to create and deploy cyber weapons that can impact information processing activities of human operators. These weapons can modify the content of results from an Internet search engine, data on a spreadsheet or a Word document, and email information. As a result of these modifications, the users of these tools can become confused, may be deceived, or have more distrust in the computer system they use. Research on techniques used to penetrate computer networks or protect computer systems using cryptographic tools continues to increase. There is, however, very little research on the behavioral impacts of cyber weapons, including quantitative metrics that can systematically assess the extent to which the users' cognitive behavioral states are modified when they are exposed to cyber weapons. This paper identified cognitive behavioral states that can potentially be impacted and highlighted metrics that can identify state changes. The CCWST tool was also demonstrated as an effective tool to deploy cyber weapons and enable cognitive behavioral state changes in humans. Future research should focus on further formalizing the

definitions of cognitive behavioral states by tying those definitions to psychological literature, systematically documenting which cyber weapon has the impact to maximize the cognitive behavioral state change in specific contexts, and performing empirical evaluations in real settings.

There were a few limitations to this study. Assumptions were made during the measurement of some metrics. "Time" was defined as the aggregate time taken for both the team members to arrive at a conclusion on a particular task. The study did not analyze the time taken for each individual to complete a part of a task. The experiment also did not take into consideration the inherent ability of an individual to perform a task or previous learning associated with the task. The websites used in this experiment were not cached. This might have led to a time difference in retrieval of information based on the websites' performance for each participant. Similarly, the communication time needed to exchange emails and attachments between participants in the same team depended upon the mail servers used in this experiment.

REFERENCES

Benzel, T., Braden, B., Faber, T., Mirkovic, J., Schwab, S., Sollins, K., & Wroclawski, J. (2009, March). Current developments in DETER cybersecurity testbed technology. *Paper Presented at Cybersecurity Applications & Technology Conference for Homeland Security (CATCH '09.),* Washington, USA. doi:10.1109/CATCH.2009.30.

Benzel, T., Braden, R., Kim, D., Neuman, C., Joseph, A., Sklower, K., & Schwab, S. (2007, August). Design, deployment, and use of the DETER testbed. *Paper Presented at the DETER Community Workshop on Cyber-Security and Test,* Boston, USA.

Carvey, H. (2005). Malware analysis for windows administrators. *Digital Investigation, 2*(1), 19-22. doi:10.1016/j.diin.2005.01.006.

Chaturvedi, A.R., Gupta, M., Mehta, S.R., & Yue, W.T. (2000, January). Agent-based simulation approach to information warfare in the SEAS environment. *Paper Presented at the 33rd Annual Hawaii International Conference on System Science,* Hawaii, USA. doi:10.1109/HICSS.2000.926647.

ChristodorescuJha, M. (2004). Testing malware detectors. *ACM SIGSOFT Software Engineering Notes, 29*(4), 34-44. doi: 10.1145/1013886.1007518.

Davis, C.M., Tate, J.E., Okhravi, H., Grier, C., Overbye, T.J., & Nicol, D. (2006, September). SCADA cyber security testbed development. *Paper Presented at 38th North American in Power Symposium (NAPS 2006),* Illinois, USA. doi:10.1109/NAPS.2006.359615.

De La Cuadra, F. (2007). The geneology of malware. *Network Security, 2007*(4), 17-20. doi:10.1016/S1353-4858(07)70047-8.

DePaulo, B.M., Charlton, K., Cooper, H., Lindsay, J.J., & Muhlenbruck, L. (1997). The accuracy-confidence correlation in the detection of deception. *Personality and Social Psychology Review, 1*(4), 346-357. doi:10.1207/s15327957pspr0104_5.

Floyd, S., & Paxson, V. (2001). Difficulties in simulating the Internet. *IEEE/ACM Transactions on Networking (TON), 9*(4), 392-403. doi:10.1109/90.944338.

Heron, S. (2008). Parasitic malware: The resurgence of an old threat. *Network Security, 2008*(3), 15-18. doi:10.1016/S1353-4858(08)70032-1.

Hess, U. (2003). Now you see it, now you don't--the confusing case of confusion as an emotion: Commentary on Rozin and Cohen (2003). *Emotion, 3*(1), 76-80. doi:10.1037/1528-3542.3.1.76.

Hutchinson, W., & Warren, M. (2001). *Information Warfare: Corporate Attack and Defence in a Digital World*. Oxford: Butterworth-Heinemann.

Kotenko, I. (2005, June). Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet. *Paper Presented at 19th European Simulation Multiconference "Simulation in wider Europe, Riga, Latvia*.

Kuhl, M.E., Kistner, J., Costantini, K., & Sudit, M. (2007, December). Cyber attack modeling and simulation for network security analysis. *Paper Presented at the 39th conference on Winter simulation: 40 years! The best is yet to come*, Piscataway, NJ, USA. doi: 10.1109/WSC.2007.4419720.

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology & Policy, 16*(2), 34-41. doi:10.1007/s12130-003-1024-6.

Martinelli, D., Medellin, L., & Akuraju, N. (2008). Assessing the variation of driver distraction with experience: Phase I (No. WVU-2006-03). Mid-Atlantic Universities Transportation Center, Region III.

Molander, R.C., Riddile, A.S., & Wilson, P.A. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: RAND.

Nikander, P., & Karvonen, K. (2000). Users and trust in cyberspace. In Bruce Christianson, Bruno Crispo, and Michael Roe (Eds.), *Proceedings of the 8th International Workshop on Security Protocols* (pp.24-35). London, UK: Springer-Verlag.

Pew, R.W., & Mavor, A.S. (1998). *Modeling Human and Organizational Behavior: Application to Military Simulations*. Washington, D.C.: National Academies Press.

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.

Prodhan, G., & Pelofsky, J. (2010). *WikiLeaks backers threaten more cyber attacks*. Retrieved December 10, 2010, from http://www.reuters.com/article/2010/12/09/us-wikileaks-idUSL3E6N80HH20101209

Provos, N. (2004). A virtual honeypot framework. *Paper Presented at the 13th conference on USENIX Security Symposium,* Berkeley, CA, USA.

Rowe, N.C. (2004). Designing good deceptions in defense of information systems. *Paper Presented at the 20th Annual Computer Security Applications Conference (ACSAC'04),* Washington, DC, USA. doi:10.1109/CSAC.2004.16.

Rowe, N.C. (2006). Measuring the effectiveness of honeypot counter-counterdeception. *Paper Presented at the 39th Annual Hawaii International Conference on System Sciences,* Hawaii, USA. doi:10.1109/HICSS.2006.269.

Rowe, N.C. (2006, January). Measuring the effectiveness of honeypot counter-counterdeception. *Paper Presented at the 39th Annual Hawaii International Conference on System Sciences,* Hawaii, USA. http://dx.doi.org/10.1109/HICSS.2006.269.

RoweCustyDuong, N.C.J.T. (2007). Defending cyberspace with fake honeypots. *Journal of Computers, 2*(2), 25-36.

Schul, Y., Mayo, R., & Burnstein, E. (2004). Encoding under trust and distrust: the spontaneous activation of incongruent cognitions. *Journal of Personality and Social Psychology, 86*(5), 668-679. doi:10.1037/0022-3514.86.5.668.

Schul, Y., Mayo, R., & Burnstein, E. (2008). The value of distrust. *Journal of experimental social psychology, 44*(5), 1293-1302. doi:10.1016/j.jesp.2008.05.003.

Spitzner, L. (2001). *Know your enemy. Parts I, II, III.* Retrieved June 5, 2009, from www. linuxnewbie. org/nhf/intel/security/enemy. html

Van Leeuwen, B., Urias, V., Eldridge, J., Villamarin, C., & Olsberg, R. (2010, October). Cyber security analysis testbed: Combining real, emulation, and simulation. *Paper Presented at 2010 IEEE International Carnahan Conference on Security Technology (ICCST),* doi: 10.1109/CCST.2010.5678720.

Vejandla, P., Dasgupta, D., Kaushal, A., & Nino, F. (2010, August). Evolving gaming strategies for attacker-defender in a simulated network environment. *Paper Presented at 2010 IEEE International Conference on Social Computing/IEEE International Conference on Privacy, Security, Risk and Trust,* Minnesota, USA. doi:10.1109/SocialCom.2010.132.

Wood, B.J., & Duggan, R.A. (2000, January). Red teaming of advanced information assurance

concepts. *Paper Presented at 2000 DARPA Information Survivability Conference & Exposition,* Hilton Head, South Carolina. doi: 10.1109/DISCEX.2000.821513.