ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Perspectives for Cyber-Deterrence: A Quantitative Analysis of Cyber Threats and Attacks on Consumers

Richmond Adebiaye[1], Haroun Alryalat[2], Theophilus Owusu[3]

Associate Professor, College of Information Technology, Ajman University of Science and Technology, UAE[1]

Associate Professor, Dean, College of Information Technology, Ajman University of Science and Technology, UAE[2]

Assistant Professor, Graduate Business School, Keiser University, Florida, USA[3]

ABSTRACT: Cyber Deterrence could be the United States' best counterintelligence defense against cyber aggression and industrial espionage on the Critical Infrastructure and Key Resources (CIKR) and Cyber Threats on US consumers. As technology improves and global trade and interconnectivity extend beyond comprehension, accountability, ideology and culture, the need to provide fool-proof security to protect US consumers is essential for public safety and national defense. This study involves data collections, which examined the relationship between reliability and validity of different perspectives regarding cyber deterrence. A descriptive statistical investigation using survey methodologies was employed to ascertain concerns of 150 victims of cyber "hacktivism" on their finances through banking systems or retail merchants as well as to determine the framework of implementing cyber deterrence as an acceptable institutionalized cyber-counterintelligence. Theory integration models via obtained responses were used to test whether the stages of interrelation of variables and the mediation of motivation by victims of data breach are statistical viable and significant in predicting Cyber-security countermeasures, and secondly to exemplify/validate the data values for "bias". The collection of the quantitative values is tabulated along a continuum in numerical form using scores, chi-square, and prevalence and frequency rates derived. This allowed the reliability and validity in the analysis of the mean patterns, nonlinear trends using ANOVA, prediction-patterns, multi-group structural equation modeling (MSEM), nested model analyses and stage transitions using binary logistic regression analyses to quantify all data breaches. The study finally presented descriptive statistics and psychometric properties to contextualize and validate analytic decisions made to support the framework for institutionalized cyber deterrence against cyber threats and attacks as an acceptable counterintelligence. The ultimate resultant composition led to frameworks that describe, explain, and validate findings of the surveys.

KEYWORDS: Cyber-reconnaissance, Cyber security, Cyber deterrence, Cyber intelligence, Counterintelligence, Critical infrastructure key resources.

I. INTRODUCTION

The sixteen (16) critical infrastructure sectors of the United States have all been affected by threats if not attacks from both foreign and domestic elements [1]. While all sixteen (16) sectors are becoming more vulnerable, the most vulnerable of these sectors is perhaps the financial services sector, which represents the payment and processing of Americans funds, savings, investment, financial transfers, purchasing and payment responsibilities. The protection of these 16 sectors vis-à-vis chemical, communications, commercial facilities, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public heath, information technology, nuclear reactors, materials and waste, transportation systems, water and wastewater systems "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" [2]. Security experts like [3],[4] and few researchers like

DOI:10.15680/IJIRSET.2016.0507157

[5][6][7] observed that “the United States defense network claims that billions of dollars have been invested in legacy protections, such as traditional and next-generation firewalls, intrusion prevention systems, anti-virus and web gateways, still all these efforts and investments no longer stop advanced malware or targeted Advanced Persistent Threats (APTs)”[8]. One cyber security researcher also concludes that “as technology evolves and continues to develop towards the inevitable connectedness that brings systems in sync with one another; an indication that United States is becoming more and more vulnerable” [9].

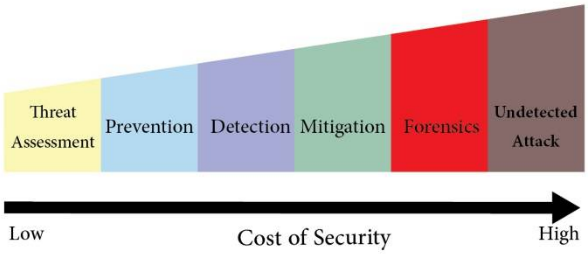

Fig. 1: An Overview of Security practices

The above diagram indicates how “proactive security schemes are aimed at attack deterrence” [10). Researchers like [11] and [12] believe that security schemes presently deployed are not yet cost effective and a good deterrent framework, which must examine threats and attacks, and would help in reducing cost of information security in the future.

II. RELATED WORK

The Pentagon’s initiative called “Plan X”, which is still shrouded in secrecy, is considered a program for building the technology infrastructure that would allow cyber offense to be used as a defense and counterattack strategy. Ultimately, this initiative has not deterred corporate anger over successive cyber-attacks. As more businesses have now introduced cyber security programs and information security department to protect their data in order to ensure that company resources continue to operate as per the requirement. One aspect of cybercrime that businesses face is the battle against attacks that steal and destroy important data and information, deploying tactics such as intrusions, industrial espionage using various malware such as viruses, worms, Trojan horses, laptop theft and distributed crackers [13]. Cyber security researchers like [14][15][16] concluded that the “financial sector of the CIKR is so essential to the safety and well-being of businesses, as well as the nation that it must be the focus of an ever-vigilant watch of cyber security professionals and the Intelligence Community (IC) because of increased reliance on software, computers, and networks” [17].

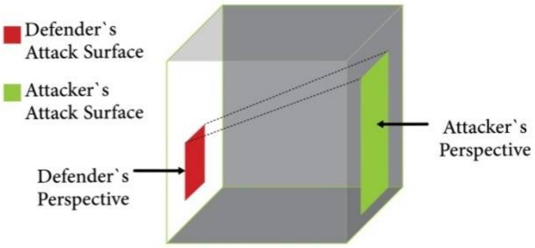

Fig. 2: Perspectives of attack and defense

The above Figure 2 diagram indicates the objective of providing effective outlook of the security of a system. Researchers such as [18] and [19] explained the importance of designing a scheme to primarily reduce security gaps and to minimize or eliminate the disadvantage of a defender by presenting a focused view of threats to the system in question”. In 2003, the US Department of Homeland Security through the “Homeland Security Presidential Directive 7” established the US National Policy for Identification and Prioritization for Protection of Critical Infrastructure (NIPP). This “National Infrastructure Protection Plan” (NIPP) document chronicles a partnership framework that enables “federal, state, regional, local, tribal, territorial, and international governments to work with each other and their private sector partners. A Critical Infrastructure Partnership Advisory Council (CIPAC) was also set up, which supports a legal framework for their collaboration [20]”. The National Infrastructure Coordinating Centre, “a subordinate component of the Office of Infrastructure Protection within the Department of Homeland Security (DHS), was also set up to “strengthen Sector Specific Agency (SSA) relationships as well as to understand sector associations”[21].[22]. This goes a long way in understanding how United States infrastructure has become so dependent upon interconnected critical systems and technology that the “domino effect from one system could affect others in a catastrophic chain reaction incapacitating a region”[23]. Thus, bearing these factors in mind, several researchers like [24] [25] [26] and the Intelligence Community (IC) must unite in establishing a stalwart national strategy to defend these CKIR” [27].

III. The need for Cyber deterrence (CD)

Cyber deterrence (CD) would be best defined as a process of integrating Cyber Intelligence Analysis and Cyber Defense Operations as countermeasures to cyber-attacks. To be able to have effective cyber deterrence, there must be a pragmatic method for an integrated pattern-modeling of security process and countermeasures. The vulnerabilities, threats and attacks must be reliably modeled and applied. According to [28], “threat modeling is the process of enumerating and risk-rating the malicious agents, their attacks, and possible impacts of those attacks on a system’s assets (Pg.13).” Another researcher [29] also explored how “proactive security schemes unlike traditional schemes are aimed at attack deterrence in the first place”. Based on this assertion, it is essential to exemplify the notion of a defense modeling in order to understand the quantitative and qualitative metrics of an attacker’s behavior.

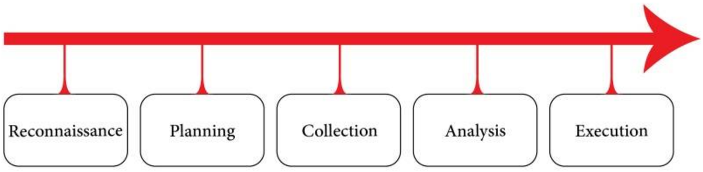

Fig 3: Steps which involve an Attack

It is equally important to understand whether cyber deterrence could be modeled to create a counter intelligence and countermeasure strategy with a known pattern. Another research also explored how cyber-attack and defense behaviors usually follow some known distributions and patterns, consequently paving the way to the creation of the “Attack Tree Model”. There is also another attack pattern, which was introduced by [30], “as a way to reuse generic segments or whole attack trees for applicable contexts” (Pg.4). However, according to [31] in a dissertation publication, “While attack trees model does not capture complex dependencies among events and also is not amenable for modeling dynamic nature of the attacks and countermeasures, the fitness of stochastic models is yet to be established as there is no sufficient evidence to indicate that attack and defense behaviors follow some known distributions” [32]. This researcher [33] designed “a new attack modeling approach based on Petri nets, called Petri Net Attack Modeling approach (PENET)” (pg. 5).

This new model introduced “relevant concepts, such as dynamic nature of attack, reparability of a system, and the existence of recurring attacks, providing intuitive modeling approach for modeling attacker behavior in vulnerable systems in security sense, based on concepts of attack trees and modeling abilities of Petri nets” [34]. The US National Security Agency (NSA) also developed a methodology for use during the system development cycle called “Mission Oriented Risk and Design Analysis of Critical Information Systems” (MORDA), which “explicitly describes the security for each design alternative, account for non-security user and service provider concerns, such as functionality and interoperability, characterizes decision-maker preference functions, accounts for the complex interdependencies of countermeasures and attacks, evaluates countermeasure effectiveness and allocates risk reducing resources”[35]. Researchers like [36][37][38][39] also developed a SOCRATES model in their military research, which is a quantitative risk assessment model and design optimization tool that is based on multiple objective decision analysis (Pg.22).

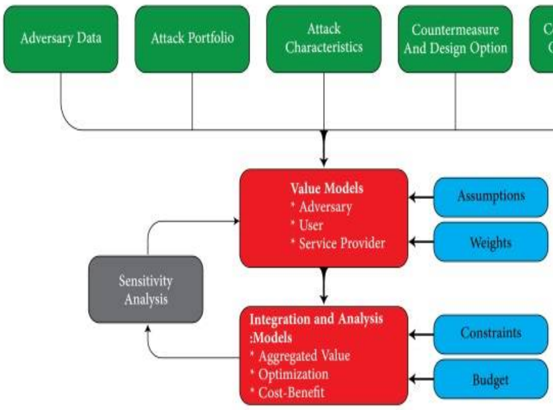

Fig. 4: Socrates model

The researchers [40],[41],[42] also explained that "Socrates Model is considered a value-based approach and was required to capture the countermeasure's ability to enhance the security of the network as well as the loss of operator value from degradation of user functions"{pg.30). Ultimately, the researchers created different value models to interpret the functionality of Socrates Model. They tested "value measures using value functions and combining standardized values into an overall value using a weighted sum" [43]. Mathematically, the value models that these researchers created assume an addictive model.

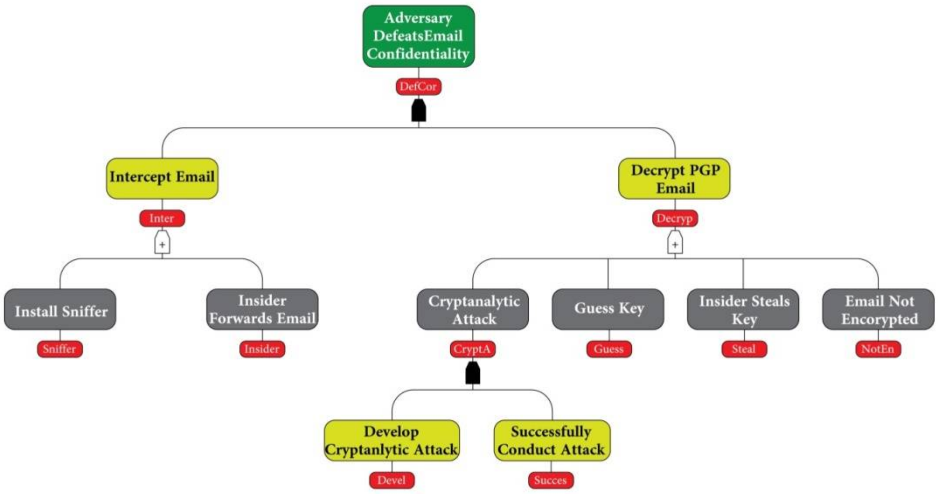

Fig. 6: A Typical example of an Attack tree

According to McAfee's Virtual Criminology Report as far back as 2007, indicated the world in the midst of a "cyber cold war." Specifically, the report states, "Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage" [44]. Offensive cyber warfare capability is a sound strategic balancing factor that potentially will be utilized by the rising/challenging hegemon against the hegemon [45]. To justify this report, researchers such as [46], [47] and [48] explored the attractiveness of cyber warfare for the weaker state and determined that this could be due to its "low cost of development and deployment, its minimum visibility during development and mobilization as a weapon, attribution, globalization of information and global accessibility of technology and the fact that stronger states are more dependent on their critical cyber infrastructure" (Pg.16).

The researchers concluded that "the analogy between the modern day cyber era conflict and the cold war conflict between the Soviet Union and the United States is primarily anchored in the idea that powerful nation-states are competing for influence and power without resorting to a direct conventional or nuclear war"[49].

IV. CATEGORIES OF CYBER-ATTACKERS

Two researchers namely [50] and [51] explained the need to tease out and understand common motivations on how cyber-attackers may be categorized. Indications also show that a given attacker may belong to more than one category. Other researchers like [52],[53],[54],[55], and [56] explained that "politically motivated cyber-attacks may be carried out by members of extremist groups, who make use of cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime". They observed in their analysis that the reasons behind the "non-politically motivated attacks are generally financial, and most attacks are considered as cyber-crime" [57], but many cyber-attacks are motivated by deeply-rooted socio-cultural issues [58].

As shown in Figure 6 below, cyber-attackers can be broadly considered "insiders" or "outsiders"[59], it is actually an attempt of acting from within an organization or attempt to "penetrate from the outside"[60].

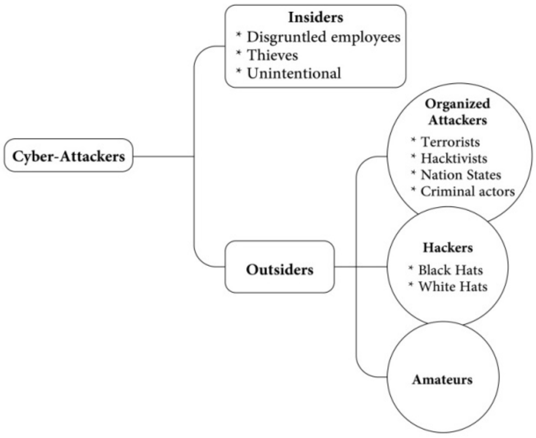

Fig. 6: Categories of cyber attackers [61]

In another research study by [62] and [63], identified three basic categories of insiders as "disgruntled employees, who may launch retaliatory attacks or threaten the safety of internal systems; financially motivated insiders, who may misuse company assets or manipulate the system for personal gains; and unintentional insiders, who may unwittingly facilitate outside attacks, but are not strictly speaking primary attackers" [64][65].

On the issue of cybercrimes affecting the national security, another researcher [66] concluded that understanding the effectiveness of the strategic culture and utilization of cyber warfare capability, by challenging/rising hegemon against the hegemon, will have consequences on U.S. national security doctrine. From the research, it could be concluded that United States is one of the most "wired" states in the world, which has potential vulnerability against cyber-attacks. The research concluded that globalization fuelled by technological advancement and spread of cyber space in physical space is manifestation of new means, through which power is exercised and distributed" [67]. One theory, which has generally been relied upon to explain IS misuse within an organization, is General Deterrence Theory (GDT), which has been used within IS research to indicate that security countermeasures can act as a deterrent by increasing the perceptions of the severity and certainty of punishment for misusing information systems" [68]. GDT uses "three variables to explain IS misuse within an organization; severity of punishment, certainty of punishment, and rival explanations", which have been operationalized in many different ways including IS specific codes of ethics [69], preventative measures [70], and ethics training [71].

V. DATA COLLECTION AND PROCEDURES

This study breakdown presents the sample size and sampling procedure, research tools / procedures, study variables, data collection process and data analysis process.

A. *Sample size and sampling procedure*

In this study, a sample of one hundred and fifty (150) respondents was randomly selected for data collections. A sample of 150 was deemed fit statistically, because it will generate data that will significantly be reliable and valid for statistical inference processes. The survey involves online interviews, where the questionnaires were sent through a web-based survey instrument [72]. The sampling design used was simple random sampling, where each respondent has an equal opportunity of being selected to be part of the sampling. Since data was gathered using online questionnaires, the questionnaires were mainly centered on the following five (5) aspects of data: (1) demographic information, (2) cyber hack threats/ incidences, (3) organizational security, (4) extent of financial losses due to cyber hacks and (5) cyber hack preparedness. The five aspects had various attributes and sub-attributes that bear the actual variables of the study. The extent of financial loss due to cyber hacks and strength of cyber deterrence were taken as the response variables, while other variables were taken as predictors values. The validity and reliability of the online questionnaires were considered using psychometric procedures as per the requirement of data collection process. The questionnaires were also piloted before the actual data collection to ensure that the information obtained through them is valid and reliable.

B. *Study variables*

The study was objectively centered on five research questions. Therefore, the data collected for analysis was based on these five questions. The study variables were categorized into three groups namely; dependent variables / response variables, independent variables / predictors and confounding variables / intervening variables.

1. The dependent variables were financial losses due to cyber-crimes and strength of cyber deterrence towards reduction of cyber-crimes.
2. The independent variables included incidences of cyber-crimes, threat acts of cyber-crimes, security awareness about cyber-crimes, whether cyber-crimes increased or decreased motivation of cyber-crimes and number of employees.
3. The intervening variables included skill gaps that accelerate cyber-crimes, system deterrent schemes, perceived severity of threatening cyber-crime, perceived probability of occurring of a cyber-crime, belief of self-efficacy to prevent cyber-crime, active cyber security and defense, and the security personnel experience in cyber-crimes. Not all variables were tested
4. Other variables were mainly the demographic factors, which included gender, age, and levels of education, type of business / industry and geographical region.

C. *Data collection and analysis process*

The collected data was first operationalized using predictor values for analysis. SPSS version 22 was mainly used in coding and analysis process, which included preliminary data analysis, which basically checks various statistical characteristics of the data. At this stage, techniques like descriptive statistics, graphs and frequency tables were used to analyze the study variables and demographic variables. The common statistical characteristics tested are the normality of data, measures of central tendency, and measures of variations. The second stage of analysis involved using correlation analysis, where various independent variables (IVs) as specified were checked to validate their effect on the dependent variables (DV) using correlation coefficients and scatter plots. The last stage involved modeling the relationships between various independent variables (IVs) and the dependent variables (DVs) using statistical techniques like regression and Chi-square (Odds ratio involved).

VI. EXPERIMENTAL DATA RESULT ANALYSIS

The analysis below indicates the demographic factors of the respondents of the survey with concerns on effects of cyber hacks and data breach on retail business customers. The results below indicate the respondents' type of involvement.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Social Media	15	10.0	10.0	10.0
	Online Purchases	30	20.0	20.0	30.0
	Store Purchases	61	40.7	40.7	70.7
	Bank accounts (credit cards)	37	24.7	24.7	95.3
	others	7	4.7	4.7	100.0
	Total	150	100.0	100.0	

TABLE 1: TYPE OF INSTITUTIONS AFFECTED

In Table 1 above, the results indicate that most of the respondents' hacks took place while engaging in purchases in retail stores. About 40.7% occurred through in-store purchases, 24.7% through bank accounts, 20.0% through online purchases, while 10% occurred through online media accounts. In Table 2 below, Out of 150 respondents sampled, 102 have serious privacy risks and concerns based on their loses, while 48 do not have serious privacy risks and concerns.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Serious concerns	102	68.0	68.0	68.0
	Non-Serious concerns	48	32.0	32.0	100.0
	Total	150	100.0	100.0	

TABLE 2: RESPONDENTS DETERMINATIONS ON PRIVACY CONCERNS

Table 2 also indicates that out of 150 cases investigated, 68% were more concerned about their privacy and information leak, while 32% were not. However, it was worth noting that those with serious concerns represent a significant target of cyber-crimes.

	Age group	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	20-30	49	32.6	32.6	32.6
	30-40	79	52.9	52.9	85.4
	41-50	22	14.6	14.6	100.0
	Total	150	100.0	100.0	

TABLE 3: DISTRIBUTION OF RESPONDENTS ACCORDING TO AGE

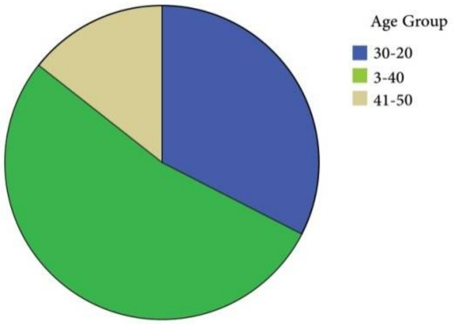

Fig. 3: Distribution of respondents according to age

Table 3 and Figure 3 above represent how the respondents were distributed across different age groups. Significant numbers of respondents (52.9%) were between 30–40 years; this is the modal class of the age distribution. On the other hand, 32.6% respondents were between 20–30 years, while 14.6% were between 40–50 years. The pie chart results indicate that majority of the respondents were middle aged adults between ages 30-40 years with a frequency of 52.9%. It is also worth noting that there were no respondents, who were above 50 years of age.

	Gender	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Male	85	56.8	56.8	56.8
	Female	65	43.2	43.2	100.0
	Total	150	100.0	100.0	

TABLE 4: DISTRIBUTION OF RESPONDENTS BY GENDER

The table above represents how the respondents were distributed across different genders. Majority of the respondents i.e. 56.8% was male with 43.2% being female. This indicates that there is a slight gender disparity among the respondents. Gender is an important socio-demographic factor in determining the socio-economic status of a population.

	Level of Education	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	High School Diploma	59	39.3	39.3	39.3
	College degree	75	49.7	49.7	89.1
	Advance College degree	14	9.1	9.1	98.2
	No degree	2	1.0	1.0	99.2
	Others	1	.8	.8	100.0
	Total	384	100.0	100.0	

TABLE 5: DISTRIBUTION OF RESPONDENTS BY EDUCATIONAL LEVELS

Table 5 above indicates the distribution of various levels of education of the respondents. College Degree holders with frequency of 49.7% of the respondents represented the major level of education achieved by the population under study. 39.3% of the respondents had high school diploma, while combined 10.9% had advanced degrees or none. Studies indicate that there is a direct relationship between level of education and the ability to purchase items either online, in-stores or having bank accounts.

A. The incidences of cyber threats to national security through business merchants

The analysis below in Table 6indicates the frequency of responses on effect of cyber-crimes on national security as a result of cyber-crimes among the retail merchants in this study.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Yes	109	72.8	72.8	72.8
	No	27	18.2	18.2	91.0
	Not Sure	14	9.0	9.0	100.0
	Total	150	100.0	100.0	

TABLE 6: NATIONAL SECURITY AFFECTED BY CYBER-CRIMES

The above results indicate that 72.8% felt that cyber-crimes are detrimental to national security of a country. In the same survey, 18.2% felt that cyber-crimes had no effect on national security, while 9.0% were not sure that cyber-crimes have an effect on national security. According to this result, it is evident that cyber-crime is statistically significant in threatening the national security of a country. On another level, the proportion of retail merchant customers, who were affected by cyber-crimes, was also analyzed.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Yes	90	60.0	60.0	60.0
	No	46	30.7	30.7	90.7
	NA	14	9.3	9.3	100.0
	Total	150	100.0	100.0	

TABLE 7: HAVE BEEN AFFECTED BY CYBER-CRIMES

In Table 7 above, the results indicate that 60% of the persons interviewed had been affected by cyber-crimes and data breach, while 30.7% had not been affected by the cyber-crimes in the last one year. 9.3% of the respondents cited that the cyber-crimes were never applied to their daily activities/ businesses.

TABLE 8: DIFFERENT CYBER THREATS AND ATTACKS PREVALENT

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Cyber-crimes	46	30.7	30.7	30.7
	Hacktivists	39	26.0	26.0	56.7
	Single hacker	26	17.3	17.3	74.0
	Malicious insider	12	8.0	8.0	82.0
	Non-malicious insider	8	5.3	5.3	87.3
	Others	10	6.7	6.7	94.0
	NA	9	6.0	6.0	100.0
	Total	150	100.0	100.0	

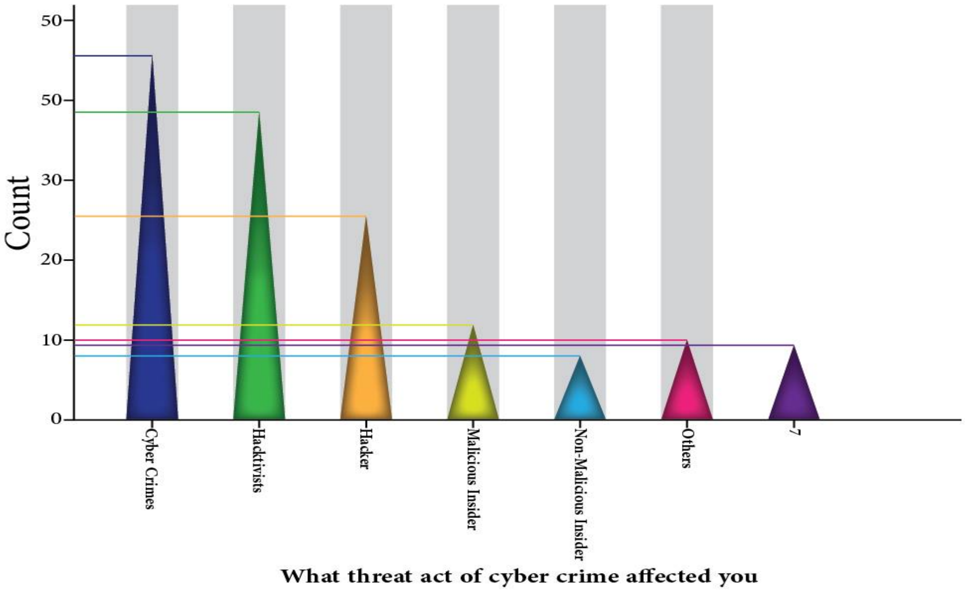

Fig. 4: Most common Cyber Threats

In Table 8 and Figure 4 above, the results indicate that cyber-crimes affected the retail merchant customers by 30.7%, followed by Hacktivists at 26%, then Hackers at 17.3%, while malicious insider threats and other direct insiders contributed 8.0% and 5.3% respectively towards cyber-crimes and data breach during the last one year. The table and bar graph below also indicate the different most common cyber-attacks analyzed.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Hack attempts (DDoS)	76	50.7	50.7	50.7
	Malware	44	29.3	29.3	80.0
	Social engineering	10	6.7	6.7	86.7
	Phishing/Spoofing	16	10.7	10.7	97.3
	others	4	2.7	2.7	100.0
	Total	150	100.0	100.0	

TABLE 9: DIFFERENT CYBER ATTACKS

In Table 9 above, the breakdown projects that Hackivists' activities in different hacking attempts including distributed denial of service and malware practices represent 50.7% and 29.3% respectively on retail business customers. Other minor attack types include social engineering and phishing at 6.7% and 10.7% respectively.

B. The probability of huge costs due to cyber-crimes

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	More than Half of Expectations	59	39.3	39.3	39.3
	Less than half of expectations	60	40.0	40.0	79.3
	N/A	31	20.7	20.7	100.0
	Total	150	100.0	100.0	

TABLE 10: LIKELIHOOD FINANCIAL LOSS DUE TO CYBER-CRIMES

In Table 10 above, the results indicate that about 79.3% responses indicated that at least their personal finances suffered due to cyber-crimes. Out of these responses, 39.3% indicated that they suffered more financial losses than expected, while 40% indicated less financial losses than half of the expected losses in the past one year. On the other hand, 20.7% indicated that they were not affected financially by cyber-crimes.

C. The motivations behind cyber-crimes

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Economic Motivations	78	52.0	52.0	52.0
	Socio-cultural motivations (e.g. Curiosity, fun, ego etc.)	25	16.7	16.7	68.7
	Political motivations	16	10.7	10.7	79.3
	Industrial and Technological advantage	14	9.3	9.3	88.7
	Lack of responsible legislation	17	11.3	11.3	100.0
	Total	150	100.0	100.0	

TABLE 11: WHAT MOTIVATES CYBER-CRIMES?

In the above Table 11, the results show that most cyber-crimes are motivated by the financial gains or benefits, while others are motivated by socio-cultural motivations (e.g. curiosity, fun, ego etc.), political, industrial and technological edge and lack of responsible legislations. Analysis indicates that economic benefits or financial motivation contributes 52%, socio-cultural motivations (e.g. curiosity, fun, ego etc.) represent 16.7%, political motivations represent 10.7%, industrial and technological edge represent 9.3%, and lack of responsible legislations represent 11.3%.

This is an indication that economic benefit is significant motivation factor in cyber-crime activities. In their research, [73] and [74] explained the need to understand the motivations of cyber-attackers. Their article also highlighted the importance of understanding how “the motivations behind cyber-attacks intended to cause economic impacts may be different from those posing a threat to national security”. Another researcher [75] also supported this notion by explaining that the real purpose and primary objective of a cyber-attack may be hidden or obscured, even if the attacker claims responsibility.

In order to validate the statistical analysis that would strengthen this study, descriptive statistics and psychometric properties of three research questions were operationalized. This helps to contextualize and validate analytic decisions made to support the framework for institutionalized cyber deterrence against cyber threats and attacks as an acceptable counterintelligence.

1. What is the relationship between active cyber defense and reciprocal attacks as successful methods towards establishing successful Cyber deterrence?
2. What is the correlation between activecyber deterrence using cyber threats?
3. How do current cyber security best practices influence active cyber deterrence?

VII. STATISTICAL RESULTS SUMMARY

A sample of 150 persons was randomly selected for data collection. Survey was sent using a web based data collection instrument [76]. The survey was mainly focused on the three research questions. The extent of financial loss due to cyber hacks and need for cyber deterrence was taken as dependent variables (DVs). The common statistical characteristics checked were the normality of data, measures of central tendency, measures of variations etc. The second stage of analysis involved using frequency distribution to analyze how cyber-crimes have threatened National Security as a result of the prevalence of cyber-crimes amongst retail merchant customers. The third stage of analysis involved using correlation analysis and Chi-square tests, where independent variables were measured. The last stage involved modeling the relationships between various IVs and the strength of cyber deterrence as DV using binary logistic regression and Chi-square (Odds ratio).

Q1: What is the relationship between active Cyber Defense and reciprocal attacks as successful methods towards establishing active Cyber Deterrence?

To determine the relationship between active cyber defense and reciprocal attacks as successful methods towards establishing successful cyber deterrence, Chi-square tests of independence were measured.

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5.837[a]	1	.016		
Continuity Correction[b]	4.952	1	.026		
Likelihood Ratio	6.142	1	.013		
Fisher's Exact Test				.022	.012
Linear-by-Linear Association	5.798	1	.016		
N of Valid Cases[b]	150				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 15.34.

b. Computed only for a 2x2 table

TABLE 15: CHI-SQUARE RESULTS

In Table 15 above, the analysis indicates that the Pearson's chi-square value is 5.837 at 1 degree of freedom, and p-value is 0.016. Since the p-value is less than 0.05, this shows a statistical significance in the relationship between active cyber defense and reciprocal attacks as successful methods towards establishing successful cyber deterrence as most respondents believe that reciprocal attacks will be significant as deterrence. Therefore, at 95% confidence level, there is a significant relationship between active cyber defense and reciprocal attacks as successful tools toward establishing Cyber deterrence.

Q2: Research question 3: Establishing whether cyber deterrence using cyber threats influence active Cyber defense

To establishing whether cyber deterrence using cyber threats influence cyber defense, correlation analysis between the two variables were measured.

		Perceived opinion on Cyber deterrence towards reduction of cyber-crimes	**system deterrent scheme do you advocate for**
Perceived opinion on Cyber deterrence towards reduction of cyber-crimes	Pearson Correlation	1	-0.232
	Sig. (2-tailed)		0.031
	N	150	150
system deterrent scheme do you advocate for	Pearson Correlation	-0.232	1
	Sig. (2-tailed)	0.031	
	N	150	150

TABLE 16: CORRELATION ANALYSIS RESULTS

Results from Table 16 above, indicate that the correlation coefficient is -0.232 at a significance of 0.031. The results indicate that there is a weak and negative correlation coefficient between cyber deterrence schemes and active cyber defense. Significantly, we can conclude that there exists a weak inverse relationship (correlation) between system deterrent schemes like using cyber threats as a force and active cyber defense, because the p-value obtained was less than 0.05. However, it should be noted that the negative correlation indicated that cyber deterrence schemes can hinder strength of active cyber defense.

Q3: Determining How current Cyber security Best Practices influence active Cyber deterrence.

To determine whether the current cyber security best practices influence active cyber deterrence, Chi-square test of independence was used for analysis, and the Chi-square tests of dependence were done.

	Value	**df**	**Asymp. Sig. (2-sided)**	**Exact Sig. (2-sided)**	**Exact Sig. (1-sided)**
Pearson Chi-Square	2.500[a]	1	.114		
Continuity Correction[b]	1.953	1	.162		
Likelihood Ratio	2.559	1	.110		
Fisher's Exact Test				.143	.080
Linear-by-Linear Association	2.483	1	.115		
N of Valid Cases[b]	150				

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 17.31.

b. Computed only for a 2x2 table

TABLE 17: CHI-SQUARE TEST RESULTS

In Table 17 above, Chi-square result indicates value of 2.500 at 1 degree of freedom, and p-value at 0.114. Other significant results indicate p-value to be more than 0.05. This shows that at 95% confidence level, the variables are not independent. Therefore, the current cyber security best practices have not been effective without influence on active Cyber deterrence or not statistically effective.

VIII. RELIABILITY, VALIDITY, LIMITATIONS AND RECOMMENDATION

According to [77], validity deals with the truth of generalizations that a research generates, and this can be achieved by ensuring that the collected data accurately gauge what is being measured at the ground (pg. 30). In this study, validity was ensured by conducting the survey in a natural and typical online setting, whereby the participants' experiences were real and accurate. Validity was also assured by cross-checking data from the participants for authenticity and duplicates. Reliability, on the other hand, is the measure of the degree to which the interview or questionnaires yield consistent results from the study sample at different occasions [78].

In this study, reliability was ensured by cross-checking consistency of the coding system used in the operationalization of the values in the online questionnaires. The researcher also used code-recode strategy by coding data and rechecking it over time using multiple data recoding by including all responding attributes of variables in the survey.

The main limitation of this study was lack of adequate time and resources to carry out a wider coverage survey with more robust statistical inferences. It is therefore imperative that further research should be done in the area of effect of cyber security management experience and practices on the strength of cyber deterrence.

IX. CONCLUSION

It is worth noting that economic factors or financial gains were the main influence of cyber-crimes as shown in the analysis under study. It was also noted that the common cyber-crimes in the survey involve hack attempts especially the popular distributed denial of service (DDoS), predominantly with use of credit cards mostly found in electronics transactions. Other findings include threats posed in online purchases and inadequate security infrastructure of retail merchants; constitute another main influence of cyber-crimes. Other most prominent are malware, social engineering, and spoofing and phishing mails were used as aactive reconnaissance method of cyber attacks. The survey also indicated that 72.8% of respondents felt that cyber-crimes are significant in affecting the national security of a country. However, 18.2% felt that cyber-crimes had no effect on National Security, while 9.0% were unsure that cyber-crimes have any effects on National Security. This shows significant concerns that cyber-crimes continuously threaten National Security.

The survey results also showed that active Cyber Security to prevent cyber-crimes and the effectiveness and strength of cyber deterrence were significantly independent. Therefore, there was a significant relationship between deploying active Cyber deterrence tools toward establishing active cyber defense. The results also realized a weak inverse relationship between deploying Cyber reciprocal attacks and active Cyber defense. The chi-square tests showed that the current Cyber security preparedness and Cyber security best practices as means towards cyber deterrence was found to be effective, as the cyber security preparedness, experience and Cyber security methods and practices were significantly associated to strength of cyber deterrence.

The survey also indicated that there is a strong but negative correlation coefficient between Cyber Threats and Attacks on consumers and strength of Cyber deterrence. Analysis also indicated consumers' preferences for cyber deterrence through a strategy of active reciprocal attack to perceived Threats. This could inevitably lead to complete and active Cyber Balance of Power, which would be strength for further research. The variables such as perceived probability of cyber-crimes occurring, perceived severity of Cyber-crimes, perceived severity of Cyber security best practices, perceived severity of consumers financial loses levels are significant in influencing the outcome of strength of cyber deterrence.

REFERENCES

[1] Al Jazeera,“How real is the threat of cyberwar?’ Inside Story: al Jazeera”, Retrieved from http://www.aljazeera.com/programmes/insidestory/2012/10/201210131111678361.html,(2012, October 13).

[2] Amir Lupovici, “The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda”, International Studies Quarterly,Vol 54, Issue 1,pp.705-32. (2010)

[3] Andreasson, K.J., “Introduction”, In K. J. Andreasson (Ed.), Cybersecurity: Public Sector Threats and Responses: XIII-XXV. Boca Raton, FL: CRC Press.(2011).

[4] Andress, J., and Winterfeld, S.,“Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners”, Waltham, MA: Elsevier.(2011).

[5] Andy Greenberg,“Sketching Obama’s Cyberplans”, Forbes, Retrieved fromhttp://www.forbes.com/2009/02/20/paul-kurtz-security-technology-security_kurtz.html, (2009, February 20).

[6] Boawn, D.L.,“Cyber counterintelligence, defending the United States' information technology and communications critical infrastructure from Chinese threats”, (2014).

[7] Bruno, G., “The Evolution of Cyber Warfare, The Council on Foreign Relations”, Retrieved from http://www.cfr.org/publication/15577, (2008, February 28).

[8] BuckShaw, D.L.,“Mission oriented risk and design analysis of critical information systems”, Retrieved from http://static1.squarespace.com/static/50ce7827e4b03f46ba4a21cf/t/51074b66e4b0a59cd794cf95/1359432550004/IDI+Mission+Risk+and+Design+Analysis.pdf, (2005).

[9] BuckShaw, D.L.,“Mission oriented risk and design analysis of critical information systems”, Retrieved from http://static1.squarespace.com/static/50ce7827e4b03f46ba4a21cf/t/51074b66e4b0a59cd794cf95/1359432550004/IDI+Mission+Risk+and+Design+Analysis.pdf, (2005)

[10] Caltagirone, S.,“The Cost of Bad Threat Intelligence”, [Web log post]. Retrieved from http://www.activeresponse.org/the-cost-of-bad-threat-intelligence/, (2015, May 22).

[11] Cebula, J.J., and Young, L.R.,“Taxonomy of Operational Cyber Security Risks”, Technical Note CEM/SEI-2010-TN-028. Pittsburgh, PA: Software Engineering Institute, (2010).

[12] Central Intelligence Agency, “Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis”Retrieved from https://www.cia.gov/library/center-forthe-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primerapr09.Pdf, (2009).

[13] Chen Han and Rituja Dongre, “Q & A. What Motivates Cyber-Attackers?” Retrieved from http://timreview.ca/article/838, (n.d.)

[14] Cohen, F.,, Phillips, C., PaintonSwiler, L., Gaylor, T., Leary, P., Rupley, F., and Isler, R.,“A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID”,Computers & Security,Vol 17, Issue 3,pp.211-221, (1998).

[15] “Data collector”, Retrieved from www.surveydatacollection.com, (n.d.).

[16] Defense News,“Poll: Cyberwarfare is top threat facing US”, Retrieved from http://www.defensenews.com/section/static26, (2013, January 5).

[17] Denning, D.E.,“Framework and Principles for Active Cyber Defense” [Essay], Retrieved From http://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20Active%20Cyber%20Defense%20-%2011Dec2013.pdf, (2013).

[18] Denning, D.E., and Neumann, P.G., “Requirements and Model for IDES – A Real Time Intrusion Detection Expert System”, (Document A005, SRI International), Retrieved fromhttp://faculty.nps.edu/dedennin/publications/IDESReport SRI 1985.pdf, (1985).

[19] Dewar, R.S.,“The “Triptych of Cybersecurity”: A Classification of Active Cyber Defence. Proceedings of the 6th International Conference on Cyber Conflict”, Tallinn, Estonia (pp. 7-21),Retrieved from https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf, (2014).

[20] Eichin, M.W., and Rochlis, J.A.,“With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988”, Retrieved from http://www.utdallas.edu/~edsha/UGsecurity/internet-worm-MIT.pdf, (1989).

[21] Farnham, G.,“Tools and Standards for Cyber Threat Intelligence Projects”,Retrieved from https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyberthreat-intelligence-projects-34375, (2013).

[22] Federation of American Scientists, “The Evolution of the U.S. Intelligence Community:-An”. (n.d.).

[23] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P.,“Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political”,IEEE Technology and Society Magazine, Vol 30, Issue 1, 28-38. Retrieved From http://dx.doi.org/10.1109/MTS.2011.940293, (2011).

[24] Ghionis, A.A.,“The limits of deterrence in the cyber world: An analysis of deterrence by punishment”, University of Sussex, (n.d.)

[25] Gragido, W., Molina, D., Pierce, J., and Selby, N.,“Blackhatonomics: An Inside Look at the Economics of Cybercrime”, Waltham, MA: Elsevier, (2012)

[26] Grau, D., and Kennedy, C.,“TIM Lecture Series – The Business OfCybersecurity. Technology Innovation”, Management Review, Vol. 4, Issue 4,pp.53–57, Retrieved from http://timreview.ca/article/785, (2014).

[27] Hafner, K. and Markoff, J.,“Cyberpunk: Outlaws and Hackers on the Computer Frontier”, New York: Simon & Schuster, (1991).

[28] Harknett, “Information Warfare and Deterrence”, p.104, (n.d.)

[29] Heuer, R. J.,“Psychology of Intelligence Analysis”,Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/booksand-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf, (1999)

[30] “Historical Overview”, Retrieved from http://fas.org/irp/offdocs/int022.html, (n.d.)

[31] House of Commons Defence Committee,“Deterrence in the Twenty-First Century” House of Commons Defense Committee: Eleventh Report Session, Retrieved from www.publications.parliament.uk/pa/cm201314/cmselect/cmdfence/1066/1066vw.pdf, (2014)

[32] Howard, J.D.,“An Analysis of Security Incidents on the Internet 1989–1995”, Doctoral Thesis, Carnegie-Mellon University, Pittsburgh, PA, (1997).

[33] Hutchins, E. M., Cloppert, M. J., and Amin, R. M., “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”,Retrieved from https://www.vita.virginia.gov/uploadedfiles/VITA_Main_ Public/Security /Meetings/ISOAG/2012/Sept_ISOAG_NetworkDefense.pdf, (2011).

[34] Intelligence and Security Alliance, Cyber Intelligence Task Force,“Cyber Intelligence: Setting the Landscape for an Emerging Discipline”,Retrieved from http://www.ossinstitute.org/storage/documents/Resources/studies/insa_cyber_ intelligence_2011.pdf, (2011).

[35] Jeff Bliss, “Dearth of Technical Experts Leaves US Open to Cyber Attack, Panel Says,” Boston Globe, Retrieved from https://www.csis.org/news/dearth-technical-experts-leaves-us-open-cyber-attack-panel-says, (2009, March 20).

[36] Kane M.,“US Vulnerable to Data Sneak Attack”, CNET News, Retrieved from http://news.cnet.com/U.S.-vulnerable-to-data-sneak-attack/2100-1029_3-949605.html, (2002, August 13).

[37] Kewley, D., Fink, R., Lowry, J., and Dean, M., “Dynamic Approaches to Thwart Adversary Intelligence Gathering. DARPA Information Survivability Conference & Exposition II,Vol. 1: 176-185. doi: 10.1109/DISCEX.2001.932214, (2001).

[38] Lachow, I.,“Cyber Terrorism: Menace or Myth?”, In F. D. Kramer, S. H., Starr, & L. K. Wentz (Eds.), “Cyberpower and National Security”,pp.434-467. Dulles, VA: Potomac Books, (2009).

[39] Lee, R. M.,“Active Cyber Defense Cycle”, Retrieved from http://www.irongeek.com/i.php?page=videos/bsideshuntsville2015/ active-cyber-defensecycle-robert-m-lee, (2015a).

[40] Lewis, J.A.,“Assessing the Risks of Cyber Terrorism”, Cyber War and Other Cyber Threats, Washington, DC: Center for Strategic and International Studies, (2002).

[41] Libicki, M.,“Cyber Deterrence and Cyberwar”, Santa monica, RAND Corporation, p. 26, (2009).

[42] Lupovici, A.,“The Emerging Fourth Wave of Deterrence Theory: Toward a New Research Agenda”, p. 722, (n.d.).

[43] Lynn III, W. J.,“Defending a New Domain: The Pentagon’s Cyberstrategy”,Foreign Affairs, September-October 2010. Retrieved fromhttp://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, (2010).

[44] Marsden, P.V., and Wright, J.D.,“Handbook of survey research, Bingley”, UK: Emerald, (2010).

[45] McMillan, J.H., and Schumacher, S.,“Research in education: Evidence-based inquiry”, (6thed.) Boston: Pearson Education, 2006).

[46] Molander, R., and Wilson, “Strategic Information Warfare”, p. 87, (n.d.).

[47] Moore, A.P., Ellison, R.J., and Linger, R.C.,“Attack modeling for information security and survivability”, Software Engineering Institute Technical Report CMU/SE,(2001).

[48] Morgan,“Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm”, p. 59, (n.d.).

[49] Morgan, P., “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm”, in National Research Council Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington DC: The National Academies Press, (2010).

[50] Norton-Taylor, R., Britain plans cyber strike force - with help from GCHQ, Retrieved from http://www.theguardian.com/uk-news/defence-and-security-blog/2013/sep/30/cyber-gchq-defence, (2013, September 30).

[51] Nye, J.,“Cyber Power”, Cambridge: Belfer Center for Science and International Affairs Harvard Kennedy School, (2010).

[52] Orodho, J.A.,“Elements of Education and social sciences research methods”, Bureau Education Research, Nairobi: Masola Publishers, (2004).

[53] Peterson, A.,“The Post just got hacked by the Syrian Electronic Army, Here’s who they are”, Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are/, (2013, August 15).

[54] Rice, M., Butts, J., and Shenoi S.,“A signaling framework to deter aggression in cyberspace”, International Journal of Critical Infrastructure Protection, (2011).

[55] Richardson, R.,“2008 CSI Computer Crime and Security Survey”, Computer Security Institute, (2008).

[56] Russell, D., and Gangemi, G.T.,“Computer Security Basics”, Sebastopol, CA: O'Reilly & Associates, (1993).

[57] Rustici, R.,“Cyberweapons: Leveling the International Playing Field Parameters”, Vol 41 No 3 (2011).

[58] Sanzgiri, A.M.,“A comprehensive threat assessment framework for securing emerging technologies”, Retrieved from http://www.cse.buffalo.edu/caeiae/documents/pdf/ameya-sanzgiri-2013-dissertation.pdf, (2005).

[59] Sanzgiri, A.M.,“A comprehensive threat assessment framework for securing emerging technologies”, Retrieved from http://www.cse.buffalo.edu/caeiae/documents/pdf/ameya-sanzgiri-2013-dissertation.pdf, (2013).

[60] Shackleford, D.,“Analytics and Intelligence Survey 2014”, (SANS Survey October 2014), Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/analyticsintelligence-survey-2014-35507, (2014).

[61] Shackleford, D., “Who’s Using Cyberthreat Intelligence and How?”,(SANS Survey February 2015). Retrieved from https://www.sans.org/readingroom/whitepapers/analyst/analytics-intelligence-survey-2014-35507, (2015).

[62] Shakarian, P., Shakarian, J., and Ruef, A.,“Introduction to Cyber-Warfare: A Multidisciplinary Approach”, Waltham, MA: Elsevier, (2013).

[63] Stevens, T.,“A Cyberwar of Ideas - Deterrence and Norms in Cyberspace”, Contemporary Security Policy, Vol 33 Issue 1, (2012).

[64] Sulek, D. and Moran, N.,“What analogies can tell us about the future of cybersecurity”, Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/08_SULEK_What%20Cyber%20Analogies%20Can%20Tell%20Us.pdf, (n.d.)

[65] Target, Data breach FAQ. Retrieved from https://corporate.target.com/about/shoppingexperience/payment-card-issue-faq, (n.d.).

[66] Timberg, C., Nakashima, E., and Douglas-Gabriel, D.,“Cyberattacks trigger talk of hacking back”,The Washington Post, Retrieved from http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-ofhacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html, (2014, October 9).

[67] Townsend, T., Ludwick, M., McAllister, J., Mellinger, A.O., and Sereno, K.A., "SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project Summary of Key Findings", Retrieved from https://www.sei.cmu.edu/library/assets/ whitepapers/citpsummary-key-findings.pdf, (2013).

[68] Tsagourias, N.,"Cyber-attacks, self-defense and the problem of attribution" Journal of Conflict & security Law, Vol. 17, Issue 2, (2012).

[69] U.S. Department of Defense,"Joint Publication 2-0 Joint Intelligence",Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf, (2013).

[70] U.S. Department of Homeland Security, "Defining Cyber War", Retrieved from http://www.homelandsecuritynewswire.com/defining-cyber-warfare, (2011, February 23)

[71] U.S. Department of homeland security,"Critical infrastructure protection partnerships and information training" Retrieved from http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing, pp.14-16, 2013

[72] U.S. Department of Homeland,"Security Financial Services Sector", Retrieved from http://www.dhs.gov/financial-services-sector, (n.d.).

[73] U.S. White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", Washington, DC: Executive Office of the President of the United States. Retrieved From http://www.whitehouse.gov/assets/documents/ Cyberspace_Policy_Review_fina..., (2009).

[74] Vallance, C.,"Cyber Emergency response team launched in the UK", Retrieved from http://www.bbc.co.uk/news/technology-26818747, (2014, March 31).

[75] Virtual Criminology Report,"Cybercrime: The Next Wave, McAfee", Retrieved from http://www.mcafee.com/us/research/criminology_report/default.html: pp.12-16, 2011

[76] Warren, P.,"Hunt for Russia's web criminals", Retrieved from http://www.theguardian.com/technology/2007/nov/15/news.crime, (2007, November 15).

[77] White C., "Cybersecurity, Innovation and national power", Retrieved from http://nationalinterest.org/commentary/cybersecurity-innovation-national-power-8205, (2013).

[78] Wilshusen, G.,"Cybersecurity: Threats Impacting the Nation' Testimony Government Accountability Office", Retrieved from http://www.gao.gov/products/GAO-12-666T, (2012, April 24).

DOI:10.15680/IJIRSET.2016.0507157