

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 2 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

APIS – 3920 – 0013 | ISSN - 2583-7990

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://ijclp.iledu.in/

Journal's Editorial Page - https://ijclp.iledu.in/editorial-board/

Volume 2 and Issue 1 (Access Full Issue on - https://ijclp.iledu.in/category/volume-2-and-issue-1-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer https://ijclp.iledu.in/terms-and-condition/

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 2 AND ISSUE I OF 2024

APIS – 3920-0012 | ISSN - 2583-7990

Published by

Institute of Legal Education

https://iledu.in

THE CYBERCRIME PREVENTION IN CRIMINOLOGY PERSPECTIVE

AUTHOR - DR. AMAL KHALAF SUFHAN AL-HABASHNEH, ASSISTANT PROFESSOR OF CRIMINAL LAW, FACULTY OF LAW/ AL - ISRA UNIVERSITY. EMAIL - AMAL.ALHABASHNA@IU.EDU.JO

BEST CITATION - DR. AMAL KHALAF SUFHAN AL-HABASHNEH, THE CYBERCRIME PREVENTION IN CRIMINOLOGY PERSPECTIVE, *INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY,* 2 (1) OF 2024, PG. 31-42, APIS – 3920-0012 | ISSN - 2583-7990.

Introduction

Cybercrime is a crime in the field of cyber technology and informatics. This can involve individuals, organizations, and governments. On the other hand, it is easy to conduct but difficult to detect, as it has all sorts of tools and mechanisms. A person who observes it is often unaware of being a criminal and is increasingly turning into a public area. In this study, the aim is to introduce the concept of crime in information and communication technologies through a general framework, to address the problem of cyber theft and default, to define the legal framework regarding international cooperation, and finally, to discuss whether there is a change in perception related to cyber theft. This includes occasions of communication, cyber theft, sexual victimization, reproduction and dissemination of pornographic images, and hate speech. In addition, these studies will aim to draw attention to the fact that with the development of technology, these crimes are transformed into an indispensable part of crime stories.

1.1. Overview of Cybercrime

Unlike the business sectors, public services, and academic/digital communities that emphasize the use of technology and other advanced systems, the ongoing increasing threat of cybercriminal acts from various technological developments calls for a comprehensive legal policy to minimize these risks. Among the many technological developments, the Internet is the easiest to use. Unfortunately, the ease of access results in various forms of criminal activities. As a result, almost every country on Earth has taken cybercrime law enforcement action. On an international level, cybercrime identities receive global viewpoints from various institutions. Furthermore, academics also offer significant attention to responding to an increased number of cybercrime cases that occur in their countries.

However, cybercrime is complex since it is anonymous and borderless. At least in its characteristics, the intruders might be part of the country's high-ranking officials, or they might be typical traditional criminals. While the potential for a victim's dispute becomes increasingly expansive, the psychological and economic effects are wide-ranging. Even in the face of these difficult challenges, their behaviors are not given as significant a consequence as regular or other types of crime. Even their tendency to consider not incarcerating electronic crimes is reflected in the legal punishment of the death penalty. Countries around the world are starting to make adequate legal efforts or comprehensive dialogues. It is also necessary to form interstate and international conventions. Their renegotiations are also a heightened attempt to stop and, in some cases, decrease the quickly approaching danger.

Importance of Cybercrime Prevention

There is a growing understanding among all stakeholders that the public-private partnerships fostered under the Convention are pivotal to the success of the global struggle against cybercrime. Through such partnerships,

services provided by the private sector are improved and, at the same time, the law enforcement community is better positioned to prevent and respond to cybercrime. Though details of implementation are often complex, there are essential ingredients that can help formulate these public-private partnerships. What is foremost in importance is the realization that as the private sector helps to harden the global infrastructure and to develop new products that enhance online security, organizational and personal security measures in the private sector and in individual organizations are vital to the international enforcement effort in the cyberspace that our global society enjoys. Also, it is imperative that all stakeholders in the enforcement community, both domestic and foreign, work in cooperation with broadband service providers to facilitate the development of innovative but necessary practices that foster the evolution of those providers as community good citizens.

Criminology Perspective

One way to identify crimes involving misuse of IT is by utilizing a criminological perspective. Based on the dynamic computer crime triangle framework, cybercrime occurs when three important components exist simultaneously. First is the offender who possesses the motivation to commit a crime. Second is the presence of at least one other party who is the target, the facilitator, or the supporter of the criminal act. Third are the cyber tools that empower the offender and create risks for the victim. When all these elements converge, a wide spectrum of cybercriminal and deviant activities can take place. This framework delineates a broad spectrum of cyber activities that straddle various forms of hacking, digital sabotage, online theft, data and identity theft, cyber fraud, digital surveillance, cyber intimidation, infringement of intellectual property rights, online child pornography, online prostitution, in addition to the social and technical engineering of digital innovation for illegal activities.

The use of a criminological perspective in understanding cyberspace criminal activities and cyber law enforcement has attracted much attention, especially among policing experts, criminologists, and legal scholars. These scholars say that due to the absence of consensus and shared definitions of cybercrime, it is very important to understand cybercrime in cyberspace by examining the nature, dynamics, and scope of cybercrime. Until now, there is no single uniform approach or theory to explain the use of IT for criminal activities. These many approaches can be classified into environmental criminology and learned, cultural, and social control theories. The former views the interaction between offenders, targets, and the context of the commission of crime, while the latter views that criminal behavior results from learned cultural interaction between various factors and social control mechanisms.

Historical Evolution of Cybercrime

In seeking an understanding of the implications of incorporating the concept of cybercrime into criminological thought, it is important first to set the stage by emphasizing that the functionality of both technology and the human components of the emerging 'Information Society' has aged dramatically in the past few years. This age has led, among other significant challenges, to growing concerns over illegal or dishonest activities conducted with, or directed at, the mass of new ICT-based systems and services. The most striking of these 'illegal or dishonest' activities has become, especially, the targets of a range of governments and the related law enforcement agencies who use 'cybercrime' as an offensive label in their war on criminal activities that are either computer technologies or are supported by them. This concern with the 'resonance or reality' of the concept 'cybercrime' is seen as an interesting test case in one of the key issues within criminology, that is, the significance or otherwise of crime control in determining the purpose and character of criminological thought. The introduction to the specific issue of how criminological thought can

be extended or made more useful by using the concept of 'cybercrime', with particular reference to the affluent 'Information Society' countries, is followed by a brief introduction to the key features of this phenomenon. This leads to a brief description of cybercrime and the cybercriminal. In the outright rejection of using 'cybercrime' as the basis for developing criminological thought, it is argued that this promotes and develops a 'social harm' based approach that not only includes all of the psychological, legal, and social reasons, and social mechanisms for information technology-related criminal actions but also directly addresses the concepts of crime and victimization. The laundering of proceeds of crime is recognized as a major criminal service linked to the cybercriminal, outlining historical aspects of criminal behaviors specifically associated with different technologies, from the earliest times through to the present day.

Early Instances of Cybercrime

In 1965, the advent of accessing computers from another location encouraged what is probably the first case of 'hacking.' This was apparently by students who modified their institute's computer to engage in presumably innocuous activities, such as accessing computer usage records at a nearby university. Nonetheless, a more notorious case of computer hacking, popularized in 1983, is that of a teenager who tapped into a computer network. Subsequently, important issues pertaining to unauthorized access to a computer and hackers being tried in courts were raised.

Clearly, incipient Internet users have been primarily those granted access through the computer due to vocational enrichment. Therefore, its purpose in effecting a community of researchers and businesspersons nourishing the Internet wound up being a rudimentary one. These initial positive effects soon became overshadowed by several illegal activities engaged in by some of the users. The cybercrime myth should be dispelled, as the concept of criminal activity in life has transmuted to denote illegal or unauthorized activity effected on or through the computer and its attachments. Simply put, this criminal activity performed respectively is crime, as it is not tagged as such necessarily because the perpetrator commits the ill.

Development of Cybercrime Laws

The development of cybercrime laws in many countries has shown a rapid and sometimes dramatic process since the late 1990s. Before the introduction of local laws, many countries did not have any provisions specifically criminalizing electronic and computer crimes used for criminal purposes. In the United States, cybercrime laws took the form of amendments. The earliest precursor to a cybercrime law is the Computer Fraud and Abuse Act of 1984. A more comprehensive act was passed in 1986 that made hacking, which is breaking into computers, a criminal act even if the computer was not damaged. Subsequent amendments were passed in 1989 to update the code to cover classified information, documents related to foreign relations, and at the same time increased the severity of the provisions for unauthorized access and use, unauthorized alteration and destruction, and trafficking in stolen computer passwords. In 1994, further amendments were made to the code together with the Cable Communications Policy Act and the Electronic Communications Privacy Act.

In Britain, the process was also characterized by successive acts with amendments. The 1990 Computer Misuse Act was the first act to criminalize hacking in Britain. Section 1 of the act criminalized unauthorized access to computer systems and unauthorized access with intent to commit or facilitate the commission of further offenses. The 1994 amendment made unauthorized alteration of computer data an offense. The Council of Europe's cybercrime laws development was embodied in the Convention on Cybercrime. Since 1997, when the concept paper of the convention was adopted, the document was finally signed in 2001. The

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

convention was opened to parties for signatures in November 2001 and it entered into force in 2004.

Types of Cybercrime

There are at least three factors that differentiate cybercrime from other types of crime. First, cybercrime is an international crime, so law enforcement in various countries is required to fight this crime if needed. Second, it is assumed that cyberspace or the internet, which is used as a medium in the occurrence of a cybercrime, does not have boundaries, making it not entirely impossible for a person to break the law in more than one country. Third, the nature of cyber features can create new or well-established offenses that can change the structure of a crime. Based on these features, the types of cybercrime are: – Crimes that use the computer as a direct weapon against physical entities, or parts of a computer itself. In other words, – Crimes that consider the computer as a tool of the crime, – Types of cybercrime that also grow due to the existence of technology.

Although internet technology has developed positively, it does not just happen without any negative impact. The use of the internet sometimes deviates from the actual objectives, leading to challenges and threats that can disrupt security and law and order, commonly referred to as cybercrime. Cybercrime is a crime that uses a computer and a network connection in a crime or as a target, including crimes such as fraud, piracy, and credit card fraud. Cyberspace can provide a place for dangerous actions because of its nature that is not humiliating, allowing criminals to act at will without having to face their opponents. Individuals who use cyberspace can remain anonymous online, which makes it easier to break the law without worrying about the consequences. That is why, for criminals, cyberspace provides a vast area of action. This is a fact that emphasizes the importance of reducing cyber concerns from a criminal perspective.

Cyberbullying

The invention and recognition of computer technology provide advantages as well as risks in its use. No one can predict that the risks related to the use of computer technology have been increasing. There is a term, cyberbullying, in the context of the use of computer technology that refers to the activities of students at schools. Cyberbullying is regarded as acts of harming an individual by manipulating electronic media and is on the rise. The effects of cyberbullying on students show similarities to those of traditional bullying. They are exposed to the negative effects of cyberbullying. Therefore, a great number of studies have been addressing the present problem of cyberbullying. Cyberbullying is defined as "an individual telling lies about victims, revealing victims' secrets and private information, or sending hate or threat emails purposely to harm victims."

Identity Theft

3. Cybercrime Cases 3.2. Identity Theft

Identity theft is one of the fastest growing crimes in the United States and the world. Identity theft is a crime in which an imposter takes on the identity of a victim and attempts to defraud. Identity theft, one of the most notorious online crimes, has surpassed drug trafficking as a money maker, and many experts believe it has become the biggest financial growth industry of the 21st century. In many countries, this crime has become a favorite of bandits. Its popularity ensures that it will continue to be known in the weeks, months, and years to come. The seriousness of identity theft and the difficulty of preventing it necessitate more aggressive prevention by increasing public awareness and urging government intervention and internet protection.

With the rapid expansion of the internet and e-commerce, all people's identities are increasingly stored as electronic data. It is not only a challenge to protect personal information, because it may lead to the loss of

personal privacy, but also because it may cascade into more dangerous cybercrime. The reasons for committing identity theft vary depending on the motive of the crime, and computer security professionals must reconsider the identity authentication process to defend against the crime. The emergence of a new technology, ubiquitous computing, can help defend against this complex crime if data protection problems are resolved. Many studies have been conducted on the identity theft prevention problem, and most discuss the specific attack vectors without solving them and do not provide overall solutions. However, it is an important comprehensive problem to solve because preventing identity theft has to slow down money laundering, financing terrorism, and cybercrimes, and make the use of online services safer.

Phishing

Phishing is an internet criminal activity that is increasingly evolving. It is a cyber crime that attempts to fraudulently acquire confidential information, such as usernames, passwords, and details of bank accounts by masquerading as a trustworthy entity in electronic communication. Phishing has become a lucrative and organized crime business. Often, groups of individuals or criminal organizations gather to plan sophisticated strategies to tackle cyber crime while maintaining a degree of anonymity and ongoing insulation from law enforcement. Many different prevention methods are used to ensure that the victim will never have access to it, but they do not want the victim to know and then change their password. The prevention methods involve the use of deceived webpages and deceptive messages to detect phishing websites. This prevention method uses information about the virtual host and SSL/TLS certificates to detect the bad virtual host and deceptive messages by the defined model. Results of this prevention method show the detection ratio at the optimal model. The detection ratio and false alarm rate of the deceived webpages and deceptive messages are 0.995, 0.267, 0.982, and 0.044.

Theoretical Frameworks in Criminology

Criminology has several theoretical frameworks, starting from the old theories and feudal systems that sought to explain the criminal phenomenon, and the birth of the classical school of criminology. They generate interest from various angles of research because they are close to the social control that contemporary society exercises. Modern authors observe that what is important is not the defense of the rights of individuals in an incisive way, being invaded by illegal acts, but in creating a legal and social protection in order to prevent them from being affected by the harms that crime causes. Law is a form of social control established by the dominant group and imposed on the rest of society to maintain order. It is a regimented and coercive discipline; that is, it guides compliance with the established norms and ensures a climate of security and functional operation of the social order.

Another important school of criminology is the positivist school, which addresses the relationship between behavior and the criminal, especially when the human being is linked to the initial crime. It has as its basic point the study of the personality of the individual and the hereditary and environmental factors that contribute to crime, well ahead of determinism, that is, the physical, psychic, and social influences. In this sense, it is extremely important to understand why an individual exhibits such behavior. It is concluded that determinism, which refers to the external influences on man according to certain causes, eliminates his freedom of choice and is the foundation of the analysis of this theory concerning the criminal phenomenon. In this case, it stops being the classic problem of the social group and is considered a pathology of the individual.

Routine Activity Theory

Crime prevention theory attempts to explain every aspect of a criminal act. The routine activity theory is a classical crime prevention

theory and is important for certain stakeholders in preventing the commission of internet crime. For the past 20 years, routine activity theory has been popular in explaining the causes of certain criminal acts and has proven to be highly significant in explaining the sudden emergence and decline of modus operandi used by certain criminals at specific places and times. Routine activity theory became a newly recognized criminal science after its initial proposal in 1979. Initially, routine activity theory explains the criminal acts of so-called undefendable high emotional needs and the social distance between two parties. The theory was proposed by classical social scientists in response to the failure of attempts to explain criminal acts based on social structures. According to routine activity theory, society will always be a victim of certain criminal acts, and there will always be a group that tends to engage in criminal behavior.

Social Learning Theory

One of the most widely accepted theories in criminology is the social learning theory. The social learning theory assumes that people learn about criminal behaviors that are available as norms. They will commit crimes if they are exposed to more reasons to commit the crime and fewer deterrents. Family and social environments play the most important part in socializing the individual to community standards and minimizing the opportunities to engage in habitual criminal behavior. The military and the police recognize, stress, and respect the need for training and other supporting actions to offset and control crime. Social learning theory suggests that training can deter cybercrime.

It may be that if certain training can more closely absorb the relationship among the parent, core rule of law, and basic organizational precepts (which control the military and police institutions and operations by their values), and if the service member is taught that one of his responsibilities in conforming his behavior to the requirements of that core value system is to prevent cybercrime, his levels of motivation to adhere to that set of standards will operate effectively. While this solution to cybercrime in the military is certainly not the only one, social learning theory and the broader criminological models suggest that it could be a vital ingredient.

Cybercrime Prevention Strategies

Cybercrime prevention strategies need to have four specific focuses: international collaborative efforts among criminal justice agencies, shared jurisdictional power of law enforcement professionals, an increase in the effectiveness of various computer and internet security measures, and enhancement of criminal justice enforcement against cybercrimes. Criminal justice agencies around the world are working together to promote some fundamental principles, recognizing that these crimes range across international borders. An enforcement response will be most effective if it is part of a collaborative effort by law enforcement, private organizations, and government agencies within countries and internationally, and that no one entity can address all cybercrime needs. This concept of shared jurisdiction and power within a diverse group of professionals provides an enforcement solution that offers the best approach for many varied crimes.

An effective response requires that the computer and internet industry has incentives to produce and market secure equipment. Many strategies have been suggested to enhance this incentive; for example, urging the federal government to spend more money to support basic research, which allows computer security innovation to take place, or that industry leaders will investigate appropriate growth in technology to showcase new techniques for computer security. Computer owners must recognize that computer security is not a one-time purchase. They must undertake a long-term investment in their equipment. Computer security packages are adequate for internet messages in part because many internet users do not

understand or install the necessary security features in hardware, software, and communications. There are almost no legal consequences or costs to individuals who do install these security programs. The focus of this principle is on enhancing criminal justice enforcement against cybercrimes. Data on this last step, including computer fraud statistics, are essential elements that demonstrate how this focus would affect the way little data help us determine the effectiveness of the criminal justice enforcement response. In other words, this data can help us identify who are the most likely offenders in securing computer networks. What social and ethical pressures are overcoming people in order to violate computer laws? Are these crimes being reported, and what explains why these crimes are not usually reported? What institutional, structural, organizational, and group pressures need to be overcome in order to promote more consistent enforcement? What unique characteristics have to be taken into account in order to develop a comprehensive and ecologically valid theory of criminal behavior in the computer age that promotes efforts to predict and control crime in this sector? The modern investigative analysis in the study of the costs and benefits of program innovations.

Legislation and Regulation

The effective anticipation of increasingly complex cyber violence absolutely requires an effective legislative arsenal in some areas, possibly combined with contractual measures to which the general and judicial public authorities should not be strangers. The efforts made in terms of international law and the cooperation in place or under discussion are naturally also to be taken into account in a systemic approach, and this in light of the gradual emergence of a surety society where private actors could take the place of public authorities, and still lack knowledge and legitimacy to do so in a proportionate manner and in the state respects, while this is legitimate in a democratic society.

The increasing use of new prevention systems or new technologies makes it necessary to keep abreast of the latest regulatory developments and certain highlights. Some large companies and administrations are subject to specific provisions, be they general or special, linked to the processing of information concerning individuals and the adoption of protection in the field of computer security. In particular, the companies of the nuclear and banking sectors, which must ensure the reliability of the computer systems that make them necessary and the consequence of a breakdown would cause, are subject to considerable obligations. As such, they must take into account the provisions of data protection regulations before processing personal data with the aim of guaranteeing a high level of security and protection of said data.

Law Enforcement Efforts

Efforts to prevent crime should be multi-systemic, inclusive, and protective through law enforcement. Protecting the community against cybercrime involves several problematic systems, such as cybercriminal perpetrators, rapid technological changes that provide completely new opportunities and increased risk of victimization, increasing electronic information use, global use of electronic technology, and the fact that a country can be a potential target for cybercrime success. Law enforcement in Malaysia is currently in a traditional phase familiar with dealing with more serious legal issues. It is quite difficult to respond to the ever-reducing number of cybercriminals worldwide. In addition to these challenges, there is no international criterion because offenders are located and found differently within jurisdictional limits. There is no international curriculum to date.

Recently, the Cyber Law enforcement in Malaysia has initiated numerous efforts related to law enforcement. These include the creation of new punitive structures for a group of offenses against computers and data, the establishment of powerful specialized

investigative units, and the creation of canceled units within law enforcement. This situation is exacerbated by widespread doubts about the law, which is an agreement or other corrective measure required to provide facilities for a victim or a witness located in their jurisdiction while committing the offense.

Role of Technology in Cybercrime Prevention

The rapid evolution of information technology has also led to cybercrime growing in intensity and possibility. More and more people have access to new information technologies, while criminals in cyberspace accurately comprehend the opportunities and bring forth improvements. Based on rational choice theory, numerous studies have revealed that increasing the price and severity of imprisonment for potential criminals will generally yield a negative result for society. As the opportunity to commit more cybercrime is correlated with the lower costs of computer execution, the proximity of fast speed, global expanse, and the ability to act covertly creates an unfavorable area for crime, further attracting possible criminals. However, no such study on the role of technological prevention in cybercrime prevention, as that carried out in conventional crime prevention, detailing how potential criminals perceive this in terms of expected protection, has hitherto been found.

Given the place of technological prevention among the types of cybercrime prevention, we begin with a brief account. We then introduce the half-price theory, which exemplifies an alternative to the conventional first strategy in crime reduction. Utilizing the half-price theory as a theoretical basis, the influence of using technological barriers as a prevention strategy on the expected loss of criminals who have set up scaling without having committed cybercrime is discussed. The paper concludes by discussing additional studies about newly upgraded technologies in the context of breaking future half-price strategies for cybercrime prevention, in addition to policy implications.

Digital Forensics

In contrast to the technical approach to understanding computer and ICT activity as a predictor of individual deviance, digital forensics is concerned predominantly with obtaining evidence that can be used in the criminal justice process. Digital forensics investigations and preparations for its conduct are focused on two main domains – the actual digital or electronic domain dealing with issues relating to crimes committed directly through a digital interface with the Internet, as well as with 'old' volume crimes to which the Internet is now annexed, aspects of cyberstalking and cyberbullying, cases of digital vandalism, incitement to hatred or targeting of members of vulnerable groups, virtual assassination, and other forms of anti-social behavior including cyberpropaganda, cyberpornography, violation of privacy, theft of digital property, and contravention of laws relating to brand identity and personalization.

As regards the digital or Internet domain per se, the infrastructure (being Internet dependent, such as phishing, spyware, access, and hacking) and stage digital or cybercrimes (either those activities that require the Internet to commit the crime, such as theft, extortion, or cyberbullying, or those crimes modernized to include the Internet in their process such as cyberterrorism or killing). While there is more detail by distinguishing between crimes of opportunity and those which evolve during various stages of the Internet crime process; in terms of criminal phase, such as the intended physical or psychological effect, methods used to prepare for the crime and those used to commit the crime.

Artificial Intelligence

Artificial intelligence (AI) is believed to be an element in the future of criminology studies. AI can be utilized to provide services related to supply and demand throughout the criminal justice process and can gather information from several database sources to lend support and advice on intelligence analysis,

assessment, and anticipation. Artificial intelligence can also be utilized in data mining and crime mapping. It can detect data patterns and group them into emerging new formats to provide forensic investigations with the requisite groundwork. Furthermore, AI, as a new method, can be used to develop a more extensive inspection of criminal behaviors and produce a criminal impact investigation simply by being designed from economic data relating to commercial crime and a combination of other sources of information. Despite the benefits of AI in criminological studies, it is essential for researchers to be aware that there is no complete substitution for humans in the examination of data analyses from fledgling sources, including cross-boundary sources.

Computer scientists, economists, criminologists, and others are regularly utilizing data analytics to fight criminal activities. While it is essential to gather information in such a way that it is both valid and accurate for effective utilization, the concern that government authorities have an unjust role in data gathering related to the transformation and reinforcement of specific norms demonstrates the need for a legal barrier. Nevertheless, the breakdown and subsequent deliberation on the defined barrier allow individuals to gain a clear understanding of the potential problems as the research transformations describe the implications of the previously highlighted challenges and barriers on the study of criminology. The correct response to the question of whether it matters if barriers between cross-disciplinary research fields like artificial intelligence, when integrated into business and criminology, no longer exist is that it is highly necessary for two reasons. Ten years before the concept of artificial intelligence emerged, criminal activities already existed. During prehistoric times, crime began transitioning alongside individuals, and cybercrime eventually came into being. The integrated field of artificial intelligence and criminology is slowly becoming one science. Researchers are regularly utilizing data analytic tools, machine learning, and AI. The documentation of such efforts and things to come is obvious. Four common areas are currently emerging in that new terrain: artificial intelligence, crime mapping, predictive policing, and forecasting the necessity of criminological research.

Challenges and Future Directions

There are a number of ongoing and potential challenges facing the conceptualization and criminalization of victimless computer crime. Criminologists continue to debate and seek to understand why people commit computer-based crime and the relationships between characteristics such as strain, conflict, identity, and attitudes. Once the causes of such variations have been identified and understood, the likelihood of someone actually committing a computer-related crime needs to be known. Considerations include the specific conditions under which pressure is experienced and how situational factors drive the criminal act. Might the causal logic surrounding computer-based crime and more traditional crimes, both in terms of general theory and practice, be similar? Highlighting which circumstances make computer-based crime attractive for certain people satisfies a rationality of sorts; the decision to commit the offense is considered a crime of opportunity. It is hoped that the existence of some of these incentives is believed to stand as a means of control.

An additional challenge for crime prevention strategies, techniques, and tools is understanding what such interventions are able to do. What are the endeavors that governments and agencies should really be doing, given the inexorable rise and technological nature of many forms of contemporary computer crime and, in particular, cybercrime? The capacity of the creators and purveyors, as well as legislators, to adhere to regulatory provisions designed to prevent such laws also needs to be considered. At present, the scale of the problem is substantial and is growing exponentially. All steps in the chain of regulatory compliance are

essential. Similarly, challenging what associated efforts can and cannot do is also crucial, given the current state of our knowledge and understanding of the underlying and key factors that motivate, create incentives, and opportunities for people to commit computer-related crimes, and the instruments and tools to prevent, deter, or indeed punish the perpetrators. What must constantly bear repetition, even more so in more advanced societies, is an enlightened comprehension of the personal and social consequences of criminality. The isolated, individualistic, and practical nature of economic crimes from the perspective of legal sanction should not be ignored. The integration of economic theory can and should help to develop a more educated and committed field. Our work seeks to contribute to this knowledge and understanding, with more sophisticated legal provisions that sentence these perpetrators.

Global Cooperation

Based on the characteristics of cybercrime and enforcement difficulties, only an isolated country cannot effectively combat cybercrime. Strictly speaking, the advancement of technology has enabled the development of the Internet. Countries must therefore promote appropriate regulations in order to provide convenient digital environments. Only then can they generate positive aspects, promote digitalization, and further develop their nation. All countries have either joined or are in the process of joining hands to respond to cybercrime. They have joined several international treaties and organizations, which deal with the development of policy concerning cybercrime. The organization has already produced a number of international treaties, laws, and guidelines in response to developing cybercrime, including the Lawful Access and the draft convention on "criminal acts in the information society".

All of these efforts are examples portraying a global focus and multinational cooperation of the international community to combat cybercrime. In promoting cooperation, consideration of the specific characteristics of the cyber environment and the nature of the crime being combated are essential. If the environment is not virtual and not being conducted by a well-organized criminal offender, this would not be a necessary issue in criminal enforcement. Given cyberspace's unique characteristics, it is impossible for people to compete with the invisible virtual body. They should not choose rivalry but cooperate with the invisible virtual body. Unfortunately, it is even satirical and odd to propose that each country join hands to cooperate with something invisible that they have never seen. The above description is rational and inevitable in the current environment of cybercrime. Cooperation between countries will have effective and successful anti-cybercrime efforts.

Emerging Technologies

One of the difficulties of defining cybercrime is its scope. This is a difficulty that many have addressed and have continued to address at several forums. As a society in which we live, we have never witnessed the extent of development and investment as we are currently seeing in spectacular technologies. The emergence of these technologies or the need to create better technologies for creating and communicating goods and services has forced a rethink and redefinition of some conduct in both civil and criminal law. Above all, it has created a new way of categorization different from those traditionally made in criminal law.

The task of overcoming these new crimes becomes even more difficult due to the current development of new technologies such as virtual reality, artificial intelligence, quantum cryptography, and programming carried out by means of direct brain instructions. These technologies break down all barriers, realities, and cognitive and emotional perimeters, rendering a solution to the existing problems even more distant. This means that we must

break with the traditional notion of fraud, both in name and in request, having to address new challenges not only through criminal law but also by the legislature as a whole. In this way, the search for a policy of criminal prevention in relation to cybercrime will become the same: the search for a policy for the prevention of the origin.

Conclusion

This is the paper entitled The Cybercrime Prevention in Criminology Perspective. The objective is to analyze and to correlate criminology, especially the prevention area that can be applied for cybercrime prevention. This paper came with secondary analysis that used the descriptive method based on the literature review which is isolated related on the cybercrime topics. The paper contributes an overview view of the criminological correlation to prevent cybercrime. Pre/Cybercrime prevention has become increasingly important with the existence of virtual world space. However far we try to avoid manipulating computer or cybercrimes in virtual worlds, the victims were infinite there and very real. This is different of the cyber-cybercime criminal who was then the consumer of the activity.

There is a gap of cybercrime prevention, whether from the understanding level or the application of prevention programs specifically. The activity in the virtual world should not be allowed undermining the life and safety of its existence that is in the physical world. Preventing cybercrime needs to be "down to earth" and too the real world specific, although by recognizing the cyber world characteristics. In reviewing cybercrimes, the criminological connecting is very much, so there is no reason for criminological approaches not to be applied for cybercrime prevention. The criminological correlation needs to be more feasible to be used as preventive tools, so it could build a safety cyber-world much better practically. For now, we know that every "human" prevention program as its main subject is a very difficult task firstly, so if these prevention programs could be constructed and evaluated more abundant, it would be an important achievement to deliver a much better real and virtual world of human life space. In the end, it sounds a transparent plea.

References:

1. Abrazhevich, D. (2004), "Electronic payment systems: a user-centered perspective and interaction design". PhD
2. thesis, Technical University of Eindhoven, Eindhoven. From Wendy Ming-Yen, Siong Choy Chong and
3. Jiat Wei Chua. (2013)."Factors affecting consumers' perception of electronic payment: an empirical analysis".
4. Internet Research Vol. 23 No. 4, 2013, pp. 465-485.
5. Abrazhevich, D. (2001), "Electronic payment systems: issues of user acceptance". In Stanford- Smith, B. and
6. Al-Qirim, N., 2007. The Adoption and Diffusion of E-Commerce in Developing Countries: The Case of an NGO
7. in Jordan. Information Technology for Development, Vol. 13, No. 2, pp. 107 –131.
8. Baddeley, M. (2004), "Using e-cash in the new economy: an economic analysis of micropayment systems",
9. Chiozza, E. (Eds), E-Work and E-Commerce, IOS Press, Amsterdam, pp. 354-360.
10. Al-Ma'aitah, Mohammad Atwah. (2012)."Using Electronic Collaborative Media according Organizational
11. Culture".International Journal of Computer Applications (0975 – 8887) Volume 37– No.5, January 2012
12. 42.
13. Al-Qirim, N., 2007. The Adoption and Diffusion of E-Commerce in Developing Countries: The Case of an NGO

14. in Jordan. Information Technology for Development, Vol. 13, No. 2, pp. 107 –131.
15. Baddeley, M. (2004), "Using e-cash in the new economy: an economic analysis of micropayment systems",
16. Journal of Electronic Research, Vol. 5 No. 7, pp. 239-253.
17. Bagozzi, R.P., Davis, F.D. and Warshaw, P.R. (1992)."Development and test of a theory of technological