2011

Cognitive Cyber Weapon Selection Tool Empirical Evaluation

Preethi Vinayak Ponangi

Wright State University

Follow this and additional works at: http://corescholar.libraries.wright.edu/etd_all

Part of the Operations Research, Systems Engineering and Industrial Engineering Commons

Repository Citation

This Thesis is brought to you for free and open access by the Theses and Dissertations at CORE Scholar. It has been accepted for inclusion in Browse all Theses and Dissertations by an authorized administrator of CORE Scholar. For more information, please contact corescholar@www.libraries.wright.edu.
Cognitive Cyber Weapon Selection Tool Empirical Evaluation

A thesis submitted in partial fulfillment
of the requirements for the degree of
Masters of Science in Engineering

By

Preethi Vinayak Ponangi

B.E., Andhra University, India, 2007

2011

Wright State University

S. Narayanan, Ph.D., P.E.
Thesis Director

Thomas N. Hangartner, Ph.D.
Department Chair

Committee on final examination

S. Narayanan, Ph.D., P.E.

Mary E. Fendley, Ph.D.

Pratik J. Parikh, Ph.D.

Andrew T. Hsu, Ph.D.
Dean, School of Graduate Studies
ABSTRACT


Keeping in pace with the latest technological innovations in the cyber world, the misuse of this powerful infrastructure has also increased proportionally. Although a lot of recent attacks have been documented in the mainstream media, counter measures for cyber defense mechanism have only received some attention in the recent research literature. Most of the global attacks in the cyber space have proved to be carefully planned premeditated attacks.

Considering that most of these attacks are co-coordinated by humans, a new area of psychological weaponry is being investigated by the research community. This study aims to empirically evaluate the effectiveness of the cyber weapon suite of tools to deploy cognitive cyber weapons onto an adversary’s computer. The user behavior was assessed based on their performance during the experiment pertaining to each task and measures such as number of repetitions, total time taken to complete each task, total number of emails exchanged by a group and user confidence were considered to evaluate CCWST effectiveness. The results showed that the hypotheses were supported thereby reinforcing the effectiveness of CCWST as a powerful tool to induce cognitive changes in an adversary’s thought process.
TABLE OF CONTENTS

1. INTRODUCTION .............................................................................................................. 1
   1.1. Background .................................................................................................................. 1
   1.2. Information Warfare ...................................................................................................... 4
   1.3. Problem ....................................................................................................................... 7
   1.4. Approach .................................................................................................................... 8

2. LITERATURE REVIEW .................................................................................................... 12
   2.1. Introduction ................................................................................................................ 12
   2.2. Types of Cyber Weaponry ............................................................................................. 13
       2.2.1. Adware .................................................................................................................. 15
       2.2.2. Spam .................................................................................................................... 15
       2.2.3. Cookie ................................................................................................................... 15
       2.2.4. Trojan .................................................................................................................. 15
       2.2.5. Phishing ................................................................................................................ 16
       2.2.6. Denial of Service (DOS) & Distributed Denial of Service (DDOS) ......................... 16
   2.3. Cyber Warfare Models .................................................................................................. 20
       2.3.1. Red Team Efforts .................................................................................................. 21
       2.3.2. Simulations .......................................................................................................... 22
       2.3.3. Test Beds ............................................................................................................. 24
       2.3.4. Honeypots ............................................................................................................ 25

3. CCWST DESIGN AND FRAMEWORK ....................................................................... 26
   3.1. Introduction to Cognitive Cyber Weapon Selection Tool (CCWST) Framework .......... 26
   3.2. Keyhole ..................................................................................................................... 28
       3.2.1 Cyber Weapons ...................................................................................................... 28
           3.2.1.1. Life Cycle of a Cyber Weapon ........................................................................ 29
       3.2.2. Keyhole GUI ....................................................................................................... 32
       3.2.3. cwDOOR Service ................................................................................................. 35
   3.3. Genie .......................................................................................................................... 36
       3.3.1. IE Genie .............................................................................................................. 36
       3.3.2. Genie Rule Grammar ........................................................................................... 38
       3.3.3. Microsoft Office Genie ....................................................................................... 40
3.4. Genie Rule Designer and Test Toolkit ................................................................. 41
3.5. Genie Demonstration Scenario ................................................................. 41

4. RESEARCH METHODOLOGY ................................................................................. 45
4.1. Introduction ........................................................................................................ 45
4.2. Cognitive or Behavioral Changes ..................................................................... 46
4.3. Scenario Objective ............................................................................................. 47
4.4. Experimental Design ......................................................................................... 51
   4.4.1. Variables: ..................................................................................................... 51
   4.4.2. Participants ................................................................................................. 51
4.5. Experimental Setup ............................................................................................ 52
4.6. Scenarios employed to determine Distraction, Confusion, Deception, and Distrust... 52
   4.6.1. Scenario to Assess Distraction ................................................................. 52
   4.6.2. Scenario to Assess Confusion ................................................................. 55
   4.6.3. Scenario to Assess Deception ................................................................. 56
   4.6.4. Scenario to Assess Distrust ..................................................................... 57

5. RESULTS AND DISCUSSION ............................................................................... 60
5.1. Results for the Scenario to assess Distraction ................................................. 60
   5.1.1. Hypothesis (1) .......................................................................................... 60
5.2 Scenario to assess Confusion ............................................................................. 61
   5.2.1. Hypothesis (2) .......................................................................................... 61
   5.2.2 Hypothesis (3) ........................................................................................... 62
   5.2.3 Hypothesis (4) ........................................................................................... 63
   5.2.4 Hypothesis (5) ........................................................................................... 64
5.3 Scenario to assess Deception ............................................................................. 65
   5.3.1 Hypothesis (6) .......................................................................................... 65
   5.3.2 Hypothesis (7) .......................................................................................... 66
   5.3.3 Hypothesis (8) .......................................................................................... 67
   5.3.4 Hypothesis (9) .......................................................................................... 68
5.4 Scenario to assess Distrust ................................................................................ 69
   5.4.1 Hypothesis (10) ......................................................................................... 69
   5.4.2 Hypothesis (11) ......................................................................................... 70
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Graph of losses in the recent past (CSI Survey, 2008).</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Increased response from 2007 to 2008 (CSI Survey, 2008).</td>
</tr>
<tr>
<td>Figure 3</td>
<td>MasterCard® home page not responding after a Distributed Denial of Service attack by the hacker group “AnonOps”.</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Information Warfare classification (Libicki, 1995).</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Thesis overview.</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Homepage of the Cyber warfare website.</td>
</tr>
<tr>
<td>Figure 7</td>
<td>A brief summary of each article and a link to the full article.</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Information Operations hierarchy.</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Types of Cyber Weapons.</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Tools used to translate adversary motive to complete control of the user’s computer.</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Broad classification of models in the area of cyber warfare literature.</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Based on Cyber terrorist model (Schudel &amp; Wood, 2001).</td>
</tr>
<tr>
<td>Figure 13</td>
<td>High Level Overview of the CCWST Software System Illustrating the Major Subsystem.</td>
</tr>
<tr>
<td>Figure 14</td>
<td>State transition diagram illustrating the life cycle of a CCWST weapon on a CUA.</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Snapshot of the Keyhole GUI.</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Snapshots of Keyhole GUI window illustrating the first two steps of creating a reusable cyber weapon.</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Snapshots of Keyhole GUI illustrating the process of setting up meta-codes and metadata required for transitioning weapons between various states in a weapons life-cycle.</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Example rule to replace style of &lt;H1&gt; tags.</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Example rule to re-direct all requests of Google to Yahoo.</td>
</tr>
<tr>
<td>Figure 20</td>
<td>An example of a rule to change all first images of any webpage to &quot;wsri.jpg&quot;.</td>
</tr>
<tr>
<td>Figure 21</td>
<td>An example rule to change the Google image on Google home page to a picture of Yahoo.</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Snapshot of the Rule Designer.</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Screenshot from computer under attack using expedia.com to find flights departing from Columbus, Ohio.</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Screenshot of search results modified by IE Genie.</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Screenshot of search results modified by IE Genie (Individual Flights shown leaving from Dayton).</td>
</tr>
<tr>
<td>Figure 26</td>
<td>An example of a distraction scenario which opens multiple pop-ups on the participants Desktop.</td>
</tr>
<tr>
<td>Figure 27</td>
<td>An example of a pop-up which claims a better deal for the same route triggered by the Keyhole operator to distract the participant.</td>
</tr>
</tbody>
</table>
Figure 28: Questionnaire data represented graphically. .............................................................. 76
TABLE OF TABLES

Table 1: Mapping of Target Computer Applications to Cyber Attack Types. .............................. 46
Table 2: Proposed cyber weapons .................................................................................. 49
Table 3: Scenario to cyber effect mapping of the results .................................................. 75
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA</td>
<td>Computer Network Attack</td>
</tr>
<tr>
<td>CND</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>CNE</td>
<td>Computer Network Exploitation</td>
</tr>
<tr>
<td>CNO</td>
<td>Computer Network Operations</td>
</tr>
<tr>
<td>CUA</td>
<td>Computer Under Attack</td>
</tr>
<tr>
<td>CCWST</td>
<td>Cognitive Cyber Weapon Selection Tool</td>
</tr>
<tr>
<td>cwDOOR</td>
<td>cyber warfare Weapon Deployment; Operation; Observation and Retraction</td>
</tr>
<tr>
<td>cwDIR</td>
<td>cyber warfare Desktop Image Recorder</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial Of Service</td>
</tr>
<tr>
<td>DDOS</td>
<td>Distributed Denial Of Service</td>
</tr>
<tr>
<td>IW</td>
<td>Information Warfare</td>
</tr>
<tr>
<td>ICCC</td>
<td>Internet Crime Complaint Center</td>
</tr>
<tr>
<td>MILDEC</td>
<td>Military Deception</td>
</tr>
<tr>
<td>PSYOPS</td>
<td>Psychological Operations</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1. Background

Revolution in information technology has led to large amounts of data being constantly generated on the internet. At present the internet is used for several purposes including learning, business, social networking, news, videos, etc. Security concerns through the breach of confidential data while using the internet for business transactions have received increasing attention. Computer Survey (Computer Security Institute Survey, 2008) reports that, though the financial losses reported by companies due to security breaches have been reduced over the years, as illustrated in Figure 1, there still seems to be a constant threat to information. As illustrated in Figure 2, the number of cyber attack incidents reported has increased from 2007 to 2008.

![Graph of losses in the recent past (CSI Survey, 2008).](image)

Figure 1: Graph of losses in the recent past (CSI Survey, 2008).
Driven by political, personal or monetary motives, hackers create havoc in the cyber space by stalling business online 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” to retaliate Julian Assange’s case of Swedish extradition. This group attracted thousands of individuals through Twitter, Facebook, online forums and chat groups to download software available at 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 and Pelofsky, 2010). Their targets were Visa® and MasterCard®, the world’s most reputed credit card payment companies. Attack of their corporate websites has raised new questions about credit and personal information and its online security. Figure 3 illustrates an example of an attacked page MasterCard® homepage as a part of a DDOS attack by “AnonOps.”
Cyber attackers have an array of weapons to choose from and the intensity and effect of an attack generally depend on the motives of an attacker. Every system is inherently susceptible to vulnerabilities, and the hacker’s strategy often lies in identifying and exploiting these vulnerabilities effectively. In a real world cyber warfare scenario, the attacker gains a “swift attack” advantage. The unsuspecting cyber administrator is often caught by the element of surprise and the attack generally does not 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 in the recent past. It is no longer a war against the technology where the intention is to exploit computer vulnerabilities. The attackers have realized that any system is bound to be operated by humans and they come with their own set of operational 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 masquerading as an authentic source like a credit bureau or computer administrator of the company.

1.2. Information Warfare

The increasing pervasiveness of information in society and in various functional areas has triggered the 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 word Information Warfare. Information Warfare is often referred to as a collection of different techniques used as a part of Information Operations. According to Libicki (1995) Information Warfare could be divided into seven different categories as represented in Figure 4.
According to Libicki (1995), Command and Control Warfare (C2W) involves destroying the enemy’s command and control center and properly timing it to disrupt enemy operations. Intelligence Based Warfare is used to gain intelligence of enemy operations to counter attack with better alternatives. Electronic warfare could be used to manipulate digital communication
signals in a war scenario. Psychological warfare deals with human minds. Examples include operations against adversarial commanders, against troops or operations against cultural conflict. While hacker warfare deals with attacking computer systems of the adversaries, economic warfare deals with blocking critical supplies to countries to debilitate the economics of the country making it vulnerable to attack. Cyber warfare on the other hand involves semantic attacks whereby misleading users are to believe in navigating a masqueraded website.

To counter this problem, the U.S. Department of Defense (DoD) has proposed three important realms in terms of Computer Network Operations (CNO) (Wilson, 2006). These three areas are listed as follows:

- Computer Network Defense (CND) - This area is responsible for defense of homeland confidential systems by means of detection and immediate response through constant monitoring.
- Computer Network Exploitation (CNE) - Network exploitation deals with reconnaissance and intelligence gathering which includes detecting adversary vulnerabilities and gaining unauthorized access to confidential adversary information.
- Computer Network Attack (CNA) - This area deals with disruption and destruction of adversary systems by using appropriate cyber weapons such as Trojans or viruses to gain control over adversary systems.

DOD is increasing its efforts in the areas of cyber exploitation and cyber attacks. In recent years, the U.S. Government has also adopted use of Psychological Operations (PSYOPS) and Military Deception (MILDEC) as a part of its warfare tactics. Psychological operations can be defined as propagating carefully selected information in foreign nations through media to alter popular perceptions and beliefs in order to further ulterior motives. In the recent and continuing
war on Iraq, under the Operation Iraqi Freedom (OIF), a PSYOPS operation, e-mails, telephone calls, faxes etc were extensively used to encourage leaders in Iraq to withdraw support of the then Iraqi President Saddam Hussein.

### 1.3. Problem

Although deception and psychological operations are being used as a part of DoD 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). Efforts have been invested to understand adversarial intent and motives by alluring hackers to specific systems called “Honeypots” (Provos, 2004). There have been efforts in the form of red teams that observe cyber terrorist behavior in a simulated cyber warfare environment (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. Also red team efforts have mostly focused on improving defense. There is little knowledge in terms of psychological effects caused by these weapons and using these weapons for the purpose of an offensive cyber attack. A proper test bed is needed to evaluate and map cyber weapons to their respective cognitive characteristics. On provision of such a tool, it would be easier to simulate a real time cyber attack scenario and observe user reactions. This would help in building a mapping between the cyber weapon employed and the subsequent cognitive effect observed in the adversarial behavior.
1.4. Approach

This research explored and mapped the possible perceptual changes to their respective
cognitive weapons when used in a particular use case scenario. A 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 framework for this tool was extensible and
scalable to make space for future cognitive weapons and to attack large number of computers
simultaneously once. The objective was not to research the possibilities of exploiting
vulnerabilities and attacking computers, since there is existing literature which exists on this
concept. The objective was rather to monitor and evaluate the performance of the cognitive
weapons and to observe and evaluate cognitive changes in the adversaries.

Figure 5: Thesis overview.
The approach and steps for this thesis involved four phases as illustrated in Figure 5. The first phase of this thesis consolidated knowledge of past literature in the field of cyber warfare. An online cyber warfare literature repository was created to assimilate previous knowledge of attack types, attack methodologies and variegated ways in which cyber warfare could be launched. This repository contains journal papers, magazine articles and other online resources which gives an overview of the state-of-the-art literature on cyber warfare as shown in Figure 6 and Figure 7. The repository consists of up to 100 papers and ranges from the years 1996 through 2010.

**PROJECT RELATED DOCUMENTS**

![Image of a computer with a list of cyber warfare terms]

<table>
<thead>
<tr>
<th>ADWARE</th>
<th>SPAM</th>
<th>COOKIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>TROJANS</td>
<td>PHISHING</td>
<td>MALWARE</td>
</tr>
<tr>
<td>DOS &amp; DDOS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 6: Homepage of the Cyber warfare website.*
ADWARE

IS SPYWARE AN Internet Nuisance or Public Menace?: Adware is a newly emerging scenario where companies and individuals inject spyware into the computers of the users. There could be the variety of reasons the companies would like to do that. Most of the spyware could be benign and may just generate pop-up ads based on the user's web interests. If the spyware is injected with a malicious motive, the spyware could be injected to track each keystroke of the user and send that information to the owner of this spyware. The information thus obtained could just be used for legitimate data mining or it could be used in the wrong way to obtain credit card or other personal information. The authors here explains the different reasons why the users are unaware of this posing threat. They support their claim by a survey they conducted on IS professionals and students of a large state university in southeastern US. They have tried to evaluate the behavioral tendencies of individuals against adware and advocate user education towards adware.

Author: Qing Hu and Tamara Dinev


Full Paper: PDF

Investigating Factors Affecting Adoption of Anti Spyware Systems: In the present situation Anti Spyware tools seems to best option to reduce the malicious effects of adware. Despite the growing threat from spyware and adware the number of users adopting Anti spyware tools to control spyware seems to be very low. The authors have researched on the reasons for the low adaptability of Anti Spyware tools and tried to come up with useful guideline of how to improve the adoption rate.

Author: Younghwa Lee and Keaneth A. Kozar


Full Paper: PDF

This knowledge helped in creating a user profile and types of software used by user on a day to day basis. This allowed in Phase 2, cyber weapons to be mapped to their most commonly used software. A high level mapping of the cognitive weapons that can be imposed and used in context with a combination of cyber weaponry currently available was also created. As a part of Phase 3, an extensible and scalable framework for the Cognitive Cyber Weapon Selection Tool (CCWST) was conceived. The idea was to simulate the cyber space to provide a controlled environment, in which a cyber administrator would be able to compare and contrast various
cyber weapons and their psychological effects on subjects. In such an environment, cyber administrator or attacker would have sufficient time to comprehend the adversarial intent and activate a relevant weapon to alter the adversary’s cognitive state. On design and development of the CCWST, efforts were made to evaluate hypotheses based on evaluation parameters to identify certain cognitive states in the adversary. The results and conclusion are discussed followed by a discussion of future research possibilities.
2. LITERATURE REVIEW

2.1. Introduction

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 were reported for the year 2009. This explains the imperative need to defend cyber attacks which have become an expensive menace for businesses online. 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 the cyber attacks which might be possible in the future. It is also essential to clearly distinguish between “developing” and “actual” attacks. This is because, although it might seem that the number of attacks have come down in a particular year, there might be an evolving threat in the near future. There is a noticeable recognition in the past to the fact that cyber warfare is an important next area of development for targeting and weaponeering with far-reaching effects in national defense and economic security (Hutchinson & Warren, 2001, Bledstein, 2008).

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.”

According to Spintzer (2004), if black hat hackers (malicious hackers) were to be compared to adversaries and a computer administrator could be compared to a defender, then the scenario of a cyber attack could very well be considered to a cyber warfare scenario. The U.S. Department of Defense has identified five key areas in its Information Operations wing both in terms of attack and defense through information. These capabilities involve Psychological
Operations, Military Deception, Operational Security, Computer Network Operations, and Electronic Warfare (CRS Report For Congress, 2007). Computer Network Operations have been further sub-divided into Computer Network Defense, Exploitation and Attack. This research deals with the Computer Network Attack wing of the cyber warfare division. Figure 8 shows the sub classification for Information Operations based on the categorization of CRS Report for Congress (2007).

![Figure 8: Information Operations hierarchy.](image)

### 2.2. Types of Cyber Weaponry

Malware includes tools that are used with the intent of gaining access to the user’s systems to monitor and extract personal information from the users’ computers. Designing firewall and anti-malware software is difficult because malware is constantly changing in its form and scale and is fairly easy to penetrate throughout the internet (Cuadra, 2007; Jha &
Christodorescu, 2004; Heron, 2008). Figure 9 illustrates the variety of forms of malware which are used in a cyber attack scenario.

![Diagram of Cyber Weapons](image)

**Figure 9: Types of Cyber Weapons.**

Literature aggregation in the field of cyber warfare resulted in distinguishing the types of cyber weapons into the following categories:

- Adware
- Spam
- Cookies
- Trojans
- Phishing
2.2.1. Adware

Adware is a newly emerging scenario where companies and individuals inject spyware into the computers of the users (Hu & Dinev, 2005; Lee & Kozar, 2005; Schultz, 2003). Most of the time the spyware injected is benign and is injected to generate pop-ups based on user’s web interests. However this tool could be used maliciously by recording keystrokes of users and other information which might compromise the personal information of an individual.

2.2.2. Spam

Junk E-mail or Spam is another weapon used by advertising companies to promote their products. A large volume of this spam is a constant reminder of the network traffic being clogged and the extra mail servers that need to be setup to handle this nuisance (Hinde, 2003; Ahmed & Oppenheim, 2006; Gomes, Cazita, Almeida, J, & Meira, 2006; Cournane & Hunt, 2004).

2.2.3. Cookie

Cookies are a substantial threat to users accessing the internet because it allows direct access to web servers to transfer information and store it in the user's computer whenever the user visits a particular website. The cookies have an ability to store information from user sessions which could generally lead to identity theft attacks (Schonberger, 1998; Sharon, 1997).

2.2.4. Trojan

Trojans are a dangerous threat to user security. These are computer programs which reside in the victim’s computer without the knowledge of the victim and then establish a direct connection to the attacker’s computer. Thus relaying all the information entered into the system directly to the attacker (Gosling, 2005). Trojan attackers have come up with a completely new
way of encrypting data on a victim’s computer and then demanding ransom to decrypt that data (Emm, 2006).

2.2.5. Phishing

Phishing is the process of sending deceptive e-mails posing as legitimate from Government, Banks in order to obtain confidential personal information (Robila & Ragucci, 2006). Social phishing or context aware phishing has become a threat in the recent years due to the use of social engineering involved to fool users into compromising personal information (Jagatic, Johnson, Jakobsson, & Menczer, 2005). The number of websites which mock the official websites has increased in the recent past owing to the convenience and ease of launching such attacks (Kirda and Kruegel, 2005; Hilley, 2006).

2.2.6. Denial of Service (DOS) & Distributed Denial of Service (DDOS)

A server, if overloaded by repeatedly targeting it with continuous requests gives way to Denial of Service attack. In a Distributed Denial of Service attack, several computers are compromised without the knowledge of users and then these computers are used as sources for repeated requests to the server, this method proves to be much more effective and is capable of bringing down servers for elongated periods of time. It also proves to be more cost effective for malicious hackers and keeps the hacker from giving out his digital signature during such an attack. RATS (Remote Administration Trojans are an example of such Trojans which download onto the system of an unsuspecting user and then surreptitiously capture screen shots, keyboard strokes or even approve access to a remote system (Stafford & Urbaczewski, 2004). A recent example of a DDOS attack can be observed in the case of “Operation Payback” launched in opposition to Assange’s arrest. The hacker group “Anonymous” launched DDOS attacks against Credit payment giants, MasterCard and Visa.
The distinction between tools of cyber weapons used is very fuzzy. Sometimes these tools could be used in combination or separately and generally the tools are chosen based on the intention of a hacker. For example, if the intention is to steal personal information, a hacker could use cookies, adware or even spam in combination with a Trojan or a Virus to gain control of the user’s machine. Adversarial motives need an entry point into the user’s computer to gain access to the user’s personal information. This entry point is often achieved by tools such as Adware, Spam etc. After compromising a user’s system, the next step is to constantly or periodically monitor user behavior which is achieved by malware such as Viruses, Trojans etc. Figure 10 represents the different stages which are involved in the successful staging of a cyber attack.

![Figure 10: Tools used to translate adversary motive to complete control of the user’s computer.](image-url)
The intention and proficiency of a hacker play a key role in the scale and complexity of an attack. Attacks have become more organized and large scale with time, especially with the involvement of mafia and many other crime syndicates (Kshetri, 2005). The intention could range from stealing personal credit card and security information to creating widespread distrust through false propaganda. Most of the time, a compromised computer might be used to launch a large scale Distributed Denial of Service (DDOS) attack. A cyber criminal decides on the mode and method of attack based on his/her intention. Based on an intention, the hacker chooses certain tools to target a large scale or individual audiences. Once the access is gained, tools such as viruses and Trojans are used to constantly monitor user keystrokes and screenshots of the users’ desktop.

“Cognitive Hacking” is a word coined by Cybenko, Giani, & Thompson (2002) to refer to the manipulation of user’s perception. According to them, cognitive hacking could be divided into two categories - “Overt” and “Covert” attacks. In a “covert” attack a subtle manipulation of user perception is targeted by advertising misleading information. On the other hand, in an “overt” attack a legitimate website is spoofed to validate misleading information. For example, the misinformation that Britney Spears died on a defaced page of CNN’s top ranked news story created ripples of disbelief. These weapons used to misinform readers of CNN could be a typical example of confusion. The overt attack could be an example of deception where the intention is not to confuse the user, but to silently deceive the user into believing in non-existent data. These incidents throw light on two issues, one the lack of proper security protocols in the companies which allow hacking successfully and the second, the long term damage that a small rumor could cause.
There are a lot of ways in which a hacker could gain access to a user’s computer. It could be through means of social engineering, adware, spam, etc. or even as simple as searching in corporate trash bins for passwords and other crucial information (Baybutt, 2002). Most of the time, the intention of such access might just be to observe user behavior. Although this might have legal consequences, still companies choose to do this, especially with the recent raise in targeted advertising (Stafford and Urbaczewski, 2004). But such access to a user’s computer might be lethal in terms of security, if there is a malicious intent associated with it. Most of these methods could effectively be blocked through means of user awareness and firewalls. But owing to the growing number of Trojan and virus attacks to systems and their evolution in terms of deception it has become a major problem to track down attacks and contain the damage to personal and production systems.

Although most of these attacks require some level of technical understanding of the back end functionality of computers, techniques such as Phishing and Spamming are fairly easy to carry out and have devastating consequences when targeted at a larger section of people. A prominent reason for such 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”
Hence using deception to defend information systems is an interesting idea. Cyber adversaries have long since used deception as a means to attack network systems and, in the opinion of Rowe N. C. (2004) it is only appropriate to return in kind. The author states that the deception should be believable enough to fool the attacker. It is extremely important to use the right deception technique based on context on the attacker.

Although such aggressive defensive tactics would mean departing from the present law and policies of the government, it is important that we change the laws to incorporate such techniques for the sheer reason that purely defensive wars are not always winnable especially against an adversary like the cyber attacker (Welch, Buchheit, & N. Ruocco, 1999). The main drawback of offensive defense is that the internet attacks are very short lived and do not give sufficient time to trace back the attack (Jayaswal, Yurcik, & Doss, 2002)

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 both as 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)

2.3. 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 classifications which contribute to research literature in the area of cyber warfare are red team efforts, simulations, test beds and honeypots and are shown in Figure 11.
2.3.1. Red Team Efforts

Information Design Assurance Red Team (IDART) was developed as a part of an information assurance assessment program by Sandia National Laboratories. Red team efforts have been developed to assess and identify critical vulnerabilities in a system which generally go unnoticed (Wood & Duggan, 2000). In a Red Team/Blue Team exercise, the researchers are divided into attackers and defenders. These teams are then observed in an environment where the attackers try to find vulnerabilities in the adversary systems, while the defenders find a way to protect their cyber assets. Such exercises often end in realistic scenarios and show variegated ways of identifying and also fixing system vulnerabilities (Sollins, et al., 2009). The IDART’s information assurance program was instrumental in modeling the behavior and characteristics of a cyber terrorist through the cyber terrorist model (Schudel & Wood, 2001). This model explains
that the terrorist planning to launch a cyber attack spends significant amount of time in intelligence gathering. An illustration of the cyber terrorist model is given below in Figure 12.

![Figure 12: Based on Cyber terrorist model (Schudel & Wood, 2001).](image)

### 2.3.2. Simulations

Using simulation to model and predict adversarial intentions through automatic agents is another area of research in the cyber warfare literature. The idea was to simulate adversarial behavior using advanced various simulation techniques available. Synthetic Environment for Analysis and Simulation (SEAS) was a simulation environment developed as a part of an effort by Purdue University (Chaturvedi, Gupta, Mehta, & Yue, 2002) and studied the interaction of agents which were assumed to be governments, transnational corporations and terrorists. Based on these interactions, and five levels of security provided to each agent, the simulations involved a variety of cyber tools ranging from computers, modems, telephones and software and the effects of these attacks on investment decisions, defensive actions were observed.
Similarly simulation of a Distributed Denial of Service (DDoS) attack by cloning separate teams of agents on different hosts was another idea conceived by (Kotenko, 2005). In this research a team work based simulation was used where a team of agents acted as malefactors or attackers and the opposite team acted as benefactors or defenders. While the attacker agents tried to exploit the vulnerability and gain additional information of particular hosts, the defender agents, tried to investigate the reason for inquiries about additional information and made intelligent decisions to suppress suspicious activities. Kotenko (2007) also proposed a cooperative cyber defense mechanism against distributed attacks for the department of homeland security of Russia. In this revised model, three levels of cyber security were implemented, where in the first level a static defense was adapted which pertained to access control, authentication verification etc., the second level which could proactively collect information and assess security and a third level could intelligently make decisions about the overall defense mode of the system being “adequate” or “optimal”.

Another example of a simulation of a cyber attack uses memory based multi-objective evolutionary algorithm (MMOEA) to apply evolving game strategies to model an attacker-defender scenario in a simulated network environment (Vejandla, Dasgupta, Kaushal, & Nino, 2010). There also have been efforts to create helper tools that could be used for effective cyber scenario generation. The authors Kuhl, Kistner, Costantini, & Sudit (2007) developed a simulation that could mock an intrusion detection system by generating messages which could alert a cyber defender of a malicious cyber attack or non malicious network activity. This approach, in the opinion of the authors, helps generate random simulated data which could then be used to generate multiple cyber attack scenarios.
2.3.3. Test Beds

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). Testing and evaluating, internet attacks require emulation and replication to understand and analyze internet incidents in close detail. However, a more feasible solution would be to use a secured black box to test lethal cyber weapons in networks alienated from outside world so the spread of such internet worms and Trojans could be well contained and yet leave space for exploration. Several test-beds have been developed since the advent of cyber warfare attacks (Davis, Tate, Okhravi, Grier, Overbye, & Nicol, 2006; Benzel, et al., 2007; Benzel et al, 2008; Van Leeuwen, Urias, Eldridge, Villamarin, & Olsberg, 2010) and often the necessity of a test-bed creation is driven by specific objectives. Defense Technology Experimental Research (DETER) was an experimental test bed developed by a collaborative team of researchers from University of Southern California and University of California, Berkley (Benzel et al, 2006). The idea was to develop a robust experimental test bed with a potential to support multiple node attacks in a distributed setup and capable of launching large scale DDoS attacks etc.

With an increase in extensive computerization of power system companies, the risk of a cyber attack in the field of electrical power system is also increasing. Although there is skepticism regarding the feasibility of such attacks (Jones, 2005) and the extent of damage or any reported incidents in the area of attacks of critical infrastructures through cyber attacks is unknown (Lewis, 2002) there have been efforts to create an experimental test bed for evaluating security vulnerabilities in critical infrastructure protection called the Supervisory Control and
Data Acquisition (SCADA) cyber security test bed (Davis, Tate, Okhravi, Grier, Overbye, & Nicol, 2006).

2.3.4. Honeypots

According to a definition by Spintzer (2004) a honey pot is defined as a

"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 to later analyze and gain insight of the cyber attacker patterns. Some of the advantages of honeypots include distracting attackers from valuable information; generate warnings in the instance of a compromise, and to enable 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 collected. There have also been distributed honeypot network systems set up to understand the underpinnings of distributed attacks called a Honeynet, (Know your enemy, 2004).

Although several of these models have been used to research in the areas of system vulnerabilities and attack types, there do not seem to be any research studies in the field of cognitive cyber weapons which are 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 empirical evaluation.
3. CCWST DESIGN AND FRAMEWORK

3.1. Introduction to Cognitive Cyber Weapon Selection Tool (CCWST) Framework

CCWST Framework is based upon a distributed software platform which 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 a wartime scenario. In the CCWST framework, it was assumed that there would be a central operator or a group of central operators who 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 expected of such a framework. First is the ability to monitor and control the adversarial computer for both reconnaissance and warfare operations and second is a large arsenal of context specific weapons that can alter information on specific software suites generally used by an adversary. Two critical pieces of software perform these functions as a part of the CCWST framework. Keyhole forms the eyes for the cyber operator to constantly monitor adversarial moments, and Genie is a cyber weapon arsenal the operator could choose to deploy relevant cyber weapons onto an adversary’s computer. The two components together bridge the gulfs of execution and evaluation between the Computers under Attack (CUAs) and the operator. Figure 13 gives a general overview of 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 Thesis. Also, the CCWST was designed to address only the Windows Operating System and all weapons related to the Internet browser were specifically for the Internet Explorer browser.

Figure 13: High Level Overview of the CCWST Software System Illustrating the Major Subsystem.

As indicated in Figure 13, The CCWST had to be a distributed system with various semi-autonomous subcomponents operating asynchronously on various computers. The independent subcomponents interacted with each other via network interconnects using customized application-level protocols. The underlying interconnect could be any standard wired or wireless communication channel that supported conventional access to network resources including the Internet. The customized, application-level protocols enabled various subsystems to coordinate their activities with each other to achieve the desired functionality.
3.2. 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 sub-system that masquerades as a windows system process to monitor adversary activities and 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 (GUI)
- Cyber Weapons Deployment, Operation, Observation, and Retraction (cwDOOR) Service

3.2.1 Cyber Weapons

In the context of the aggregate system a notion of a cyber weapon was summarized to be a well defined unit of software that undergoes a predefined sequence of state transformations as part of its lifecycle. The state transformations correspond to various operational notions associated with a weapon such as: deployed, activated, and deactivated. These state transitions are triggered by the cyber IO operator and are achieved through metadata and meta-code associated with each weapon.
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 impacting and inducing changes in the cognitive, perceptual, and behavioral aspects of an adversary. Every cyber weapon also has associated metadata and meta-code required to transition the weapon through various states in its life cycle. The life cycle of a cyber weapon from the perspective of the CCWST infrastructure is described in the next section.

As an integral part of the CCWST project we developed a variety of weapons that target different classes of software such as: browsers, word processors, spread sheets, 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.

3.2.1.1. Life Cycle of a Cyber Weapon

As mentioned earlier, the CCWST infrastructure operates with an abstract definition of a cyber weapon in order to ease the overall design and development of the core infrastructure components. The core components of CCWST treat a cyber weapon as a well defined unit of software that undergoes a series of state transitions in order to achieve the desired effects. The series of state changes essentially constitutes the life cycle of a cyber weapon. Figure 14 illustrates an overview of the life cycle of CCWST cyber weapon. Every state change is triggered indirectly by the cyber IO planner and changes in a weapon’s state are induced using meta-codes. Meta-codes are essentially simple software commands and rules that are used to induce the changes in the state. The meta-codes have associated metadata that provide the necessary inputs for the meta-codes to operate. Concrete examples of meta-codes and metadata are presented in the following section along with a description of the process of creating a cyber weapon.
Figure 14: State transition diagram illustrating the life cycle of a CCWST weapon on a CUA.

As shown in Figure 14, the life cycle of a CCWST weapon commences on a CUA when a new weapon is deployed on a given CUA by a cyber IO operator. The deployment is coordinated by a centralized Keyhole and the cwDOOR service on the CUA. Initially the weapon begins its life cycle in the Deploying state. In this state, the necessary data for the weapon is still being obtained from the centralized Cyber Weapons Repository via the Keyhole. Once all of the weapon data and associated meta-codes are obtained, the cwDOOR service then runs the deployment meta-code associated with the weapon. The deployment meta-code runs and essentially performs any installation operations for the weapon on the CUA. Once the deployment meta-code is successfully completed, the weapon transitions to the deployed state. Simpler weapons may not have any special meta-codes and these weapons immediately transition to the deployed state once all the necessary data has been obtained from the Keyhole.

Once the weapon has been successfully deployed, a cyber IO operator may transition the weapon into the activated state by activating the weapon. In the activated state the cyber weapon begins to perform its operation to impact the adversaries cognitive, perceptual, and behavioral states. As shown in Figure 14, the weapon does not instantaneously transition, but transitions via
the activating state. In this state, the meta-code that may be necessary to suitably activate the weapon is run. If the meta-code fails to succeed then the weapon transitions back to the deployed state after reporting a suitable error message to the cyber IO operator via Keyhole GUI.

An active weapon may transition to the deactivating state in two different ways. In the first case, the software representing the CCWST weapon completes running and the weapon automatically transitions to the deactivating state. On the other hand, the weapon might be a perpetual piece of software that is explicitly deactivated by the cyber IO operator.

In this case, a meta-code is executed to actually terminate the weapon thereby transitioning it to the deactivating state. Once the weapon has been successfully deactivated, it transitions back to the deployed state where in it can be reactivated in the future as needed. As shown in Figure 14, if a weapon encounters errors in the activated state it transitions to the retracting state automatically.

The retracting state of a weapon indicates that the weapon is being removed from the CUA. Typically, only weapons in the deployed state can transition to the retracting state. However, a weapon may also transition to the retracting state if an error occurs in the activated state. In the retracting state, all the data associated with the weapon are deleted from the CUA.

Any supplied meta-codes for uninstalling the weapon are executed prior to deleting the files. The meta-codes may perform additional clean up operations that may be necessary to appropriately retract the weapon from the CUA. Once the retraction process has been completed, the weapon transitions to the retracted state. Once a weapon has reached the retracted state, it has completed its life cycle and the weapon is completely discarded from the CUA by the cwDOOR service.
3.2.2. **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 individual or a team of adversaries. In addition to creation and management of cyber weapons in the Cyber Weapons Repository the Keyhole also coordinates the deployment, observation, activation, and retraction of cyber weapons deployed on various Computers under Attack (CUA). The Keyhole interacts with the cwDOOR service deployed on each CUA using a pre-specified application-level protocol to perform the various tasks as directed by the cyber IO operator.

![Snapshot of the Keyhole GUI.](image)

**Figure 15:** Snapshot of the Keyhole GUI.

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 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 action. Figure 15 illustrates the main screen of the Keyhole application.

In the CCWST system, creation of a weapon is performed using the GUI provided by Keyhole for this task. The GUI is organized as a wizard that guides the operator through the various steps required to create a weapon. The wizard provides an intuitive and user friendly approach to creating a weapon. The CCWST system assumes that the necessary software modules that constitute the core weapon have been developed and tested independently. In addition, meta-codes for deployment, activation, deactivation, and retraction are also developed. Commonly MS-DOS batch files (.bat files) provide a convenient mechanism for creating meta-codes for performing some of these operations.
A snapshot of the first two steps of the weapon creation process as presented in the Weapon Creation Wizard in Keyhole’s GUI are illustrated in Figure 16. In the first step, the cyber IO operator is required to provide a name and a brief description of the weapon. In the second step, all the files constituting the weapon are added to the weapon. The files include all data files; meta-code files, executable files, and MS-DOS batch files that are necessary to perform various state transitions in the life cycle of the weapon.

Figure 16: Snapshots of Keyhole GUI window illustrating the first two steps of creating a reusable cyber weapon.
Figure 17 Snapshots of Keyhole GUI illustrating the process of setting up meta-codes and metadata required for transitioning weapons between various states in a weapons life-cycle.

The meta-code can be in the form of a standard executable program or in the form of an MS-DOS batch file. The metadata is used to provide additional information to the meta-codes in the form of command line parameters. The GUI permits multiple parameters with optional values to be specified. In addition, the parameters may be set to be overridden by the user during weapon deployment as illustrated in Figure 17. This feature enables the cyber IO operator to reuse an existing weapon and adapt its behavior to suit the exact scenario during deployment.

3.2.3. cwDOOR Service

Cyber Weapons Deployment, Operation, Observation, and Retraction Service (cwDOOR) service is to act as a backdoor on each Computer under Attack (CUA). This unobtrusive software subsystem provides the necessary functionality for a cyber IO planner to observe, deploy, and manage cyber weapons. The cwDOOR service also plays an important role in managing the life
cycle of various cyber weapons deployed on a CUA. The architecture and design permits a single CUA to be independently monitored and controlled by multiple cyber IO operators and planners.

3.3. Genie

Genie is the suite of client-side plug-ins (weapons) that execute on the target computer presumably on command. While the Keyhole model perhaps permits any scripted language to behave as a Genie, two customized Genie modules that operate in the context of the user's IE browser (IEGenie) and Microsoft Excel (ExcelGenie) were developed as a part of the Genie arsenal.

3.3.1. IE Genie

IEGenie manipulates the web pages and document object model for targeted content attack on the CUA. The hyper linking 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. As the content-deception may extend from manipulating content on a single page to a whole click-stream, it is extremely important for these tools to memorize and tailor deception over a prolonged session spread across different web pages. IE Genie is therefore implemented as a simple single-cell finite state automaton that uses simple XML grammar to define and execute actions in the browser's context. Structured XML grammar lets CUAs be tailor-targeted to specific users and uses.

Content attacks mostly seek specific elements on a web page after navigation and modify the structural layout or the content of the web page. Page attacks, on the other hand, seek to deny and/or alter (broker) web page requests even as the browser is making the request. Content-attacks only modify specific elements on a web page after the page is downloaded and rendered.
In Figure 18, all tags marked as <H1> are stripped of their headline style and rendered as inline text.

```xml
<rule startstate="-1"
   endstate="-1"
   trigger="tagname"
   regexfind="H1"
   action="replaceInnerHTML"
   regexreplace="xslt text()" />
```

Figure 18: Example rule to replace style of <H1> tags.

Page attacks are limited to capturing the page-navigating events. Genie receives events when a user's browser (including inner frames) is presumably navigating to a new location. Genie can then, based on rules, either permit, deny, or alter the request for the user thus invoking DOS attacks. Genie can further capture GET and/or POST data and alter the request-payloads to create confusion, distrust, and deception. In the example illustrated in Figure 19, a rule invoked before navigation to a page hijacks all requests that go to the google.com domain and re-directs them to a similar end-point on Yahoo. So Genie is able to keep in memory the previous state of user navigation to the web page of Google and is able to change it to a user defined page thus imitating the variable programming model.
3.3.2. Genie Rule Grammar

IE Genie's behavior is driven by the rules file that is published to it. Multiple rules may be rolled up into a single rules file and multiple rule files may simultaneously be published to the IE Genie for quickly adapting its behavior. Each file is an XML formatted ordered list of finite state rules that establish the context and series of page/content transformations. In case where multiple rule files are published (to the user's application data folder), the de-facto “rules.rul” file takes precedence. Command operators can, at runtime, rename and switch the active rules file using the Keyhole framework.

The command operator or the operations team may compile rules into a complete scenario (list of rules) and publish the file to IE Genie on a CUA. Each rule is simply a tuple of the start-state, trigger, object, action, and end-state elements.

- Start State: Some rules apply only to specific pages and/or websites. Since IE Genie lacks complex predicate-logic, start states provide a means to control application of rules. A start state of -1 suggests that a rule should apply universally to all pages/requests.
- End State: The end state is the target state for the finite state engine, if a rule applies. If a

```
<rule startstate="-1">
  endstate="-1"
  trigger="url"
  regexfind="(?<serverprefix>\.)\s*google.com"
  action="replace"
  regexreplace="${serverprefix}yahoo.com">
```

Figure 19: Example rule to re-direct all requests of Google to Yahoo
A series of rules apply, the end state provides a basis for the start state of the next rule.

- **Trigger:** The element or the logical predicate that defines if a rule should trigger.

- **Object:** If a rule should qualify to trigger, the object defines the element that is ready to be transformed. It is not mandatory to define an object or the action because some rules are merely used to switch state from one to other so following rules may apply. Object and the trigger definition may not emanate from the same element.

- **Action:** Upon encountering a trigger and an object-candidate for transformation, action identifies the type of modification that is performed over the object. The action can range from none to complete redaction and/or replacement. The range of actions may include such properties as URL, posted data, InnerHTML, InnerText, CSS styles, tag names etc.

An exhaustive list of actions, trigger element characteristics, and object properties is available in the annotated source code of IE Genie.

Two examples of a rules file are discussed below. The first example, shown in Figure 20, is a simple re-branding trick. The second example, shown in Figure 21, is more complex page attack that is spread out to two web pages. In the first example, all first images (presumably corporate logos) on the web pages are altered to show WSRI.jpg for a quick rebranding attack.

```xml
<rule startstate="-1"
      endstate="-1"
      trigger="xpath"
      regexfind="/img[0]"
      action="replaceInnerHTML"
      regexreplace="&lt;img src='wsri.jpg'&gt;"
>

Figure 20: An example of a rule to change all first images of any webpage to "wsri.jpg".
In the second example, google.com looks normal if directly navigated by the user. If a user navigates to Yahoo instead, the request is denied, redirected to google.com and the top logo on that google.com webpage is rebranded to a yahoo logo. This example shows how a finite state model helps apply conditional rule-predicates.

```xml
<rule startstate="-1"
      endstate="100"
      trigger="url"
      regexfind="yahoo.com"
      action="replace"
      regexreplace = www.google.com

      startstate="100"
      endstate="100"
      trigger="xpath"
      regexfind="/img[0]"
      action="replaceSrc"
      regexreplace="yahoo.jpg"/>
```

Figure 21: An example rule to change the Google image on Google home page to a picture of Yahoo.

### 3.3.3. Microsoft Office Genie

Office Genie is the cyber weapon designed to spy and invoke content-attacks in Microsoft Office applications. Office acts as a terminal window to compile, author, and exchange information sought in IE environment.
3.4. Genie Rule Designer and Test Toolkit

Although XML rules are fairly straight-forward to write in XML with a structured DTD, rule-chaining (with state transitions), rule-sequencing, schema validation can become complex for some scenarios. In order to help the command center write and compile complex scenarios, a simple Windows Forms based GUI designer toolkit is provided. The toolkit provides an easier means to ensuring adequate and accurate information is provided to meaningfully structure a sequence of rules. The designer lets one create or edit new or existing rule-templates for a quick and easy deployment to CUA. Figure 22 gives an illustration of the Rule Designer application snapshot.

![Rule Designer Snapshot](image)

**Figure 22: Snapshot of the Rule Designer.**

3.5. Genie Demonstration Scenario

A simple example of the potential of IEGenie is demonstrated in the following example. Using the scenario described previously, Figure 23 illustrates the adversarial user investigating flights on Expedia.com. The user is attempting to find flights departing from Columbus, Ohio (CMH) to Seattle (SEA).
Figure 23: Screenshot from computer under attack using expedia.com to find flights departing from Columbus, Ohio.

Once the adversarial user enters all the information related to the flight they are interested in, the search engine returns the results associated with the query. However, the IE Genie was used to modify the results of the query, such that the results returned by the search engine suggest that the flights displayed are those departing from Dayton, Ohio and not Columbus, Ohio. The destination city which is Seattle (SEA) still remains the same. The results modified by the IE Genie are displayed in Figure 24 and Figure 25.
Figure 24: Screenshot of search results modified by IE Genie.

Figure 25: Screenshot of search results modified by IE Genie (Individual Flights shown leaving from Dayton).
This successful demonstration of the Cyber Weaponry to modify the results from the search indicates that the CCWST is ideal for impacting adversarial behavior in a variety of settings.
4. RESEARCH METHODOLOGY

4.1. Introduction

The Cognitive Cyber Weapon Selection Tool (CCWST) forms a robust framework through which the ability of Genie to induce psychological and cognitive changes in the adversary can be demonstrated. Although the Keyhole and Genie architectures have the ability to monitor and induce cognitive changes, it is necessary to understand to what extent the tool can cause disruption in the adversary’s cognitive thought processes. To evaluate CCWST it was necessary to identify target software to deploy cognitive weapons and develop specific metrics to objectively ascertain the effectiveness of the Genie arsenal. This chapter elaborates the reasoning for the research methodology adopted by this research.

As a first step in understanding the characteristics of weapons that might be developed for a cyber warfare situation we mapped the suite of software used by people to the attack types used by hackers to compromise user computers. Each row was marked with an “X” symbol if it seemed to be a relevant mapping between the application and the cyber attack type. The numbers on the top of the matrix and on the extreme right indicate the total count of “X” for the respective columns and rows. The matrix illustrated in Table 1 shows that Malware and Trojans scored a six on a scale of 1 through 6 which suggests that these weapons could possibly be used on almost all software including word processing, spreadsheet, messaging, e-mail, browser and operating systems. It could also be deduced from the mapping that browser and messaging applications are the most critical piece of software which are vulnerable to all the malware attacks listed in Table 1. It was decided based on these inferences that IEGenie, ExcelGenie and certain Windows batch
files would be used as a part of the cognitive weapon arsenal to attack the Internet Explorer application, Microsoft Excel Spreadsheet application on Windows based systems.

<table>
<thead>
<tr>
<th>Target Computer Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>Attack Type</td>
</tr>
<tr>
<td>Spam</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Adware</td>
</tr>
<tr>
<td>Cookies</td>
</tr>
<tr>
<td>Trojans/Bots</td>
</tr>
<tr>
<td>Phishing</td>
</tr>
<tr>
<td>Denial of Service</td>
</tr>
</tbody>
</table>

Table 1: Mapping of Target Computer Applications to Cyber Attack Types.

4.2. Cognitive or Behavioral Changes

The next step was to identify the behavioral changes that could be caused by CCWST to disrupt adversarial intent in a cyber warfare scenario. These behavioral changes intended to be caused in the adversary had to be decided by the Keyhole operator at real time based on
reconnaissance data constantly relayed to the operator through Keyhole and thus predicting adversarial intent.

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 alluring 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.

Once the behavioral changes were identified that could be caused in the adversary, it was important to select a scenario that could use the Internet, spreadsheet software and e-mails so the CCWST could be demonstrated through the Genie arsenal. The scenario had to involve tasks where deploying Genie weapons could impact the task in the way intended by the Keyhole operator. An information retrieval situation was considered to be ideal and all encompassing for experimenting with CCWST. Hence, a scenario where two users would choose an airfare ticket was decided to be the scenario for the effectiveness evaluation of the CCWST weapon suite.

### 4.3. Scenario Objective

Team 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 as a part of the CCWST evaluation scenario. They were permitted to use only
Internet Explorer (web browser) and their emails and Microsoft Excel for documenting their details of the itinerary. In such a scenario, the following were the weapons created through Genie which were deemed relevant to use, in order to transition the user into the state of being deceived, confused etc. The weapons are tabulated in Table 2. The proposed cyber weapon gives the name of the weapon, the classification column, indicates the functionality of the weapon and the Table also includes a brief description of the weapons capability to induce behavioral changes.
<table>
<thead>
<tr>
<th><strong>Proposed Cyber Weapon</strong></th>
<th><strong>Classification</strong></th>
<th><strong>Brief Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Genie – Air Fare Changer</td>
<td>Social Psychology &amp; Incorrect Information</td>
<td>This cyber weapon changes air fares published on various websites to different values causing adversaries to get confused as they will be viewing different costs for the same air routes.</td>
</tr>
<tr>
<td>Genie – Air Fare Deceiver</td>
<td>Incorrect &amp; Phantom Information</td>
<td>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.</td>
</tr>
<tr>
<td>Genie – Adware</td>
<td>Incorrect Information &amp; Visual Perception</td>
<td>This cyber weapon will attempt to distract the user by placing advertisements and notices in various web pages with attractive slogans to distract the adversaries.</td>
</tr>
<tr>
<td>Keyhole – Message Box</td>
<td>Incorrect Information</td>
<td>This cyber weapon pops up additional messages on the adversaries’ computer causing them to get distracted.</td>
</tr>
</tbody>
</table>

**Table 2: Proposed cyber weapons.**

Relevant metrics were needed to evaluate and statistically prove the successful transition of the adversary into an altered cognitive state of being deceived, distracted, confused or distrust. If
a user was given access to a compromised system where Genie weapons were already deployed and activated, the experimental set up could be compared to evaluating a software interface on a computer. The literature proposes several methods to evaluate software interfaces. Some of these methods include evaluation procedures for web interfaces like thinking out loud during a user experiment session, question-asking, cognitive walkthrough, pluralistic walkthrough, focus groups, interviews etc. (Waes, 2000; Ivory & Hearst, 2001, Lee, Hong, Smith-Jackson, Nussbaum, Tomioka, 2006). Almost all these methods require some kind of an interaction with the user during an experiment by the principal investigator. But in the case of the CCWST the objective of testing the user would be lost without providing significant amount of detail about the software and its purpose. Hence, an alternative approach had to be adopted to test and evaluate a surreptitious software program like the CCWST. We theorized a set of metrics that could be closely tied down to the user behavior. The following metrics were identified to be good indicators of user behavior and as predictors of changes in the cognitive thought process of the user. The metrics are listed as follows:

- Time taken to perform a particular task
- Error in the desired objective
- Number of emails exchanged by two individuals
- Repetition to validate certain information
4.4. Experimental Design

The experiment involved a between subject design with two levels of the Group as the independent variable (Experiment and Control Group).

4.4.1. Variables:

**Independent Variable: Group**

A participant was considered to be in the Control Group (Non-Weapon: NW Group) if he or she performed the experiment on a computer which had no cyber weapons installed. A participant was considered to be in the Experiment Group (Weapon: W Group) if the participants had cyber weapons installed on their computers.

**Dependent Variables**

- **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 no. of emails sent and received by any one individual of a group.
- **Number of Repetitions:** The number of times the individuals re-visit 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.

4.4.2. Participants

Twenty participants were tested in this experiment. The participants were recruited through posters and advertisements throughout the Engineering campus. To be considered for the
study, the participants were required to have normal or corrected-to-normal acuity, a fairly good knowledge about Windows-based applications, Microsoft Excel, ability to search and retrieve information from the internet, and familiarity in operating mouse and a keyboard.

4.5. Experimental Setup

A total of five computers were used for the experiment. Four of these computers with a minimum of Intel Core 2 CPU and 0.99 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 was an Intel Core 2 Duo, with 2.99 GB of RAM. The suite of 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 for all the computers at the subject stations in the experiment.

4.6. Scenarios employed to determine Distraction, Confusion, Deception, and Distrust

The following scenarios were employed during task execution of the experiment to determine the effects of cyber weapons on the individuals and map them to their respective pre-hypothesized behaviors.

4.6.1. Scenario to Assess Distraction

The objective of this scenario was to assess the effectiveness of CCWST in transitioning the participant into the cognitive state of distraction. This scenario was implemented in two instances of the whole experiment in the Experiment group.
• In the first instance when the participant of the Experiment group was working on a specific task, several pop-ups would appear on the screen at once which opened several deal sites.

• In the second instance, 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.

Based on these two tasks, it was hypothesized that the dependent variables would vary as follows:

If the participant was distracted by the advertising pop-ups, it would delay the participant’s actual objective thus increasing the time taken for the task, when compared to the time taken to complete this task by the Control group. An illustration of the several pop-ups which appear on the users screen and the pop-up which claims to offer a better deal are shown in Figure 26 and Figure 27 respectively.
Figure 26: An example of a distraction scenario which opens multiple pop-ups on the participants Desktop.

Figure 27: An example of a pop-up which claims a better deal for the same route triggered by the Keyhole operator to distract the participant.

From the distraction scenario the first Hypothesis was formulated as follows:

Question (1): How would the time vary between NW and W groups in a distraction scenario?
Hypothesis (1): The time taken to complete a task in the distraction scenario, would be higher in the W group when compared to the NW group.

4.6.2. Scenario to Assess Confusion

This scenario was implemented through two tasks in the experiment.

- In the first task, the participants were asked to identify the cheapest airline ticket from Columbus to Cincinnati at [http://www.travelocity.com](http://www.travelocity.com). In the Experiment group, when the participant visited Travelocity website, he or she was re-directed to [http://www.orbitz.com](http://www.orbitz.com). However, after repeating this task a couple of times, the participant was directed to Travelocity again.

- In the second task, when the participant searched for flights from Columbus to Cincinnati, he or she would be re-directed to a search page which listed flights from Dayton to Cincinnati instead.

Based on these two tasks in the scenario, the following questions and related hypothesis were formulated:

Question (2): How does the number of emails exchanged between NW group and W group vary in the scenario to assess confusion?

Hypothesis (2): The number of emails exchanged between the participants of the W group is greater than the number of emails exchanged in the NW group.

Question (3): How does the number of repetitions vary between participants of the W group and the NW group?

Hypothesis (3): The number of repetitions is higher in the W group when compared to the NW group.
Question (4): How does the time taken to complete tasks related to confusion scenario vary between participants of the W group and the NW group?

Hypothesis (4): In tasks related to confusion scenario time taken to complete a task is higher in the W group when compared to the NW group.

Question (5): How does the confidence measure of a team of participants in tasks related to confusion scenario vary between participants of the W group and the NW group?

Hypothesis (5): In tasks related to confusion scenario, the confidence measure of W group is lesser when compared to the NW group.

4.6.3. Scenario to Assess Deception

This scenario was implemented through two tasks in the experiment.

- In the first task, 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 “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 Control group and Experiment group.

- In the second task, the price was changed again on http://www.expedia.com for Experiment Group to deceive the participant to think that it was the actual price on the website.
Based on these two tasks in the scenario, the following questions and related hypothesis were formulated:

Question (6): How does the total number of emails exchanged within a team of participants in tasks related to deception scenario vary between participants of the W group and the NW group?
Hypothesis (6): In tasks related to deception scenario, the total number of emails exchanged within W group and total number of emails exchanged within NW group are equal.

Question (7): How does the total number of repetitions within a team of a team of participants in tasks related to deception scenario vary between participants of the W group and the NW group?
Hypothesis (7): In tasks related to deception scenario, the total number of repetitions within W group and total number of repetitions within NW group are equal.

Question (8): How does the task completion time vary between the W and NW group vary in the deception scenario?
Hypothesis (8): The task completion time between W and NW group is equal for the deception scenario.

Question (9): How does the confidence measure of the participants vary between the NW and W group?
Hypothesis (9): The confidence measure of participants is equal for W group and NW group.

4.6.4. Scenario to Assess Distrust

This scenario was implemented by asking the participants of each group to e-mail the attachment of the final Excel Document after achieving all the tasks in the experiment. The participants were then asked to tally their document to their partners to see if all the values matched their own 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.

Based on these two tasks in the scenario, the following questions and related hypothesis were formulated:

Question (10): How does the total number of emails exchanged within a team of participants in tasks related to distrust scenario vary between participants of the W group and the NW group?
Hypothesis (10): 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 in the distrust scenario.

Question (11): How does the total number of repetitions within a team of participants in tasks related to distrust scenario vary between participants of the W group and the NW group?
Hypothesis (11): 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.

Question (12): How does the total time to complete the task vary between the W group and the NW group in the distrust scenario?
Hypothesis (12): 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 for the distrust scenario.

Question (13): How does the confidence measure vary between the W group and the NW group for the distrust scenario?
Hypothesis (13): The confidence measure for the W group is greater than the NW group for the distrust scenario.
5. RESULTS AND DISCUSSION

5.1. Results for the Scenario to assess Distraction

5.1.1. Hypothesis (1)

Null Hypothesis: \( H_0 \): There is no significant difference between the mean of the time taken to complete tasks within the Weapon and No Weapon groups in the scenario related to distraction.

Alternate Hypothesis: \( H_1 \): The mean of the user confidence measure in the No Weapon Group is greater than the mean of the user confidence measure in the Weapon Group in the Scenario related to confusion.

A two-sample t-test on the data gave the following output in Microsoft Excel for 95% confidence (\( \alpha = 0.05 \)) 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. It was observed that all the participants would just ignore the pop-ups which intended to create distraction. All the participants in the Weapon group closed all the pop-up windows and proceeded with their tasks thus avoiding any distractions to interrupt their tasks.
5.2 Scenario to assess Confusion

5.2.1. Hypothesis (2)

Null Hypothesis: $H_0$: There is no significant difference between the mean of the number of emails exchanged in the Weapon and No Weapon groups.

Alternate Hypothesis: $H_1$: The mean of the number of emails exchanged in the Weapon Group is greater than the mean of the number of repetitions in the No Weapon Group.

A two-sample t-test on the data in Microsoft Excel for 95% confidence ($\alpha=0.05$) indicated a p-value of 0.048 for a one-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we can reject the null hypothesis with 95% confidence. Hence we can conclude that the mean of total number of emails exchanged in the Weapon group is greater than that of the No Weapon group. Since the number of emails exchanged would be the same for the individuals of a group, only five observations were collected for each group.
5.2.2 Hypothesis (3)

Null Hypothesis: \( H_0 \): There is no significant difference between the mean of the number of repetitions in the Weapon and No Weapon groups.

Alternate Hypothesis: \( H_1 \): The mean of the number of repetitions in the Weapon Group is greater than the mean of the number of repetitions in the No Weapon Group.

In Microsoft Excel for 95% confidence \((\alpha=0.05)\) indicated a p-value of 5.57E-08 for a one-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we can reject the null hypothesis with 95% confidence. Hence we can conclude that the mean of total number of repetitions for the Weapon group were greater than the mean of total number of repetitions of the No Weapon Group. This suggests that the participants of the Weapon Group took greater number of repetitions to confirm their values and repeated each task more number of times when compared to the No Weapon Group.
5.2.3 Hypothesis (4)

Null Hypothesis: \( H_0 \): There is no significant difference between the means of the time taken to complete tasks related to confusion scenario in the Weapon and No Weapon groups.

Alternate Hypothesis: \( H_1 \): The mean of the time taken to complete the tasks in Scenario related to confusion in the Weapon group is greater than the mean of the time taken to complete tasks related to confusion scenario in the No Weapon group.

In Microsoft Excel for 95% confidence (\( \alpha=0.05 \)) indicated a p-value of 0.404 for a one-tail two-Sample t-Test assuming unequal variances. The p-value indicates that there is no sufficient evidence to reject the null hypothesis. Hence it cannot be concluded that the mean of the total time taken to complete the tasks related to Scenario 2 in the Weapon group is greater than that of the No Weapon Group. Since the time taken to complete the task, was a collaborative measure. The total time for a particular task to complete was the same for individuals of a group. Hence the number of observations recorded for time taken was only five for each group.
5.2.4 *Hypothesis* (5)

Null Hypothesis: $H_0$: There is no significant difference between the mean of the user confidence measure in the Weapon and No Weapon groups in the scenario related to confusion.

Alternate Hypothesis: $H_1$: The mean of the user confidence measure in the No Weapon Group is greater than the mean of the user confidence measure in the Weapon Group in the Scenario related to confusion.

A two-sample t-test on the data gave the following output in Microsoft Excel for a confidence level of 95% ($\alpha = 0.05$)

The above results indicate a p-value of 0.008 (<0.05) for a one-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we can reject the null hypothesis with 95% confidence. Hence 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. This indicates that for the scenario related to confusion, the user confidence was lower when weapons were activated on the participants’ computers in the Weapon Group when compared to the No Weapon group.
5.3 Scenario to assess Deception

5.3.1 Hypothesis (6)

Null Hypothesis: \( H_0 \): There is no significant difference between the mean of the number of emails exchanged in the Weapon and No Weapon groups for deception scenario.

Alternate Hypothesis: \( H_1 \): There is a significant difference between the mean of the number of emails exchanged in the Weapon and No Weapon groups for deception scenario.

A two-sample t-test on the data gave the following output in Microsoft Excel for a confidence level of 95% (\( \alpha = 0.05 \))

The number of emails exchanged was the sum of the emails sent to the partner and the emails received from the partner in any one email account of a group.

The above results indicate a p-value of 0.745 (>0.05) for a two-tail two-Sample t-Test assuming unequal variances. Based on the p-value, there is no sufficient evidence to reject the null hypothesis. Hence it may not be concluded that the number of emails exchanged in the Weapons group is not equal to the mean of number of emails exchanged in the No Weapons group for deception scenario.
5.3.2 Hypothesis (7)

Null Hypothesis: \( H_0 \): There is no significant difference between the mean of the number of repetitions in the No Weapon and Weapon groups.

Alternate Hypothesis: \( H_1 \): There is a significant difference the mean of the number of repetitions in the No Weapon and Weapon groups.

A two-sample t-test on the data gave the following output in Microsoft Excel for a confidence level of 95% (\( \alpha = 0.05 \))

The number of repetitions was calculated by observing the videos and counting the number of times a page was re-visited to confirm values.

The above results indicate a p-value of 0.035 (<0.05) for a two-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we can reject the null hypothesis with 95% confidence. Hence the two groups are significantly different from each other at a significance level of 0.05.
5.3.3 Hypothesis (8)

Null Hypothesis: \( H_0 \): There is no significant difference between the means of time to complete a task related to Scenario 3 in the No Weapon and Weapon groups.

Alternate Hypothesis: \( H_1 \): The mean of the time taken to complete a task related to Scenario 3 is greater in the Weapon group when compared to the No Weapon group.

Time was calculated by watching the recorded videos of the Desktops of the participants in the Data collection phase.

In Microsoft Excel for 95% confidence (\( \alpha=0.05 \)) a two-tail two-Sample t-Test assuming unequal variances indicates a p-value of 0.53 (>0.05) for. Based on the p-value, there is no sufficient evidence to reject the null hypothesis. Hence it may not be concluded that the means of total time taken to finish tasks related to the deception scenario are significantly different between the No Weapon group and Weapon group.
5.3.4 Hypothesis (9)

Null Hypothesis: $H_0$: There is no significant difference between the mean of confidence ratings of individuals in the No Weapon and Weapon groups for the deception scenario.

Alternate Hypothesis: $H_1$: There is a significant difference between the mean of confidence ratings of individuals in the No Weapon and Weapon groups for the deception scenario.

The confidence rating was collected from individual participants by considering all tasks related to the deception scenario.

In Microsoft Excel for 95% confidence ($\alpha=0.05$) a two-tail two-Sample t-Test assuming unequal variances indicates a p-value of 0.09 (>0.05) for a two-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we do not have sufficient evidence to reject the null hypothesis and hence we cannot determine if the means of confidence rating in the deception scenario are unequal.
5.4 Scenario to assess Distrust

5.4.1 Hypothesis (10)

Null Hypothesis: $H_0$: There is no significant difference between the means of the no. of emails exchanged in the tasks related to distrust scenario in the No Weapon and Weapon groups.

Alternate Hypothesis: $H_1$: The mean of the number of emails exchanged in the scenario related to distrust scenario in the Weapon group is greater than the mean of the number of emails exchanged in the tasks related to distrust scenario in the No Weapon group.

In Microsoft Excel for 95% confidence ($\alpha=0.05$) a two-tail two-Sample t-Test assuming unequal variances indicates a p-value of 0.055 for a one-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we can reject the null hypothesis with a confidence of 95% and hence it can be concluded that there is sufficient evidence that the mean of total number of emails exchanged within the Weapon Group is greater than the mean of total number of emails exchanged for the No Weapon Group.
5.4.2 Hypothesis (11)

Null Hypothesis: $H_0$: There is no significant difference between the means of the no. of repetitions in the tasks related to distrust scenario in the No Weapon and Weapon groups.

Alternate Hypothesis: $H_1$: The mean of the number of repetitions to complete the tasks related to distrust scenario in the Weapon group is greater than the mean of the number of repetitions of the tasks related to distrust scenario in the No Weapon group.

In Microsoft Excel for 95% confidence ($\alpha=0.05$) a two-tail two-Sample t-Test assuming unequal variances indicates a p-value of 4.73E-07 for a one-tail two-Sample t-Test assuming unequal variances. The p-value indicates that we can reject the null hypothesis with a confidence of 95% and hence it can be concluded that there is sufficient evidence that the mean of the number of repetitions for the Weapon Group is greater than the mean of the number of repetitions for the No Weapon Group for the fourth Scenario.
5.4.3 Hypothesis (12)

Null Hypothesis: $H_0$: There is no significant difference between the means of the time taken to complete the tasks related to distrust scenario in the No Weapon and Weapon groups.

Alternate Hypothesis: $H_1$: The mean of the time taken to complete tasks related to distrust scenario in the Weapon group is greater than the mean of the time taken to complete tasks related to distrust scenario in the No Weapon group.

In Microsoft Excel for 95% confidence ($\alpha=0.05$) a two-tail two-Sample t-Test assuming unequal variances indicates a p-value of 0.47 for a one-tail two-Sample t-Test assuming unequal variances. The p-value suggests that there is no sufficient evidence to reject the null hypothesis with a confidence of 95%. Hence it cannot be proved that the mean of the total time taken to complete the task by Weapon group is greater than the mean of the No Weapon group.
5.4.4 Hypothesis (13)

Null Hypothesis: \( H_0: \) There is no significant difference between the means of the user confidence ratings related to distrust scenario in the No Weapon and Weapon groups.

Alternate Hypothesis: \( H_1: \) The mean of the user confidence ratings related to distrust scenario in the No Weapon group is greater than the mean of the user confidence ratings related to distrust scenario in the Weapon group.

In Microsoft Excel for 95% confidence (\( \alpha=0.05 \)) a two-tail two-Sample t-Test assuming unequal variances indicates a p-value of 0.024 for a one-tail two-Sample t-Test assuming unequal variances. The p-value suggests that we can reject the null hypothesis with a confidence of 95% and hence it can be concluded that the users’ confidence on successfully performing the task in the No Weapon Group is greater than that of the Weapon Group.
5.5. Summary of Hypothesis Testing

The following were the deductions made from the Hypothesis tests conducted in the previous section.

Scenario to assess Distraction:

- Hypothesis 1: There is no significant difference between the time taken to complete a task related to distraction between the Weapon and No Weapon group.

Scenario to assess Confusion:

- Hypothesis 2: The mean of user confidence ratings for the No Weapon Group is greater than the mean of user confidence ratings of the Weapon Group.
- Hypothesis 3: The mean of the number of repetitions for the Weapon Group is greater than the No Weapon Group.
- Hypothesis 4: The mean of the total number of emails exchanged were higher in the Weapon Group when compared to the No Weapon Group.
- Hypothesis 5: There was no sufficient evidence to prove that the mean of Time taken to complete tasks related to Scenario 2, was greater in the Weapon group when compared to the No Weapon group.

Scenario to assess Deception:

- Hypothesis 6: There is no sufficient evidence to prove that the means of user confidence rating are different for the Weapon Group and No Weapon Group.
- Hypothesis 7: The means of number or repetitions are different for the Weapon and No Weapon Group.
- Hypothesis 8: There is no sufficient evidence to prove that the means of the number of emails exchanged for the No Weapon and Weapon groups are different.
• Hypothesis 9: There is no sufficient evidence to prove that the means of the total time taken to complete the tasks related to Scenario 3 are not equal for the No Weapon Group and the Weapon Group.

Scenario to assess Distrust:

• Hypothesis 10: The mean of the number of repetitions for the Weapon Group was greater when compared to the mean of the number of repetitions of the No Weapon Group.

• Hypothesis 11: The mean of the number of emails exchanged within the Weapon group is greater than the mean of the number of emails exchanged in the No Weapon Group.

• Hypothesis 12: There was no sufficient evidence to prove that the mean of the total time taken to complete tasks related to distrust scenario is higher in the Weapon Group when compared to the No Weapon Group.

• Hypothesis 13: The mean of participant’s confidence in the in the distrust scenario was greater in the No Weapon Group when compared to the Weapon Group.
<table>
<thead>
<tr>
<th>Scenario\Effect</th>
<th>Total Time to complete tasks</th>
<th>Number of Repetitions</th>
<th>Number of emails exchanged</th>
<th>User Confidence Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distraction</td>
<td>✗</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Deception</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Distrust</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Confusion</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 3: Scenario to cyber effect mapping of the results.

- ✗ - Indicates that the hypothesis test result was not in accordance with the assumption.
- ✓ - Indicates that the result of hypothesis test was in accordance with the assumption.
- N/A - Not Applicable.

5.7. Questionnaire Data

A post questionnaire was given to the subjects after finishing the experiment which asked basic demographic information and their levels of comfort using online websites to shop etc. The details of the analysis of this questionnaire are documented below and illustrated in Figure 28.
The ethnicity, gender and age information were collected as a part of the questionnaire. The distribution seems to be varied. There were 9 Whites, 9 Asians, 1 Hispanic and 1 Black / African American who participated in the study. 12 Males and 8 Females participated in the study and the almost all subjects were within the 20 – 40 years of age, with one subject in the 10 – 20 years age range and another subject in the 40 – 60 years range.

For a question on whether they were able to finish all tasks assigned to them 85% replied in the affirmative and 15% said that they weren’t able to finish their tasks. For a question on
whether the instructions of the experiment were laid out clearly, 95% answered “yes” and 5%
said “no”.

95% of the subjects were very comfortable in searching for information online, the rest were
comfortable. About 90% answered that they use internet for shopping regularly. The rest
answered they use internet once in a while.

Most of the subjects use all the sites mentioned in the options such as Google, Expedia,
Orbitz etc. Some subjects mentioned that they use Kayak because it summarizes the prizes of all
the deal sites. 95% of the subjects use spreadsheet applications daily. 75% of the subjects said
they were comfortable with the overall experiment, 10% said they were fairly comfortable and
15% said that they were not comfortable in doing the experiment.

5.8. Discussion

The results from scenario of distraction were not consistent with the hypothesis predicted.
This might have been because the time calculated was almost similar, and whenever pop-ups
were introduced as a medium to distract users, they would often choose to just close the pop-ups
and not follow the lead. The results from confusion, distrust and deception scenarios were found
to be consistent with the hypotheses except for the time dimension. Although it virtually
appeared that the Weapon group was taking more time when compared to the No Weapon group
in such scenarios, when it came to actually comparing the data, the difference was in mere
seconds, which might have resulted in a low margin of difference, thus failing the hypothesis
test. Through this experiment, we were successfully able to prove that the number of repetitions
of a user’s action in a task, user confidence rating and number of emails exchanged in a task
could be significant indicators of user behavior to test the effects of cognitive cyber weapons in a
cyber warfare scenario. This research could be used as a preliminary step in understanding and
developing more complex cyber warfare scenarios using the Cognitive Cyber Weapon Selection Tool test bed. Such research would benefit the cyber operator, who could make weapon deployment decisions in split second to employ a specific set of weapons to induce a very specific alteration in the adversary’s cognitive thought process.

5.9. Future Research

There is a need to develop and enhance the current evaluation parameters available and to validate if such parameters are context specific and change with context or they are generic. Further research can develop a repository of cognitive weapons which could suggest a list of cognitive weapons based on the wartime situation for the cyber operator to choose from. This could have a tremendous potential as a cognitive weapon decision engine, which learns from the operator’s history of deployments. The tool could also help us understand the underlying patterns associated with trust and team situational awareness in complex real time warfare situations.


Dr. Schultz, E. (. (2003). *Pandora’s Box: spyware, adware, auto-execution*. NGSCB.


ACM.


xii


APPENDIX – A

Instructions for the Experiment

Objective: A team of two participants must plan and finalize a travel itinerary consisting of airline travel and lodging information from Columbus to Cincinnati.

Instructions:

***The participants should strictly adhere to the instructions provided in this document.

The users are permitted to use only Internet explorer, Excel to check and document travel details.

The users are allowed to use only e-mails to communicate. Any sort of verbal communication with other participants is not allowed.

The principal investigator will not be able to answer any questions after the commencement of the experiment.

A minimum of two e-mails are to be sent after completion of every task. The first e-mail will include information of the flight and price details and the second e-mail is an acknowledgement that you have received your partner’s information.

You must look for the lowest price for the specified air route and enter the details in the Microsoft Excel document “Flight_Details_Template.xlsx” after every task.

If you are not able to perform a certain task due to any reasons, you can confirm the abnormality with your partner. After attaining a common consensus, the task can be skipped and the next task can be started.
**Scenario**

You and your partner are invited to a one-day conference in September at Cincinnati (CVG, OH). You need to start at Columbus (CMH, OH) to attend the conference. Your adviser has asked you to send in the lowest flight prices to cover your expenses for the trip. You are to compare the best prices in several deal sites to find the flight with the lowest price. Your objective in this study is to visit all the deals sites specified in the tasks and come up with the information that’s been asked for. You also need to document the details in an Excel Template provided to you on the desktop of your computer. In the last task, you are supposed to attach the Excel Document to your e-mail and send it to the other partner for one final confirmation that the details are all correct.

**Task 1**

The participant is to look for the cheapest flight from CMH to CVG at Expedia. The options that need to be selected are tabulated below.

Open Internet Explorer browser window.

Type [http://www.expedia.com](http://www.expedia.com) in the address bar and enter the following search parameters. Click “Search for Flights”.

Search Parameters:

- One way trip
- Leaving From : CMH (Columbus)
• Going To: CVG (Cincinnati)
• Departing: 9/12/2010
• Time: Any
• Adults: 2
• Seniors: 0
• Children: 0

Enter the lowest price details in the “Flight_Details_Template.xlsx” document on the Desktop.

Save changes.

Open the website http://www.gmail.com in the Internet Explorer browser window.

Use the following username and password to login.

Username: _________________

Password: _________________

Compose an e-mail to send the information of flight search to your partner.

Your partner’s e-mail id is ____________________

Acknowledge the e-mail sent by your partner to you by replying to your partner’s e-mail. If you didn’t receive an e-mail from your partner wait for his/her e-mail. Once received, check if all the information is same when compared to your information. If not exchange information mutually until both of you know that you have the lowest price. Stop exchanging e-mails after you have reached a common consensus on the least price value.
Sending Emails:

This is the snapshot of the first e-mail which has to be sent to your partner.

This is a snapshot of the acknowledgement e-mail that has to be sent.
After the acknowledgement e-mail compare the values of your partner’s e-mail with your e-mail to see if the prices are the same. If your price is lower than your partner’s, send an e-mail to your partner that their document to reflect the lowest price value.

If your price is higher than your partner’s, wait for the e-mail from your partner to make the necessary changes to your excel document.

Make sure that the description of the problem should not exceed two lines in length in the e-mail.

Close the Excel Document and any Internet Explorer browser windows which are open.

This ends the first task in the experiment.

Question:

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option

1 2 3 4 5 6 7 8 9 10

Task 2

The participant is to look for the cheapest flight from CMH to CVG at Travelocity. The options that need to be selected are tabulated below.

Open Internet Explorer browser window.

Type http://www.travelocity.com in the address bar and enter the following search parameters. Click “Search for Flights”.

Search Parameters:
• One way trip
• Leaving From: CMH (Columbus)
• Going To: CVG (Cincinnati)
• Departing: 9/12/2010
• Time: Any
• Adults: 2
• Seniors: 0
• Children: 0

***If you are not able to search for flights or face any issues, re-start the browser window and try repeating the search. If there are still issues, repeat one more time to confirm and skip this task to go to the next task.

Send an e-mail to your partner with the flight search details as in the previous task.

Acknowledge the e-mail sent by your partner to you and check if all the information is matching. If not exchange information mutually until both of you know that you have the lowest price. Stop exchanging e-mails after you have reached a common consensus.

Change the value in the Excel Document to the price which is the lower of the two.

Close the Excel Document and any Internet Explorer browser windows which are open.

This ends the second task in the experiment.

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Task 3
The participant is to look for the cheapest flight from CMH to CVG at Orbitz. The options that need to be selected are tabulated below.

Open Internet Explorer browser window.

Type http://www.orbitz.com in the address bar and enter the following search parameters. Click “Find”

Search Parameters:

- One way trip
- From : CMH (Columbus)
- To: CVG (Cincinnati)
- Leave: 9/12/2010
- Return: 9/13/2010
- Time: Anytime
- Rooms: 1
- Adults: 2
- Children: 0

Send an e-mail to your partner with the flight search details as in the previous task.

Acknowledge the e-mail sent by your partner to you and check if all the information is matching. If not exchange information mutually until both of you know that you have the lowest price. Stop exchanging e-mails after you have reached a common consensus.

Change the value in the Excel Document to the price which is the lower of the two.

Close the Excel Document and any Internet Explorer browser windows which are open.

This ends the third task in the experiment.

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option
Task 4

The participant is to look for the cheapest flight from CVG to CMH at Expedia. The options that need to be selected are tabulated below.

Open Internet Explorer browser window.

Type http://www.expedia.com in the address bar and enter the following search parameters. Click “Search for Flights”.

Search Parameters:

- Check Flight
- Select “One way”
- From: CVG (Cincinnati)
- To : CMH (Columbus)
- Departing: 9/12/2010
- Time: Anytime
- Adults: 2
- Seniors: 0
- Children: 0

Send an e-mail to your partner with the flight search details as in the previous task.
Acknowledge the e-mail sent by your partner to you and check if all the information is matching. If not exchange information mutually until both of you know that you have the lowest price. Stop exchanging e-mails after you have reached a common consensus.

Change the value in the Excel Document to the price which is the lower of the two.

Close the Excel Document and any Internet Explorer browser windows which are open.

This ends the fourth task in the experiment.

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

Task 5

The participant is to look for the cheapest “flight” from CVG to CMH at Travelocity. The options that need to be selected are tabulated below.

Open Internet Explorer browser window.

Type [http://www.travelocity.com](http://www.travelocity.com) in the address bar and enter the following search parameters. Click “Search”.

Search Parameters:

- Check “Flight only”
- From: CVG (Cincinnati)
- To : CMH (Columbus)
- Select “Exact Dates”
- Depart: 9/12/2010
- Time: Any
- Adults: 2
- Seniors: 0

Send an e-mail to your partner with the flight search details as in the previous task.

Acknowledge the e-mail sent by your partner to you and check if all the information is matching. If not exchange information mutually until both of you know that you have the lowest price. Stop exchanging e-mails after you have reached a common consensus.

Change the value in the Excel Document to the price which is the lower of the two.

Close the Excel Document and any Internet Explorer browser windows which are open.

This ends the fifth task in the experiment.

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

**Task 6**

The participant is to look for the cheapest flight from CVG to CMH at Delta. The options that need to be selected are tabulated below.

Open Internet Explorer browser window.
Type [http://www.delta.com](http://www.delta.com) in the address bar and enter the following search parameters. Click “Search for Flights”.

Search Parameters:

- Check “Round-trip”
- From: CVG (Cincinnati)
- To: CMH (Columbus)
- Leave: 9/12/10
- Return: 9/13/10
- Time: Anytime
- Adults: 2

Send an e-mail to your partner with the flight search details as in the previous task.

Acknowledge the e-mail sent by your partner to you and check if all the information is matching. If not exchange information mutually until both of you know that you have the lowest price. Stop exchanging e-mails after you have reached a common consensus.

Change the value in the Excel Document to the price which is the lower of the two.

Close the Excel Document and any Internet Explorer browser windows which are open.

This ends the sixth task in the experiment.

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option
Task 7

In this task, attach your excel document to your email and send it to your partner. Open your document and review the details and compare with your partner’s document. See if the values match. Arrive at a common consensus on the lowest price for flights from CVG to CMH and CMH to CVG.

This ends the seventh task in the experiment.

Please rate your confidence about your performance in this task on a scale of one 1 to 10, 1 being “Not confident” and 10 being “Highly confident”. Circle the option

1 2 3 4 5 6 7 8 9 10
APPENDIX – B

Questionnaire

Questionnaire for CCWST Empirical Evaluation Procedure experiment

1. Please provide the following information:
   - Please tick your relevant age group
     - 10 – 20 years
     - 20 – 40 years
     - 40 and above
   - Gender:
     - Male
     - Female
   - Ethnicity:
     - Hispanic
     - American Indian
     - Asian
     - Black or African American
     - Native Hawaiian or Pacific Islander
     - White

2. Were you able to achieve all the objectives designated to you during the allotted time?
   - Yes
   - No
3. Were the tasks outlined for you during the experiment clear?
   - Yes
   - No

4. How comfortable are you with searching for information online?
   - Very comfortable
   - Comfortable
   - Not comfortable

5. How often do you use the internet for shopping online?
   - Regularly
   - Once in a while
   - Do not use internet for shopping online

6. Which of the following options do you use to search for best deals on air tickets online?
   - Search engines (Google, Bing, etc.)
   - Travelocity
   - Expedia
   - Orbit
   - Others (Please mention if other) _____________________

7. What other media of communication other than e-mail would you use to communicate with your partner?
   - Instant messaging (Chat)
   - Social networking sites (Scraps, Writing on wall etc.)
8. How often do you use spreadsheet applications (MS Excel etc.) in your daily activities?
   - Daily
   - Once in a while
   - Do not use spreadsheet applications.

9. How comfortable were you with the overall experiment?
   - Very comfortable
   - Fairly comfortable
   - Not comfortable