Cybercrime, Censorship, Perception and Bypassing Controls: An Exploratory Study

Ibrahim Baggili[1], Moza Al Shamlan[2], Bedoor Al Jabri[2], and Ayesha Al Zaabi[2]

[1] Tagliatela College of Engineering, Department of Electrical and Computer Engineering
and Computer Science, University of New Haven, CT
Ibaggili@newhaven.edu
[2] Zayed University, College of Technological Innovation
Advanced Cyber Forensics Research Laboratory
m80001612@zu.ac.ae, {budur44,ayesha.alzaabi}@hotmail.com

Abstract. Countries have employed the Internet proxy as a censorship mechanism for various reasons. Concurrently, cyber criminal activities continue to rise. This research explores peoples' engagement in bypassing the Internet proxy and if it is related to cyber criminal engagement. Through an experimental design, participants were randomly assigned to three groups. Using manipulation paragraphs, in the first group (Group 1), a positive view on the Internet proxy was presented. In the second group (Group 2), a negative view on the Internet proxy was presented. The third group (Group 3) was used as the control group, where the participants' view of the Internet proxy was not manipulated. All three groups were asked to self-report their rate of proxy bypass (SRPBE) and cybercrime engagement (CCI). The results indicated a significant positive correlation between self-reported cyber criminal engagement and self-reported proxy bypass engagement. The results also showed that individuals with more knowledge in computers are more likely to bypass the Internet proxy. However, individuals with better knowledge in computers are not necessarily the ones that are more likely to commit cyber criminal activities. The results were inconclusive on whether or not the manipulation paragraphs used had an effect on the participants' view of the Internet Proxy.

Keywords: Cybercrime, psychology, censorship, Internet proxy, UAE.

1 Introduction

With time the Internet continues to grow. More users today are engaged in the World Wide Web and are actively infused with this technology. The Internet World Stats website reveals the number of increasing Internet surfers in different regions of the world. Data also reveals that there are about fifty seven million surfers in the Middle East alone. In the case of the United Arab Emirates (UAE), it was determined that it has the fifth highest number of Internet users amongst other Middle Eastern countries [1]. Furthermore, it is one out of a number of countries that applies an Internet proxy to censor Internet content.

The reasons behind the employment of an Internet proxy may vary. In the UAE, the purpose could range from religious, to social, to political reasons [2]. One of these

M. Rogers and K.C. Seigfried-Spellar (Eds.): ICDF2C 2012, LNICST 114, pp. 91–108, 2013.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2013

reasons could also be to prevent cyber criminals from accessing and downloading hacking and exploitation tools. For example, when attempting to visit the website http://remote-exploit.org, a website that contains software that could be used for malicious purposes, we find that the Internet Proxy in the UAE prohibits access to such a website. If a primary reason for censoring Internet content is to prohibit users that are actively engaged in cybercrime from downloading hacking tools and content, it becomes important to investigate the relationship between bypassing the Internet proxy and cybercrime engagement.

Internet censorship remains a topic of debate despite the many reasons behind why an Internet proxy is applied. In the UAE for instance, Sheikh Abdulla Bin Zayed, Minister of Information and Culture is in favor of an open Internet, for he states that the UAE's Internet Service Providers should not block access to websites because every citizen is entitled to knowledge and learning [3].

Due to the restricted Internet access in the UAE, it is hypothesized that users may engage in ways to bypass the Internet proxy. The purpose and intentions behind such user activity is yet to be empirically examined. Understanding this relationship can shed light on the effectiveness of the Internet proxy, and whether it is fulfilling the purpose of evading cyber criminals from accessing illegal content.

2 Problem Statement

One of the reasons of employing an Internet proxy is to not only censor illegal content, but also to curb cyber criminal engagement. Currently, there is no formal published research that studies the relationship between cyber criminal engagement and proxy bypass engagement. It is important to study this relationship in order to validate the productivity of the Internet proxy.

3 Research Questions and Hypotheses

In this study, the researchers attempted to answer the following questions:

- Is there a relationship between Self Reported Proxy Bypass (SRPB) and cybercrime engagement?
- Is there a relationship between the level of knowledge in computers and SRPB?
- Can respondents be manipulated using manipulation paragraphs to affect their perception of the employment of an Internet proxy?

To answer the abovementioned questions three major hypotheses were formulated:

- H1: There is a positive correlation between self-reported cybercrime (CCI) and self-reported proxy bypass engagement (SRPB).
- H2: Individuals with better knowledge in computers are more likely to bypass the Internet proxy and engage in cybercrime.
- H3: Decreasing the positive perception of the Internet proxy increases self reported cybercrime and proxy bypass engagement.

4 Literature Review

4.1 Censorship and The Internet Proxy

Censorship is a widely implemented practice. Censorship is "The restriction of what people may say, hear, write, read, or see" [4]. The Fileroom website, an archive of various materials lists censored cases in different regions of the world (thefileroom.org). This website, in partnership with the National Coalition against Censorship (NCAC) aims to fight types of censorship that may violate the right of human expression. On the other hand, there are supporters of censorship, which are those who are usually applying it, which in many cases is the government, special interest groups, or individuals. Organizations and people that are pro-censorship look at it from a different perspective mostly perceiving it as a security measure to ensure the wellbeing and morals of societies [4].

There are different types of censorship ranging from censorship in tangible material such as books and magazines, to intellectual ideas, services, and the placement of restricting rules and regulations that prohibit people from exercising a particular action. When it comes to censorship of the Internet, the United Arab Emirates (UAE) is in the top ten ranks according to a research that The National newspaper has reviewed, along with China, Iran and Saudi Arabia. This list also includes the United States, Germany, France, Canada, Tunisia, and Bahrain [5]. For instance, Chinese Internet Service Providers (ISPs) censor topics like Tibet, Taiwan and Tiananmen (for political reasons), and even high profile websites like BBC and Voice of America. Moreover, the Iranian government censors content that may include pornography, politics, religion, and anything that may have a heavy western influence like music, videos or movies; resulting in a 10+ million blocked websites ranging from Wikipedia to YouTube to Amazon. Also, the Saudi Arabian government put a ban on any anti-Islamic websites along with women's rights topics, gambling and pornography. The above mentioned countries are only a small sample of nations that apply censorship [6].

Although the stated reasons behind applying censorship may seem to be moral, there may be a dual purpose. For example, although Internet censorship may be perceived as a way of protecting children from "dangerous or disturbing ideas and information" [7], others may think of it as an effective way of controlling people's minds. If we look at the cases of different countries, nations propose independent reasons behind applying Internet censorship. For example, in the UAE, if you try to access a blocked website, the following message appears on the browser: "Access to this site is currently blocked. This site falls under the prohibited content categories of the UAE's Internet Access Management Policy". The prohibited content categories are provided, and the reasons behind blocking a website can be political, social, cultural, or religious.

Censorship is an old concept and has been around for many years. Censoring may include the destruction of a certain work, banning it, or making it illegal to produce or sell [8]. In the following part of the literature review, censorship examples are discussed with relation to criminal activities.

Looking back at the second World War, Hitler, for instance, applied censorship and banned various books for the sole purpose of implementing a “Totalitarian philosophy” [9]. He attempted to control what the people in Germany read, how they thought, and what they believed in. The employment of his philosophy shifted people’s beliefs. Although he was a powerful man and tried to indoctrinate people’s minds with his ideology, many had opposed him. In reality, many had planned conspiracies and assassinations in hopes of terminating Hitler and his regimes [10].

In the 1970’s, alcohol was prohibited in the United States by the 18th amendment. During the World War, people felt the need to become patriotic and consume their time in conserving grain, rather than drinking alcohol. This prohibition led to organized crime [11]. Large quantities of alcohol were smuggled in from Canada, overland and via the Great Lakes [12], thus indicating how the alcohol ban led to an increase in the rate of crime and illegal activities.

In 1979, the Chinese government decided to restrict the number of people in Chinese families and allow most of them to only have one child; they called it the one-child policy [13]. The population of Chinese people made up a quarter of the world’s population when they were only using seven percent of the land on earth. This rise in the population was because of Mao Zedong who led the Chinese people into giving birth to as many children as possible between 1950 and 1960 to bury the United States in a human wave [14]. Although the one-child policy prevented at least 300 million births, and boosted prosperity [14], it led to a gender disproportion in the population. Since the Chinese society tends to favor a male inheritor, this led to the abortion of many female babies [15]. The policy in place led to illegal activities such as infanticide, human trafficking, having illegal children and sending them off to isolated regions where they cannot be found, and girls being picked up by gangs to be used for banned activities [16]. Despite the primary goal that was set behind applying this ban or policy, there is an indication of the rise in illegal activity due to the restrictions that this policy has placed upon the people of China.

In the mid nineteenth century, abortion in the United States was illegal. In addition to it being a crime at the time, it was perceived to be a sin as well [17]. Although abortion was prohibited, women always found a way around that. NARAL, which is a pro-choice American Foundation mentions an excerpt of a story from the book “Women speak out about abortion”. The passage indicates how women had sought illegal abortion, even in poor hygienic conditions, in order to secretly abort unwanted children [18]. Although abortion was illegal, it was discovered that about a million illegal abortions a year were performed in the U.S. [17], thus indicating how the employment of this law had failed to serve its purpose, and resulted in the increase of secretly performed abortions.

In the U.S., the government’s interference in banning certain violent video games is questioned. It has been stated that there is weak evidence with regards to the link between video games and youth aggressiveness; even when the video game industry was booming between 1994 and 2000, a decrease in the rate of crime was witnessed, [19] (this does not necessarily eliminate the relation between those two elements, yet it sets a possible indication of their negative correlation). One research study on the relationship between violent video games and its effect on children was conducted.

This research suggested that conducted experiments have proved the following similar results: "playing violent video games can indeed cause increases in aggressive thoughts, feelings and behaviors" [20]. Despite the findings of this research there is still controversy over this topic.

Censoring violence in media has also been a topic of debate. Those supporting this type of censorship are concerned about its effect on those watching such violence on television. Scientific studies have shown the connection between violence and media violence, but they have not been able to show a causal relationship between the two [21]. Despite the uncertainty of this relationship, the research emphasizes its negative effect on children. Opponents believe that despite the large number of research conducted on violence in the media, very few studies look into this issue in real life. One study was conducted by Dr. Brandon Canterwall in three countries (Canada, U.S., and South Africa) in order to identify the connection between media violence and the rate of crime. The study was conducted from 1945 to 1974 when the television was first broadcasted in the U.S. and Canada, yet banned in South Africa. In the U.S. and Canada, homicide rates doubled when television was first introduced, yet the rates remained stable in Africa [22].

Censorship and bans on literature and media are merely a barrier for some people; a barrier which can be almost always be overcome. When it comes to books that have been banned for political or social reasons, one can merely find an online book store from which to purchase the book, whether it be a physical copy or an electronic copy. In fact, there was a website dedicated to that purpose; Banned-Books.org. This website was an online bookstore that sold banned books, audiotapes and videos [23]. There have also been events protesting the banning of books, such as Banned Books Week, which has been an annual celebration of the "freedom to read" since 1982. The organization hosts events nation-wide across the United States where bookstores welcome authors that have been subject to censorship to read their books in the bookstores and to speak about being censored [24].

Newspapers or magazines may either be banned or contain censored articles within the printed pages because they could be culturally offensive, religiously unacceptable, or harmful to the image of political or royal persons. If this is the case, then individuals seeking the non-censored versions may be able to find it on the Internet, and in most cases, newspaper or magazine websites are not censored. "And so, if the government wants to ban the Sunday Times from the newsstands, it should block its website too. Or, of course, do neither." [25].

In certain countries, movies showing at the cinemas or aired on television that contain extremely violent or sexual scenes are usually only shown after those scenes have been censored. The same is applied to music videos. Some music videos may not be shown on television because of their highly suggestive nature. This is easily circumvented by either purchasing a DVD (which in most cases are not censored), viewing them online through an illegal video streaming website, illegally downloading the movies, and downloading the censored scenes from file sharing or peer-to-peer services.

Most of the aforementioned examples illustrate a relationship between bans and undesired activity. However, until now, no research in the UAE has been conducted with regards to the relationship between the Internet proxy and cyber criminal engagement. In this research, the aim is to reveal the nature of this relationship, and it is hypothesized that like most of the examples illustrated above, that cyber criminal engagement is positively correlated with bypassing the Internet proxy. This hypothesis is primarily based on the “all that is banned is desired” principle, and the idea that obstructing the freedom of users will trigger illegal activity or cybercrime.

4.2 Cybercrime

The UAE is ranked second as the most vulnerable of the Gulf countries to fall victim to cybercrimes. The world is more connected than ever before, and the credit goes to technology, because with its positive use arose its misuse. Therefore, studying cybercrime in the UAE is of critical importance.

We ask ourselves: What is cybercrime? A clear-cut definition does not exist, yet we know it when we see it, or when we experience it. There have been many attempts at defining cybercrime. For example, in the book Cybercrime: vandalizing the Information Society, the author differentiates between computer crime and cyber crime. Computer crime is “a crime in which the perpetrator uses special knowledge about computer technology”, whereas cybercrime is “a crime in which the perpetrator uses special knowledge of cyberspace” [26]. Shinder (2002) also explains that there are different categories of cybercrime. Mainly, there are two basic categories: Violent and non-violent cybercrime. Under each category, different types or subcategories were suggested. Under non-violent cybercrime; cyber trespass, cyber theft, cyber fraud, and destructive cybercrime. On the other hand, violent cybercrime encompasses cyber terrorism, assault by threat, cyber stalking, and child pornography [26].

In 2002 Furnell further illustrates the public’s attitude and awareness of the cybercrime issue. A survey was conducted in the U.K. in order to determine the degree of the public’s understanding of cybercrime and how the media has played a role in shaping that understanding. Consequently, the survey addressed questions that revolved around three main issues: using unlicensed software, unauthorized use of IT facilities, and password sharing. The survey indicated that the participants were involved in the three activities to some extent. However, despite the respondents’ engagement in those issues, over 80% of the participants acknowledged that they understand that their actions result in cybercrime [27].

The aforementioned results of the survey conducted in the U.K. reveal people’s acknowledgement of the cybercrime issue, yet they still practice it. Why do people commit cybercrime? What is their motive or personal reasoning? Can their perceptions be affected in order to halt this activity? An article mentions various reasons of engaging in cybercrime, ranging from a user’s excitement to challenge him/her self, ease of anonymity, to holding a grudge [28]. Although individuals may engage in such activities for different reasons, manipulating perception may have an effect on users’ ideas of this activity.

4.3 Perception

Scientifically, perception is the way people interpret what they sense in the environment around them; the way they view the world [29]. Perceptions are provisional much similar in the way in which scientific hypotheses are provisional; as in peoples' perceptions of anything around them changes when they learn new information about them [30].

Any information that people gather or are given can change the way they view a certain object or idea. Peoples' perceptions are easily molded and changed both directly and indirectly. John Stauber and Sheldon Rampton wrote a book unfolding and describing what it takes to create public opinion, as well as revealing evidence of opinion manipulation from the early 20th century [31].

Edward Bernay states in his book Propaganda that "scientific manipulation of public opinion was necessary" and determined that "a relatively small number of persons pull the wires which control the public mind" [32]. He, in fact, was one of those individuals that formed peoples' opinions about numerous concepts and products in the United States. Examples of which range from promoting bacon as breakfast food, popularizing smoking cigarettes among women, to presenting the first World War as a positive concept that benefits the world [31].

The media especially plays an enormous role in influencing peoples' perceptions about ideas. Perception manipulation has been practiced in all forms of media. Some even say the type of medium chosen in order to get a message across may even be more important than the message itself [33-34]. Ultimately, it will get the desired effects.

Ball-Rokeach and DeFleur (1976) state that "audience dependency on media information resources [is] a key interactive condition for alteration of audience beliefs, behavior, or feelings as a result of mass communicated information" [35]. Today's media is no longer constrained to television, radio and print magazines. It seems to be fast-paced, unstoppable and unrestrained. The properties that make up what global media resulted in an almost involuntary reaction which is the manipulation of the public's opinion and behavior [36].

Johnson in 2007 set an example of such impact of perception manipulation once again but from a military viewpoint. The simple manipulation of a "flash of an image" such as images of dead women and children can change the public's perception of war. When war is depicted in such a way, people are influenced into considering how negative war is, and pushes back the idea of any benefits that war may bring [36].

Experimental research has grown more popular and prevalent in social psychological research. In this kind of research, components include a manipulation of at least a single independent variable, and the randomized assignment of participants of the research to the manipulation or condition [37].

For example, there are numerous examples of manipulation within medical experiments and research. Influencing patients into believing they are receiving treatment (when in reality they are not) can result in change in their behavior and in cases even cause physical change. This goes to show that one's perception can be molded into something that may contradict one's original ideas, beliefs, and even reality.

In one study by Massachusetts Institute of Technology scientists, it was shown that magnetic fields can alter human brain operation; more specifically their moral judgment. The groups of subjects in the experiment were asked to read short stories and were then asked to decide whether the actions of the characters in the stories were morally acceptable or unacceptable. One group was then subjected to transcranial magnetic stimulation, while another was not. The temporary stimulation appears to have changed the answers of the first (manipulated) group where the results showed that the subjects were indecisive about what was morally acceptable or unacceptable, and that they focused on the outcome of the story as opposed to the intention of the characters in the stories [38].

The University of Harvard conducted research that explored how effective the placebo effect can be on people that suffered from pain, arterial hypertension and asthma. Some subjects were given the actual medication, while another group of subjects were not given any medication, and instead given a pharmacologically inactive substance, but were led to believe that they were given legitimate medication. Approximately 40% of the subjects who were administered fake medicine indicated that they felt relief from their physical pain [39].

Other instances in the medical field that experiment with the use of the placebo effect include surgical procedures as well. Hospital patients suffering from chest pain caused by chronic heart ischemia were separated into two groups: those who underwent the surgical procedure to rectify it, and those who were only led to believe that they had the procedure done (by preparing them for the operation, sedating them, and incising their skin so it appears that they have gone through surgery). Those who were operated on legitimately showed 40% improvement, while those who went through the "pretend" surgery showed 80% improvement, [39]. Again, this demonstrates the power of manipulation of people's perception.

5 Methodology

This study uses an experimental approach. Participants were randomly assigned into three groups. In the first group (Group 1), a positive view on the Internet proxy was presented. In the second group (Group 2), a negative view on the Internet proxy was presented. The third group (Group 3) was used as the control group, where the participants' view of the Internet proxy was not manipulated. All the participants in each group were asked to complete two self-reported instruments CCI which represents an index measure of cyber criminal engagement and SRPBE which aims to measure the engagement of the participants in bypassing the Internet proxy. All participants were also asked a single question about their level of knowledge of computers. The responses were analyzed in order to test the following hypotheses:

H1: There is a positive correlation between self-reported cyber crime (CCI) and self-reported proxy bypass engagement (SRPBE).

H2: Individuals with better knowledge in computers are more likely to bypass the Internet proxy and engage in cyber crime.
H3: Decreasing the positive perception of the proxy increases self reported cybercrime.

5.1 Theoretical Constructs

Figure 1 illustrates the different variables and predictors in this research. The two predictors are Proxy Bypass Engagement and Proxy Perception. The independent variable is self-reported cybercrime engagement.

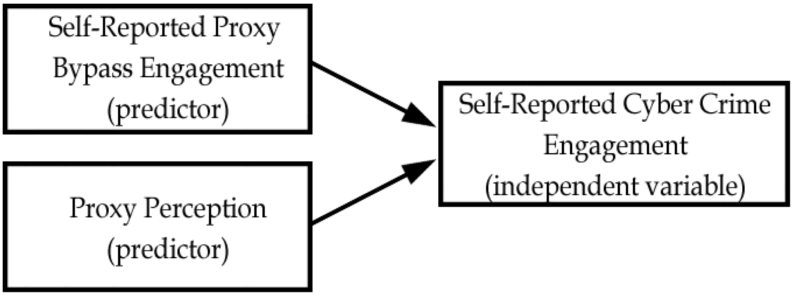

Self-Reported Proxy Bypass Engagement (predictor)
Proxy Perception (predictor)
Self-Reported Cyber Crime Engagement (independent variable)

Fig. 1. Theory diagram

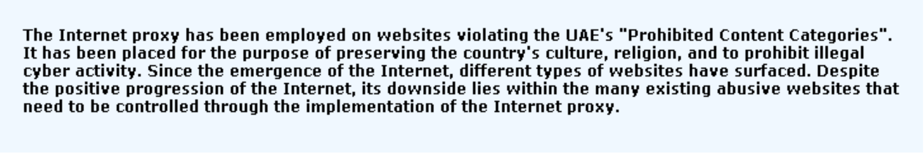
5.2 Instruments

5.2.1 Proxy Bypass

The researchers created this self-reported measure in order to compare its relationship with self-reported cybercrime. The survey encompasses questions around the respondents' degree of proxy bypass engagement. The types of questions used were meant to reveal the degree to which the participants were involved in proxy bypass, and the reasons behind their engagement in this activity (to challenge one's skills, access certain websites, or for malicious reasons). A measure for each respondent was then created in order to assess each participant's level of bypassing the Internet proxy.

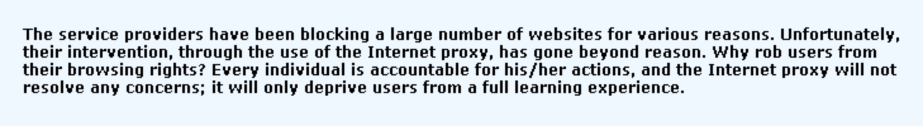
5.2.2 Proxy Perception

This survey instrument was disseminated to three separate groups in which the "manipulation page" was phrased in a manner that either advocated the employment of the proxy (Group 1), criticized it (Group 2), or the survey was distributed without any prior effort of manipulation (Group 3, control group). The aim of the first two groups was to attempt to create a biased opinion, in a positive or negative manner, so as to find out whether the "manipulation page" would influence participants' perception of the proxy. The manipulation paragraphs used are shown in Figures 1 and 2.



The Internet proxy has been employed on websites violating the UAE's "Prohibited Content Categories". It has been placed for the purpose of preserving the country's culture, religion, and to prohibit illegal cyber activity. Since the emergence of the Internet, different types of websites have surfaced. Despite the positive progression of the Internet, its downside lies within the many existing abusive websites that need to be controlled through the implementation of the Internet proxy.

Fig. 2. Positive Manipulation Paragraph



The service providers have been blocking a large number of websites for various reasons. Unfortunately, their intervention, through the use of the Internet proxy, has gone beyond reason. Why rob users from their browsing rights? Every individual is accountable for his/her actions, and the Internet proxy will not resolve any concerns; it will only deprive users from a full learning experience.

Fig. 3. Negative Manipulation Paragraph

5.2.2.1 Self-Reported Cyber Crime

Following the questions around self-reported proxy bypass engagement, participants were also asked to answer questions related to self-reported cybercrime. The self-reported cybercrime survey was originally created by Dr. Marcus Rogers, a professor at Purdue University. The Index measurement was created by Dr. Rogers is an instrument that has been repeatedly used and cited in various studies [40] [41] [42].

6 Research Protocol

6.1 Participants

After seeking ethical clearance, the researchers were able to disseminate a survey to 4,473 e-mail addresses, which included students and faculty. The researchers gathered data for a period of two weeks, and the total number of participants in this study was (n=107) after eliminating 188 participants with incomplete responses 93 of which were females, and 14 of which were males. The program Gpower was used in order to determine the sample size necessary for the study.

- For a one-tailed test, with medium effect size (0.5), an alpha of (0.05) and a power (0.9), the recommended sample size is 140.
- For a two-tailed test, with medium effect size (0.5), an alpha of (0.05) and a power (0.9), the recommended sample size is 172.

It is unfortunate that the sample size the researchers received was not significantly high, becoming a limitation of this study. However, the yielded results illustrate theoretical saturation and a reasonable effect. The authors also note a high dropout rate, and this was expected due to the measurement's length.

6.2 Study Protocol

1. The following process was followed:

   a. Ethical clearance was sought from the university research office.
   b. A pilot survey test was conducted prior to the distribution of the survey.
   c. The emails were randomly assigned to the three different groups. The surveys were then disseminated via email to Zayed University faculty, staff and students.
   d. The consent form was included as the first page of the survey for all participants that would agree to contribute to the study. Participants were instructed to carefully read and agree to the pre-consent forms before beginning the survey. The survey could not be completed if participants did not agree to the consent form.

6.3 Reliability

In order to show that a set of data is internally consistent, it is generally accepted that the reliability measure Cronbach's alpha should be greater than 0.7. In this research, both CCI and SRPBE surpassed 0.7. Consequently, the measurements show a level of acceptable internal consistency. Table 1 illustrates the reliability measure results.

Table 1. Reliability statistics of SRPBE and CCI

Cronbach's Alpha	Variable	N of Items
.929	SRPBE	28
.803	CCI	60

6.4 Data Analysis

After analyzing the data, 188 incomplete responses were eliminated. The data was analyzed using a variety of statistics. Primarily, the data was tested for normality and outliers using Q-Q plots and box plots. It is important to note that a total of 12 responses were eliminated after closely examining the Q-Q and box plots. In order to test whether correlations existed between a set of measures, Pearson's correlation was used. Additionally, Analysis of Variance (ANOVA) was used in order to test the effect of the included manipulation paragraphs in the surveys for groups 1 and 2. After eliminating outliers, the total number of participants was 95.

6.5 Demographics

The demographics were analyzed to gain a better understanding of the sample as shown in Table 2.

Table 2. Sample demographics

Demographic Variable	N of Items	Population %
	Gender	
Females	82	86%
Males	13	14%
	Age	
Less than 17	1	1%
17-20	37	39%
21-25	31	33%
26-30	4	4%
Above 30	22	23%
	Education Level	
High school	8	8%
Undergraduate	59	62%
Graduate	8	8%
Postgraduate	20	21%
	Academic Major/Expertise	
Business	19	20%
Education	13	14%
Liberal arts	8	8%
Health sciences	15	16%
Social sciences	5	5%
IT/ Computers	17	18%
Other	18	19%
	Level of computer knowledge	
Poor	1	1%
Fair	8	8%
Average	33	35%
Good	40	42%
Excellent	13	14%

7 Results and Discussion

7.1 Hypothesis 1

H1: There is a positive relationship between self-reported cybercrime (CCI) and self-reported proxy bypass engagement (SRPBE).

In this research, it was hypothesized that a significant positive correlation would exist between self-reported cyber criminal engagement and self-reported proxy bypass engagement. Table 3 illustrates that a significant correlation does exist between those two variables. A correlation is significant at the 0.01 level, meaning that there is a 99% chance (1-0.01) that the correlation is positive and equal to 0.285.

Table 3. Pearson correlation between SRPBE and CCI

Variables	N	Significance level (2-tailed)	Pearson Correlation
SRPBE x CCI	95	0.05	0.285**

**** The correlation is significant at the 0.01 level (2-tailed).**

This study examined relationship between self-reported proxy bypass and self-reported cyber crime engagement. The results found illustrate a relationship similar to the literature review. This result can be interpreted in different ways. One way of interpreting the result is that individuals that are engaging in cyber criminal activities are also the same individuals that are bypassing the Internet proxy. Another plausible explanation for this result is similar to the notion discussed in the literature review, which indicated that "What is banned is desired". Individuals bypassing the Internet proxy are indeed engaging in cyber criminal activities, which are activities that are banned by society. H1 is supported from the experimental results, and thus it is accepted.

7.2 Hypothesis 2

H2: Individuals with better knowledge in computers are more likely to bypass the Internet proxy and engage in cybercrime.

For the SRPBE measure (Table 4) the means illustrate that those with excellent knowledge in computers have the highest SRPBE mean. This illustrates that individuals with excellent knowledge in computers are the ones that are engaging in bypassing the Internet proxy more often. A plausible explanation for that is that certain technical skills are needed in order to bypass the Internet proxy. This part of the hypothesis is accepted – that individuals with more knowledge in computers are more likely to bypass the Internet proxy.

Table 4. Mean SRPBE for computer knowledge

Computer Knowledge	Mean SRPBE	N	St. Deviation
Average	12.30	33	14.92
Excellent	25.20	13	23.09
Fair	11.63	8	13.00
Good	13.60	40	17.46
Poor	0.00	1	
Total	14.42	95	17.42

As for the mean in the CCI measure (Table 5), those that have good computer knowledge show the highest cybercriminal engagement. This indicates individuals with at least good knowledge have engaged in cyber criminal activities. A plausible explanation for that is that most people have engaged in cyber criminal activities such as downloading illegal music, software and movies from the Internet. It is then plausible that one does not need strong technical knowledge in computing to simply enage in cyber criminal activites. This part of the hypothesis is rejected, because the results illustrate that individuals do not need high levels of computer knowledge to engage in cyber criminal activites.

Table 5. Mean CCI for computer knowledge

Computer Knowledge	Mean CCI	N	St. Deviation
Average	11.06	33	10.97
Excellent	11.31	13	7.17
Fair	9.90	8	9.98
Good	13.10	40	10.60
Poor	0.00	1	
Total	11.74	95	10.21

7.3 Hypothesis 3

H3: Decreasing the positive perception of the proxy increases self reported cybercrime engagement and proxy bypass engagement.

The means illustrated for the control group in both SRPBE (Table 6) and CCI (Table 7) measures reveal that the manipulation paragraphs may have had an effect. This is illustrated in the increasing mean from Group 1 to Group 3 in the SRPBE and CCI. This indicates that decreasing the positive perception of the proxy increases self-reported cyber crime and proxy bypass engagement.

Table 6. Group means for SRPBE measure

Group	Mean	N	St. Deviation
1 (Positive view)	12.23	26	17.27
2 (Negative view)	15.16	31	19.32
3 (Control)	15.32	38	16.20
Total	14.42	95	17.42

Table 7. Group mean for CCI measure

Group	Mean	N	St. Deviation
1 (Positive view)	10.92	26	10.18
2 (Negative view)	11.81	31	9.86
3 (Control)	12.24	38	10.74
Total	11.74	95	10.21

When applying ANOVA in order to examine if the means in the groups where significantly different from one another in CCI and SRPBE, the results revealed that there was little significance. Reasons of this insignificance are unclear and may vary. It is possible that participants did not spend their time reading the manipulation paragraphs; therefore their perception was not significantly manipulated. Also, the sample size could be another factor; if the sample size was larger, results of a possible significance could have been more obvious. The researchers also question the viability of the manipulation paragraphs used, perhaps the words that were used where not strong enough to manipulate the participants' perceptions.

In reference to the literature review, manipulating perception has proven to have had an effect on individuals. Although it is unclear whether H3 is accepted or rejected, we do observe a trend in the means of both CCI and SRPBE of the means increasing from Group 1, to Group 3. The researchers expected that the mean of the control group would be in the middle – between the positive and the negative, but the results indicated otherwise. It is plausible that if the participants are not provided with a manipulation paragraph, that they are more likely to reveal their true opinion, this could be the reasons that both CCI and SRPBE means are higher in the control groups. Hypothesis 3 is therefore rejected. The authors note that a more comprehensive study using various other manipulation techniques should be conducted in order to re-examine the effect of manipulation on self-reported cybercrime and proxy bypass engagement.

8 Limitations

There are some limitations in this research. Primarily, there was a significant difference between the number of male and female participants in the experiment. This was expected that given that the number of female students surpasses the number of male students at Zayed University. Moreover, due to time constraints, sending out the survey to other universities was not possible. An extended process of approval from the Human Board would have been required, and this study was set to conclude within a limited time frame. Therefore, only Zayed University students and faculty were engaged in this study. Furthermore, the number of completed surveys did not match the power calculations to witness a strong effect.

9 Future Research

This study was conducted only at Zayed University in the UAE. The UAE, as mentioned before, is one of the top ten countries when it comes to censorship of the Internet [5]. This research could be expanded in the future to include students from different universities across the UAE and different countries that employ an Internet proxy. This would be favorable to gain external validity. Future research might lead to the discovery of whether implementing a proxy is actually preventing individuals from committing cybercrime. Moreover, the results of this research can be compared to future findings of different countries.

10 Conclusion

In this research, the results indicated a significant positive correlation between self-reported cyber criminal engagement and self-reported proxy bypass engagement. The results also showed that individuals with more knowledge in computers have a higher proxy bypass engagement. However, individuals with better knowledge in computers are not necessarily the ones that are more likely to commit cyber criminal activities. With regards to perception manipulation, the results are not conclusive on whether or not the manipulation paragraphs had an effect on people's view of bypassing the Internet proxy.

References

1. Internet World Stats: Middle East Internet Usage Statistics, Population, Facebook and Telecommunications Reports (2009), http://www.internetworldstats.com/stats5.htm
2. OpenNet Initiative: Internet Filtering in the United Arab Emirates (2005), http://opennet.net/sites/opennet.net/files/ONI_UAE_2009.pdf
3. Olsen, E.: Rare Criticism of Gulf State Internet Censorship (2002), http://blogcritics.org/culture/article/rare-criticism-of-gulf-state-internet/
4. Day, N.: Censorship: Or Freedom of Expression. Learner Publishing Group (2001)
5. Kwong, M.: Reports High Website Censorship. The National Newspaper (2009), http://www.thenational.ae/news/uae-news/uae-reports-high-website-censorship
6. Nick: Top 10 Countries Censoring the Web (2008), http://www.dailybits.com/top-10-countries-censoring-the-web/
7. Vandergrift, K.E.: Intellectual Freedom, and Youth (1997), http://comminfo.rutgers.edu/professional-development/childlit/censorship.html
8. Day, N.: Censorship: Or Freedom of Expression. Learner Publishing Group (2001)
9. Cortes, M.V.: Internet Censorship Around the World, University of Chile, Chile (2000), http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm
10. Schrader, P.: An Obsolete Honor: A Story of the German Resistance to Hitler. iUniverse (2008)
11. Kenney, K.: Prohibitions in the 1920s (2009), http://kim-kenney.suite101.com/prohibition-in-the-1920s-a90037
12. 1920-30.com: Prohibition in the United States (2005), http://www.1920-30.com/prohibition/
13. Hesketh, T., Lu, L., Xiang, Z.W.: The Effect of China's One-Child Family Policy after 25 years. The New England Journal of Medicine (2005), http://www.nejm.org/doi/full/10.1056/NEJMhpr051833
14. Macartney, J.: Factfile: China's one-child policy. TimesOnline (2008), http://uyghuramerican.org/old/articles/1458/1/Factfile-Chinas-one-child-policy/index.html
15. CNN: China to keep one-child policy. CNN (2008), http://articles.cnn.com/2008-03-10/world/china.onechild_1_preference-for-male-heirs-traditional-preference-gender-imbalance?_s=PM:WORLD
16. Hall, A.T.: China's one policy and male surplus as a source of demand for sex trafficking in China (2010), http://nfsacademy.org/wp-content/uploads/2011/02/Hall-Chinas-One-Child-Policy.pdf

17. Feminist.com: History of Abortion. Touchstone Publishing (1998), http://www.feminist.com/resources/ourbodies/abortion.html
18. NARAL Foundation: Choices: Women Speak Out About Abortion (2009), http://www.prochoiceamerica.org/media/fact-sheets/abortion-distorting-science-safety-legal-abortion.pdf
19. Thierer, A.D.: Regulating Video Games: Parents or Uncle Sam? CATO Institute (2003), http://www.cato.org/publications/commentary/regulating-video-games-parents-or-uncle-sam
20. Gentile, D.A., Anderson, C.A.: Violent Video Games: The Effects on Youth, and Public Policy Implications. Handbook of Children, Culture, and Violence. Thousand Oaks (2006), http://www.psychology.iastate.edu/faculty/caa/abstracts/2005-2009/05ga2.pdf
21. Wagner, M.A., Wagner, J.: Should We Censor Violence in the Media? (2002), http://www.yellodyno.com/pdf/Violence_in_the_media.pdf
22. Rhodes, R.: Hollow Claims About Fantasy Violence. The New York Times (2000), http://www.nytimes.com/2000/09/17/opinion/hollow-claims-about-fantasy-violence.html?pagewanted=all&src=pm
23. Castillo, F.: Banned and Controversial Books (2008), http://banned-books.com/bblist.html
24. Banned Books Week (2009), http://bannedbooksweek.org/about
25. Flanagan: The Futility of Censorship. Yahoo! News (2009), http://business.maktoob.com/20090000404858/The_futility_of_censorship/Article.htm
26. Furnell, S.: Cybercrime: vandalizing the Information Society. Addison-Wesley Professional Publishers (2001)
27. Shinder, D.: Scene of the cybercrime: computer forensics handbook (2002), http://www.google.com/books?hl=ar&lr=&id=nQyucKKH6RgC&oi=fnd&pg=PR25&dq=cyber+crime+&ots=WVbXcJB81-&sig=Oszwa45V1PaTUTneqKDE9UuvX-I#v=onepage&q=cyber%20crime&f=false
28. (Stocks, n.d.)
29. Heffner, C.: Introduction to Sensation and Perception (2004), http://allpsych.com/psychology101/sensation_perception.html
30. Wikia: Perception: Perception and Reality (2001), http://psychology.wikia.com/wiki/Experimental:Perception
31. Lacasse, M.: How the industry manipulated public opinion: Why you believe what you believe (2009), http://www.healingdaily.com/beliefs.htm
32. Bernay, E.L.: Propaganda. Kennikat Press (1972)
33. Budd, R.W., Ruben, B.D.: Beyond Media: New Approaches to Mass Communication. Transaction Publishers (1987)
34. Thayer, L.: On the Mass Media and Mass Communication: Notes Toward a Theory. Oxford University Press (1986)
35. Ball-Rokeach, S.J., DeFleur, M.L.: A dependency model of mass media effects. Communication Research 3, 3–21 (1976)
36. Johnson, B.K.: Dawn of the Cognetic Age: Fighting Ideological War by Putting Thought in Motion with Impact (2007), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/win07/johnson.html

37. Reis, H.T., Judd, C.M.: Handbook of Research: Methods in Social and Personality Psychology. Cambridge University Press, Cambridge (2000)
38. Bland, E.: Magnets can manipulate morality: study (2010), http://www.abc.net.au/science/articles/2010/03/30/2859767.htm
39. Amaral, J.R., Sabbatini, R.M.: Placebo Effect: The Power of the Sugar Pill (1999), http://www.cerebromente.org.br/n09/mente/placebo1_i.htm
40. Rogers, M.: A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study. University of Manitoba, Canada (2001)
41. Baggili, I.M.: Effects of Anonymity, Pre-Employment Integrity and Antisocial Behavior on Self-Reported Cyber Crime Engagement: An Exploratory Study. Doctoral dissertation, Purdue University, USA (2009), http://dl.acm.org/citation.cfm?id=1834973
42. Baggili, I.M., Rogers, M.: Self-Reported Cyber Crime: An Analysis on the Effects of Anonymity and Pre-Employment Integrity. Zayed University, UAE, Purdue University, USA (2009), http://www.cybercrimejournal.com/ibrahimmarcusIJCCJuly2009.pdf