The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 4 ||Pages|| 45-51||2013||
ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

Impact of Cyber Crimes on Nigerian Economy

[1,]MaitanmiOlusola, [2,]Ogunlere Samson, [3,]AyindeSemiu, [4,]AdekunleYinka
[1,2,4,]*Department of Computer Science, Babcock University, Ilisan Remo, Ogun State, Nigeria*
[3,]*Department of Basic Sciences, Babcock University, Ilisan Remo, Ogun State, Nigeria*

----------Abstract----------
A lot of people in the world, mostly Nigerian have a limited knowledge of the crime occurring in cyberspace, known as cybercrime. Cybercrime happens in the world of computer and the Internet. This kind of crime has a severe impact on our economy, lives and society, because our society is becoming an information society, full of information exchange that is happening in cyberspace. Our research work is aimed at knowing the level of awareness of individuals on the existing phenomenon in Nigeria, and their impacts on Nigerian economy. A survey was carried out with the aims of getting these results using questionnaire as an instrument, the responses were quantitatively analysed using some statistical techniques. The results show that cracking, software piracy, and pornography among others are prevalent crimes in Nigeria. While the impacts of these crimes on Nigerian economy cannot be over emphasized. Recommendations were proposed on how these crimes can be minimized if not totally eradicated.

Keywords: *Cybercrimes, Cyber laws, Crimes*

Date Of Submission: 05 April 2013 Date Of Publication: 30,April.2013

I. INTRODUCTION

Cyber crime began with disgruntled employees causing physical damage to the computers they worked with, withthe aim to get back at their superiors. As the ability to have personal computers at home became more accessible and popular, cyber criminals began to focus their efforts on home users[1]. Further research on this reveals that history of cybercrime was further established that the first published report of cybercrime occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment, allowed them to access into mainframe computers, and then refers to as computer crime rather than cybercrime. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because availability of Internet was restricted within some sections (e.g. US military) in that era. In the following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime.

In fact, the former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition.Since Internet was invented, other new terms, like "cybercrime" and "net" crime became the order of the day as people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental.We therefore come to terms with a conclusion on the meaning that cybercrime is an evil having its origin in the growing dependence on computers in modern life. A simple yet sturdy definition of cybercrime would be unlawful acts wherein the computer is either a tool or a target or both". Defining cybercrimes as illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime in a broader sense computer-related crime: any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Cyber Crime refers to all activities done with criminal intent in cyberspace. These fall into three categories:

- Crimes against persons.
- Crimes against Business and Non-business organizations.
- Crimes against the government.

Meanwhile, in an attempt to uncover these crimes billions of Naira is lost through these crimes annually with little or no hope of curbing it due to its complex nature.Most perpetrators of this crime are never caught and if at all caught, are never prosecuted because of lack of concrete evidence, organizational and societal awareness. As a result the extent and impact ofCybercrime is uncertain because lack of reporting leads to uncertainty with regard to the extent and impact of the crime. This is especially relevant with regard to the involvement of these crimes as compared to other organized crimes. Available information from the crime statistics in Nigeria is lacking and if any, do not reflect the real extent or impact of this crime in our every-day living.

1.1 Objectives

From the aforementioned challenges, the objectives of this study therefore are to create awareness among Nigerians, Government and corporate organizations on the danger of this new breed crime called cybercrime that is currently ravaging our economy. It is our hope that Nigerian Government (house of representative and Senate) and her law enforcement agencies will find our analysis in this paper useful and as tool to finding solution to reducing this ugly trend of crime before it completely wreaks havoc on our economy if it has not already done so. Also, recommendations were proposed on how this menace can actually be reduced in Nigeria. To achieve these objectives this study is divided into five sections. Following this introduction, Section II, examines existing literature on cybercrimes, Section III, presents the methodology employed in collecting and analysing data, Section IV, presents an analysis of the collected data; and Section V, deals with the conclusion and recommendations drawn up from the study.

II. LITERATURE REVIEW

What is Cybercrime?

A cybercrime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the Internet[2]. Cyber crime has been increasing in complexity and financial costs since corporations, government and individual or society at large started utilizing computers in the course of doing business. As technology increases between governments, corporate organizations and individuals that are involved in international and local businesses; criminals have realized that this is a cost effective method to make money. Efforts to address Internet crime include activities associated with defending networks and data, detecting criminal activities, inquiring into crime and taking legal action against criminals [3].Cyberspace security is crucial for maintaining the continuity of these vital services and for preserving the public's trust in information systems. But can this be achieved world-wide? Well, this is a topic for another day as our focal point in this paper is all about cybercrimesand its impact on the Nigerian economy.

Some examples of cyber crimes include sending spam emails (spamming), stealing personal information (identity theft), breaking into someone's computer to view or alter data (hacking) and tricking someone into revealing their personal information (phishing), making Internet services unavailable for users (Denial of service –DOS), advanced free fraud 419 (aka Yahoo-yahoo), credit card fraud (ATM), plagiarism and software piracy, pornography, stealing money bit-by-bit in a cunning way (salami attacks) and virus dissemination etc.So many crimes are committed every day in the Nigerian cyberspace. A recent report in the **Daily Trust, (2010)**by the Internet Crime Complaint Centre, which is a partnership between the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre, revealed that Nigeria is now ranked third among the list of top ten sources of cybercrime in the world with 8% behind the US (65%) and the UK (9.9%).Criminals that indulge in the advance fee fraud schemes (419) are now popularly called 'Yahoo Boys' in Nigeria [4]. The country has therefore carved a niche for herself as the source of what is now popularly called 419-mails, named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that forbid advance fee fraud. For instance, Nigeria is ranked first in the African region as the target and origin of malicious cyber activities; and this is spreading across the West African sub-region [5]. What Nigerian government, corporate organizations and the society at large do not know is that the heavy economic impact on the country, (either in financial terms or otherwise), will have an adverse consequences on unemployment rate, social services and international reputation.

Therefore, a detailed introduction of cybercrime needs to be presented with the view to fully analyze the indices that make up this crime so that our government and society will be aware of this crime and its implication on the economy. In this paper, we will introduce the origins and the evolution of cybercrime, the different categories of cybercrime (target cybercrime, tool cybercrime and computer incidental). In 2011, [3]opinedin their paper titled "Cybercrimes and the Nigerian Academic Institution Networks", examineddifferent types of cybercrimes that are frequent in

Nigeria and also checks the rate at which these crimes are carried out by the use of academic institution networks as the access point,but not the impact on Nigerian economy which is the focal point of this paper.

2.1 Categories of Cybercrime

Brenner (n.d) asserted that there are three main categories of cyber crimes as mentioned below:

a. **Target cybercrime**: the crime in which a computer is the target of the offense.
b. **Tool cybercrime**: the crime in which a computer is used as a tool in committing the offense (the place in which tool cybercrime happens is not physical environment but cyberspace - which make cybercrime).
c. **Computer incidental**: the crime in which a computer plays a minor role in committing the offense.

The boundaries of these categories are not so clear. For example, if someone uses high-tech hacking intoa computer or server, it's hard to say whether it is in tool cybercrime or in target cybercrime. So why do we still categorize cybercrime? We do this in other that we can analyzecybercrimebetter and more efficiently. Although, looking critically at these categories, one will know for sure that there is some intersection. We will focuson each part of cybercrime respectively and finally have a comprehensive concept.

III. IMPACT OF CYBER CRIME

The impact of cybercrime has been, and will be in the future, felt by all governmentsand economies that are connected to the Internet. Criminals will use the Internet,computers and other digital devices to facilitate their illegal activities as long as the financial gains outweigh the consequences when caught.Knowing about the quantity of Cybercrime as well as the economic impact is vital for both governments as well as businesses which could be a necessary tool to adjust the legal and regulatory frameworks as well as institutional capacities. Prosecutors and law enforcement agencies must have resources, training and equipment required to address cybercrime in order to keep current on this newest method of crime fighting.Lack of reporting this crime leads to uncertainty with regard to the extent and impact. This is especially relevant with regard to the involvement of organized crime. Available information from the crime statistics in Nigeria, if at all available, does not reflect the real extent of the crime or damages cause as a result of the crime. Different motivations of private users and businesses not to report Cybercrime is another concern for the Government. This can be seen from an article published in the [6].

As a result the extent and impact of Cybercrime is uncertain if not critically analyzed.For Examples, an analysis carried out by [7]in Germany on the impact of cybercrime in Germans economy revealed:

- Losses in German based on numbers provided by Federal Police: 75 million USD
- Losses in Germany based on Symantec: 33 Billion USD
- Number of "data manipulation" in Germany in 2010 based on official statistics: 2.000
- Number of Germans affected by computer virus: 12.000.000

What is known is that the losses caused by Cybercrime can be significant. Losses are not only related to direct financial losses but also necessary investments in Cyber security and loss of reputation when incidents happen. It is important to give guidance in this regard e.g. reporting obligation / establishment of reporting mechanisms (complaint center) [8].

3.1 Types of Cybercrimes most prevalence in Nigerian

The following are some of the cybercrimes most prevalence in Nigerian.

3.2 Yahoo Attack

Also called 419 because section 419 of the Nigerian criminal code has a law against such offenders. It is characterized by using e-mail addresses obtainedfromthe Internet access points using e-mail address harvesting applications(web spiders or e-mail extractor). These tools can automatically retrievee-mail addresses from web pages. Nigerian fraud letters join the warning ofimpersonation scam with a variation of an advance fee technique in which ane-mail from Nigeria offers the recipient the chance to share a percentage of a hugeamount of money that the author, a self-proclaimed government official, is trying tosiphon out of the country [9].

3.3 Hacking

Here, Nigerian hackers are engaged in brainstorming sessionsattrying to break security codes for e-commerce, funds point cards ande-marketing product sites.

3.4 Software Piracy

Piracy involves the unlawful reproduction and sharing of applications software, games, movies/videosand audios.

3.5 Pornography

Pornography covers all types' photography, films and videotapes with varying degrees of sexual contents.The Internet has provided a free market for this crime as so many pornographic sitesare now all over the net. This is one of the most popular cybercrimes in Nigerianacademic institutions [4].

3.6 Credit Card or ATM Fraud

Credit card or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction or when withdrawing money using ATM card. The hackers can abuse this card by impersonating the credit card holder.

3.7 Denial of Service Attack

This is an act by the fraudster who floods the bandwidth of the victim's system or fillshis e-mail inbox with junk mails depriving him of the services he is entitled to accessor supply.

3.8 Internet Relay Chat (IRC) Crime

IRC servers have chat rooms in which people from anywhere in the world can cometogether and chat with each other. Criminals use it for meeting co-conspirators. Hackersuse it for discussing their exploits and sharing the techniques.

3.9 Virus Dissemination

A virus is a computer program that infects files, frequently executable programs,by inserting a duplication of itself into the file. There are different types of virus and each type requires human participation (usually unaware) of their spread.

3.10 Phishing

Phishing refers to cloning product and e-commerce web pages in order to dupe unsuspecting users. This is a technologically advanced scam that often uses spontaneous mails to trickpeople into disclosing their financial and/or personal data.

3.11 Cyber Plagiarism

This is the act of stealing peoples' ideas through the Internet public domains. This is very common in academic institutions as students and lecturers alike use it to steal other people's ideas and publish them as their own original work.

3.12 Spoofing

To have one computer on a network to act like another computer, usually one withexceptional access rights, so as to gain access to the other systems on the network.

3.13 Cyber Stalking

The fraudster follows the victim by distributing mails and entering the chat roomsfrequently.

3.14 Cyber Defamation

The fraudster sends e-mails containing defamatory content to people related to thevictim or posts it on a website.

3.15 Salami Attack

Salami assaults are flamboyant economic scams or exploits against confidentialityby comprehensive data gathering.

3.16 Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents (searchsecurity.techtarget.com [10].

IV. METHODOLOGY OF THE RESEARCH

The method we employed in this research was the survey method while the research design used was the purposive research design technique so as to meet up with the targeted presentation date. The survey method was used because our aims are to get the awareness from users of the computer vis-a-viz the Internet and to determine the impacts of these menaces on the economy.

The population of this study is the Bursary Department and Computer Science Department of Babcock University in order to get the impacts from the professional while the Computer and Internet users mostly students and Lecturers. A sample size of 60 was selected using the random sampling procedure from the targeted population of 120. The method used to collect data for this study is structured questionnaire. A total of 60 copies of the questionnaire were personally administered out of which 55 copies were retrieved in usable form. This represents a response rate of 91.6%. The responses from the respondents were collated and analysed using the simple percentage procedure and bar chart.

V. ANALYSIS OF DATA

The responses to the questions in the questionnaire provided the basis for the following analysis. The key to the table are SA: strongly agree, A:agree, U: undecided, D: decided, and SD: strongly decided

Table 1, Perceived awareness level of respondents to cyber crimes

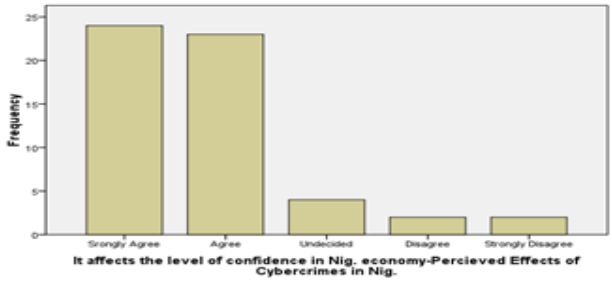
Source: Field survey

Types of Cyber crimes	Options	Frequency	Percent
Cracking	SA	29	52.7
	A	24	43.6
	U	1	1.8
	D		
	SD	1	1.8
	Total	55	100
Software Piracy	SA	29	52.7
	A	17	30.9
	U	2	3.6
	D	5	9.1
	SD	1	1.8
	Missing	1	1.6
	Total	55	100
Pornography	SA	22	40
	A	18	32.7
	U	4	7.3
	D	4	7.3
	SD	5	9.1
	Missing	2	3.6
	Total	55	100
ATM fraud	SA	29	52.7
	A	17	30.9
	U	2	3.6
	D	2	3.6
	SD	4	7.3
	Missing	1	1.8
	Total	55	100
Yahoo yahoo/extortion	SA	25	45.5
	A	21	38.2
	U	1	1.8
	D	2	3.6
	SD	5	9.1
	Missing	1	1.8
	Total	55	100

From the table 1. It shows clearly that cracking is a major crime in our society with the frequency of 29 and percentage of 52.7% while the least which was strongly disagree went for 1 with a percentage 1.8%. This improvement may not be too far from the fact that Internet is almost available for every user. Almost the same level of awareness goes for pornography, software piracy and ATM fraud with the frequencies of 22, 29 and 29; and percentages of 40%, 52.7%, 52.7%. It won't be out of place if we assume that the increment in all these mentioned cases are also as a result of the availability of Internet connectivity. Another prominent cyber crime we have in our society today is the yahoo-yahoo (cyber extortion) which seem uncontrollable, table 1 shows that 25 respondents strongly agreed that it is a noticeable crime with a percentage of 45.5% while only 1 respondent remained undecided with a percentage of 1.8%. Despite the high level of benefits derived from the use of the Internet, it almost seems the disadvantages are appearing to be overwhelming.

5.1 Effects of Cyber crimes on Nigerian Economy

The bar charts below shows the effects of cyber crimes on Nigerian economy.



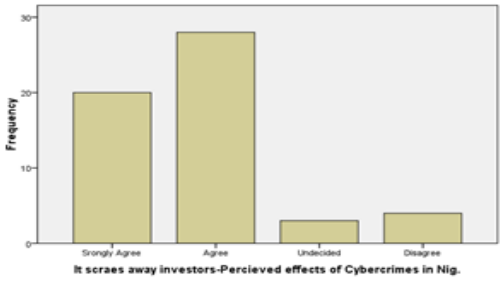
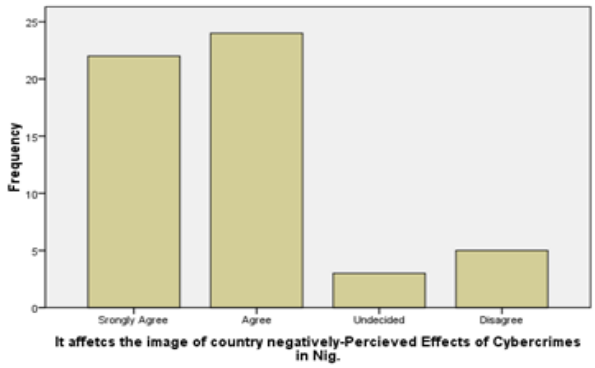


Fig.1 Effects of cyber crime on the level of confidence of Nig. economyFig.2 Effects of cyber crime on the level of investors

The result displayed on figure 1 above shows the effects of cyber crime on the level of confidence of the country. It is very clear based on the accumulated results that majority of the respondents believed that cyber crime has a significant effects on the level of confidence of any nation. Prospective investors are no longer save, people tends to run for safely and seek shelter where such could be found and this may not be too far from the reasons why we lose most indigenous investors to other African countries because of our low level of confidence. Nigeria is a country where offenders are rather celebrated rather than punished. In the same veinisthe result shown in figure 2, which is, the effects of cyber crime on the level of investors. It is easy to establish that once the level of confidence is low and investors are counting loses as against profits, for such business to survive; they would have to migrate to countries where profits margins would be higher.



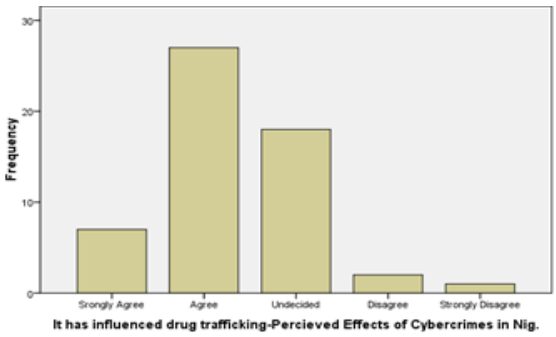
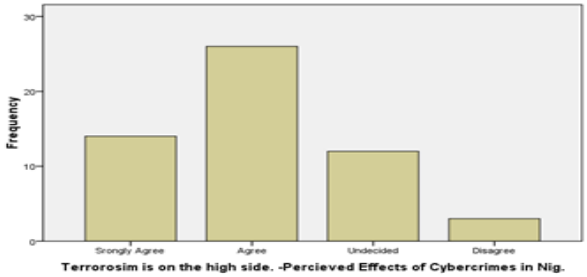


Fig.3 Effects of cyber crimeon the image of Nigeria Fig. 4 Effects of cyber crime on drugs

The results shown above in figure 3 and figure 4 illustrate the effects of cyber crime on the image of the country as well as on drug. Figure 3 shows that if a country like Nigeria is highly polarise by cyber crime, communication within and outside such a country would be difficult because everybody will appears as a suspect which would in turn have a negative impression on such a country. Therefore, respondents strongly agreed and also agreed that this is possible while few respondents disagree with this view. Figure 4 in similar way demonstrated the effects on drug trafficking. A large portion of the respondents agreed that cyber crime would have a consequential effects on drug trafficking. This is possible because transaction takes place on the Internet both legal and illegal transactions. Drugs are both, sold and delivered on the Internet.



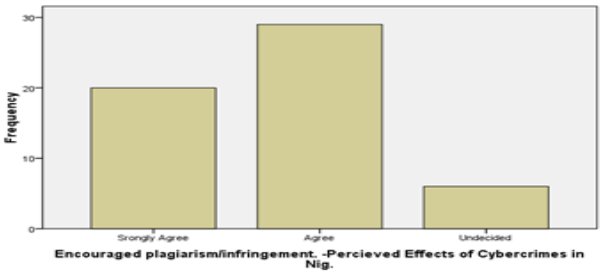


Fig. 5 Effects of cyber crime on terrorism Fig. 6 Effects of cyber crime on plagiarism/infringement

Figure 5 shows the effects of cyber crime on terrorism. This is clear from the chart that most respondents agreed that cyber crime has high effects on terrorism. Nigeria at today is a case study of one of the countries that suffer greatly in the hands of local terrorist called 'boko haram'. They were able to penetrate their acts through the use of Global System of Telecommunication (GSM), YouTube among others. Also, the results shown on figure 6 where most respondents agreed that cyber crime has a significant effect on plagiarism/infringement. In academics, it is a popular slogan that 'you either publish or perish' Most researchers are no longer interested in adequate research that can find solutions to the impending challenges facing countries around the world rather, copy and paste (CAP) is the order of the day. The same syndrome is also affecting our students from all cadres.

VI. CONCLUSION AND RECOMMENDATIONS

From our investigation on cybercrimesweobserved its threat to the economy of a nationand even peace and security. Thereforethere is need for a holistic approach tocombat these crimes in all ramifications. Ourproposal therefore is the need for cyberpolice who are to be trained specially tohandle cybercrimes in Nigeria. In addition,the police should have a Central ComputerCrime Response Wing to act as an agencyto advise the state and other investigativeagencies to guide and coordinate computercrime investigation. We are also proposing thatthe country should set up National ComputerCrime Resource Centre, a body, whichwill comprise experts and professionals toestablish rules, regulations and standards ofauthentication of each citizen's records andthe staff of establishments and recognizedorganization, firms, industries etc.Forensics commission should be established, which will be responsible for thetraining of forensics personnel/law enforcement agencies. Above all, acomprehensive law to combat computer andcyber related crimes should be promulgatedto fight these phenomenon'sto a halt. Ourproposal on the nature of law to combatcybercrime is not included in this paper. We recommend that before anybody enters into any kind of financial deals with anyonethrough the internet he/she should use anyof the search engines to verify the identityof the unknown.

REFERENCES

[1] N.A. Azeez, O. Osunade, Towards ameliorating cybercrime and Cybersecurity*(IJCSIS) International Journal of Computer Science and Information Security, Vol. 3,* No. 1, 2009

[2] M. Sackson Computer Ethics: Are Students Concerned. *First Annual EthicsConference*(1996) Available online at http://www.maths.luc.edu/ethics96/papers/sackson.doc

[3] C. Shafic, andAdamu*Cybercrimes and the Nigeria Academic Institution Networks Cybercrime, its impact on government, society and the prosecutor*2011

[4] O. Longe, I.Omoruyi, and F.Longe, Implications of the Nigeria Copyright Law for Software Protection.*The Nigerian Academic Forum Multidisciplinary Journal.Vol. 5,* No. 1.pp 7-10. 2005.

[5] N. Ribadu Cybercrime and Commercial Fraud: A Nigerian PerspectiveModern Law for Global Commerce Congress to celebrate the fortieth annual session of UNCITRALVienna, 9-12 July 2007

[6] HEISE News, 2007 http://www.heise.de/open/meldung/Auswaertiges-Amt-spart-im-IT-Bereich-kraeftig-dank-Open- Source-151012.html

[7] M. Gercke*Asia-Pacific Regional Workshop on Fighting Cybercrime* 21. – 23.09. Seoul 2011 Available at http://www.itu.int/ITU-D/asp/CMS/Events/2011/CyberCrime/S3_Marco_Gercke_1.pdf

[8] Crimes Commission (Establishment) Act 2004.

[9] S.WBrenner, *Cybercrime: Criminal Threats from Cyberspace, an Imprint of ABC-CLIO, LLC,* Santa Barbara, CA, 2010, ISBN 978-0-313-36546-1 available at http://law.suffolk.edu/highlights/stuorgs/jhtl/book_reviews/2010_2011/Anna%20Cometa%20-%20Cybercrime.pdf

[10] Cyber terrorism http://searchsecurity.techtarget.com/definition/cyberterrorism