



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

THE CYBER THREAT LANDSCAPE: CHALLENGES AND EXISTING LAWS

AUTHORED BY – AFREEN AFSHAR ALAM

Abstract

Cybercrimes are accountable for creating interruption in the functioning of computing. It caused the downfall of so many companies and individual entities all over the globe. The interruption posed by cybercrimes are rampantly spreading everywhere. This paper aims to highlight the different issues, reason of occurrence, existing laws governing them, the types of committing cybercrimes. This research paper will exhibit the application and progression of technologies that have broadened the different sorts of crimes such as theft crimes and terrorism. The main aim is to educate to individual who is unaware vis-a vis cybercrimes and highlighting its significance and technological advancement in the society and it is a fact that understanding the threat are very pertinent issues that the society is confronting. This paper will study and discuss various aspects and issues of Cybercrimes, prevention procedures and existing laws to prosecute those who are involved with such a crime.

Key words- cybercrime, hackers, cyberthreat, infringement, internet, security.

Introduction

The contemporary era is the era of computing. Technology is quickly evolving in a world driven by social networks, online transactions and cloud computing. But with the technological progression comes the problem of cybercrime, which continually changes new attack types, tools and techniques that allow attackers to infiltrate more complex or well-controlled environments. The whole globe is engulfed with the advent of computing and also along with it the different types of cybercrimes. Everywhere businesses and consumers are using computer and internet. They are creating, transmitting and storing information in the electronic form. In this modern technological age, keeping personal data safe have been very difficult. Even classified data is available due the onslaught of cybercrimes being perpetrated by the hackers all over the world as we are interconnected with internet. The use of technology has become detrimental since everyone can access or retrieve private information from the internet. People

think that technology is for the ease of our daily lives, in fact it was considered to be boon for human being. However, it turned into a bane for the people.ⁱ

There are dangers of using technology now a days. The main dangers are the threat of cybercrimes. The Problem mainly lies in the use of computers with the internet connectivity. The common users don't know the intricacies of computing juggernaut and they fall prey to the cyber hackers very easily. Numerous innocent individuals using computers effortlessly fall victim to cybercrimes around the world. Cybercrimes are such crimes that cause damage to any another individual using a computer and a network. Cybercrimes are cause by penetrating into the computing landscape resulting in the loss of privacy and confidentiality. The situation when the privacy and personal confidentiality is lost, by dint of hacking can also be termed as cybercrimes.ⁱⁱ

Other types of cybercrimes could be financial theft, cyber terrorism, espionage, infringement, spamming, cyber warfare and many other crimes that occurs across the border. Cybercrimes can happen to anyone once their information is breached by an unlawful user. According to Norton, during the last couples of years, change has swept all across the internet. The threat landscape dominates with the worms and viruses unleashed by unlawful hackers.ⁱⁱⁱ

Cybercrime are also perpetrated by the means of bogus emails sent by "phishers" aiming to steal personal information.^{iv} Cybercrimes now a days pose a serious threat. Tackling it is a difficult task for law enforcement agencies all over the world as these kinds of crime are extremely technical and full of intricacies. In addition to it, many states must update legislations, disallowing cybercrimes and fixing suitable penalties for those who commit such crimes. Of late, the billionaire businessman Warren Buffett is said to have said that "no company could be prepared for a major cyber-attack".^v

Defining the Problem

When we talk about crimes perpetrated through Computer, we do not really know the larger damaging aspects. The traditional crimes such as theft and fraud are done by physical means. But they can now be carried out in digital ways and are considered cybercrimes. The most easy way to describe a cybercrime is that: A cybercrime is a crime that is done through the use of a computer and the internet.

New World Encyclopedia defines it as “a term used broadly to describe activity in which computers or computer networks are the tool, target, or place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories.”^{vi}

Bukisa: “It is this access to the technical specifications of how the Internet and Internet technologies are implemented that allows an attacker to subvert systems, networks and the Internet for their own ends.”^{vii}

Webopedia: “Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet.”^{viii}

Director of computer crime research center defines it as “cybercrime is an illegal behavior directed by the means of electronic operations that targets the security of computer system and the data processed by them”.^{ix}

WiseGeek: “Cybercrimes are generally defined as any type of illegal activity that makes use of the Internet, a private or public network, or an in-house computer system. While many forms of cybercrime revolve around the appropriation of proprietary information for unauthorized use, other examples are focused more on an invasion of privacy. As a growing problem around the world, many countries are beginning to implement laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime.”^x

Search Security defines it as “for any illegal activity that uses a computer as its primary means of commission. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence.”^{xi}

The above mentioned statements and observations can be conceptualized as: All the crimes done through the computer with an internet network is called a cybercrime.

The cyberthreat

In the interconnected modern world, threats to cyber security can come from very unexpected

places. It's become a huge problem for all the countries. In current times, cyber exploitation and cybercrimes are becoming more serious, sophisticated and specially targeted. The 2010 report to the US Congress by the US-China Economic and Security Review Commission indicated that the number of reported incidents of malicious cyber activity targeting US Department of Defense's system have been on an increase.^{xii}

There are various short and long term impact of cyberthreats. In the short term it impacts the daily activities of the individual user. If the cybercriminals have access to the up to date data and information of the individual, they can carry out financial frauds which could lead to significant financial losses. In the long term it can lead to loss of intellectual property, which could further lead to social discontent and unrest. In very serious cases it leads to National security breaches.^{xiii}

The cyberlaw in India is a combination of law of Contract, Intellectual property, Data protection, and privacy laws. With the Computer and internet taking over each aspect of our life, there is a constant need for strong cyber laws in the country. Cyber laws in India supervise the digital circulation of information, software, information security, e-commerce, and monetary transactions. The rise of the 21st century marked the progression of cyberlaw in India with the Information Technology Act, 2000 (mostly known as the IT Act).^{xiv} It came into force on October 17, 2000. The core purpose of the Act is to provide legal recognition to electronic commerce and to facilitate the filing of electronic records with the Government. It is also called the Indian Cyber Act or the Internet Law.

The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Internet Laws in India not only validates digital signatures but also provides for how authentication of the documents, which has been accepted and generated by using the digital signatures, can be done.^{xv} It was later amended in 2008 and was notified in the official Gazette in Feb 2009. The major drive was to ensure the amplified protection of the interest of computer and internet users against computer related offences. The amendment included the change in the definition of some technical terms such as communication devices.

Types of cybercrimes

- **Cyber Terrorism** - When a threat of extortion or any other kind of harm is being subjected towards a person, organization, group or the State, it is known as the crime of Cyber Terrorism. Mostly, it includes the well-planned attack strategies on the Government and corporate computer system.

- **Identity theft** - When personal information of a person is stolen with the purpose of using their financial resources or to take a loan fraudulently in their name then such a crime is known as Identity theft.
- **Cyberbullying** - When a teenager or an adolescent harasses, defames or intimidates someone with the use of the internet, phone, chat rooms, instant messaging or any other social network medium. Then the person is said to be committing the crime of Cyberbullying. When the same crime is done by adults it is known as Cyberstalking.
- **Defamation** - Though every individual has his or her right to speech on the internet platforms as well, but if their statements cross a line and harm the reputation of any other individual or organization, then they can be charged with the offence of Defamation.
- **Hacking** - The most common cybercrime is Hacking. In this crime, the person gets access to other another person's computers and passwords to use it for their own wrongful gain or amusement.
- **Copyright** - With the colossal surge in internet users, when the data/information is distributed on all platforms, copyrighting your work aids you to restrict the use of your work. Any use of your copyrighted without permission is a punishable offence.
- **Trade Secrets** - Internet organization spends a lot of their time and money in developing software, applications and tools. They rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offence.
- **Harassment and Stalking** - Harassment and stalking are prohibited over internet platforms as well. When a person makes threatening statements about someone else online, there is violation of both civil and criminal laws. Cyber laws protect the victims and prosecute the offender against this offence.

Privacy Concerns

Threats to privacy of ordinary citizens in the wake of amplified use and upgradation of information technology has made the task more daunting for the governments and lawmakers worldwide. Cybercrime violates an individual person's privacy and the security of their data, it is particularly very dangerous in the case of hacking, malware, identity theft, financial fraud, medical fraud and certain other offences against persons that involves the revealing of personal information, messages, images, video and audio recordings without the person's consent or permission. Data is considered a commodity both online and offline by both legal and illegal

actors.^{xvi} For this very reason, data is a primary target of cybercriminals. Data also plays an essential role in the commission of many cybercrimes, mainly because it is not adequately protected and can be illegally accessed and obtained.

A notable example of data breach happened in India's national centralized government ID database (Aadhaar), which stores the biometric data (i.e., thumbprints and iris scans) and identity data of 1.2 billion Indians, and is used to verify nationals' identities for financial, government, utilities, and others services, was subjected to a database breach in 2018, resulting in the compromise of identity data, such as access names, twelve-digit identity number, phone numbers, email addresses, and postal codes, but not the biometric data.^{xvii}

The data generated in cyberspace are a fingerprint of an individual which is detailed, processed and made permanent.^{xviii} The cyberspace generates a blue print of our whole personality as we navigate through a health site, pay our bills, or even when we shop at Amazon.com. The data collected by surfing through all these domains creates a fitting profile of who we are.^{xix} When hackers and cyber vandals steal this personal information, it becomes a gross violation of our privacy.

Prevention and Procedure

In the contemporary age of technology, it seems difficult to avoid the cybercrime. However, to a certain extent it can be checked by applying several laws that are available to the people in their respective countries. Now a days, most internet browsers that provides email service, run a spam blocking features to block unwanted messages, like phishing emails and other types of fraudulent messages. Users can also install anti- virus programs like fireball and other spyware mechanism.^{xx} As a precautionary measure, people must be avoid the websites that asks for your name, mailing address, social security number, bank account, etc.

While shopping online do ensure that the website is secure and check or lookup the URL whether it begins with HTTPS or VeriSign seal. Do not confuse HTTP with HTTPS. HTTP stands for hypertext transfer protocol.^{xxi} It is a protocol that allows communication between the different systems. Usually, it is used for transferring data from a web server to a browser to view web pages. But data is not encrypted, and it can be intercepted by the third parties to gather data being passed between the two systems. This can be addressed by using a secure

version called HTTPS, where the "S" stands for secure. This involves the use of an SSL certificate, wherein "SSL" stands for secure sockets layer, which creates a secure encrypted connection between the web server and the web browser.^{xxii} Without HTTPS, any data passed is always insecure. This is particularly important for the sites where sensitive data is passed across the connection, such as e-commerce sites that accept online card payments, or login areas that require users to enter their identifications. Even Google recently announced that HTTPS is a ranking signal.^{xxiii} According to research performed by GlobalSign,^{xxiv} more than 80 percent of respondents would abandon a purchase if there was no HTTPS in use.

Conclusion

Technology is a double-edged sword and can be used for both the good or bad. As the society today is getting more and more reliant on technology, the chances of crime based electronic offenses are bound to increase.^{xxv} In the modern world the cybercrimes are a continuous problem, in spite of the fact that many countries have passed different laws and regulatory framework to check and curb it. Combating such crimes are the great problem for all countries of the world. The IT Act was the first legislation in the nation on technology, computers and ecommerce and e-communication. It is important to remember IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a crucial element of IT law. The Government and law makers should ensure that the technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes.

A general international view of cyber law indicated that numerous countries do have their national legislations and laws for combating cyber criminality, but they drastically differ from each other as a result of which, a specific cyber space activity which is considered as a criminal offence in one country may not be necessarily so in another country. Thus all the countries need to work together in order to safeguard the cyber space for all its citizens.

ⁱ Center, Finjan Malicious Code Research. "Web Security Trends Report." Securing your web (1996-2008): 1-20.

ⁱⁱ Bendovschi Andreea, "Cyber-Attacks – Trends, Patterns and Security Countermeasures", Procedia Economics and Finance 28 (2015).

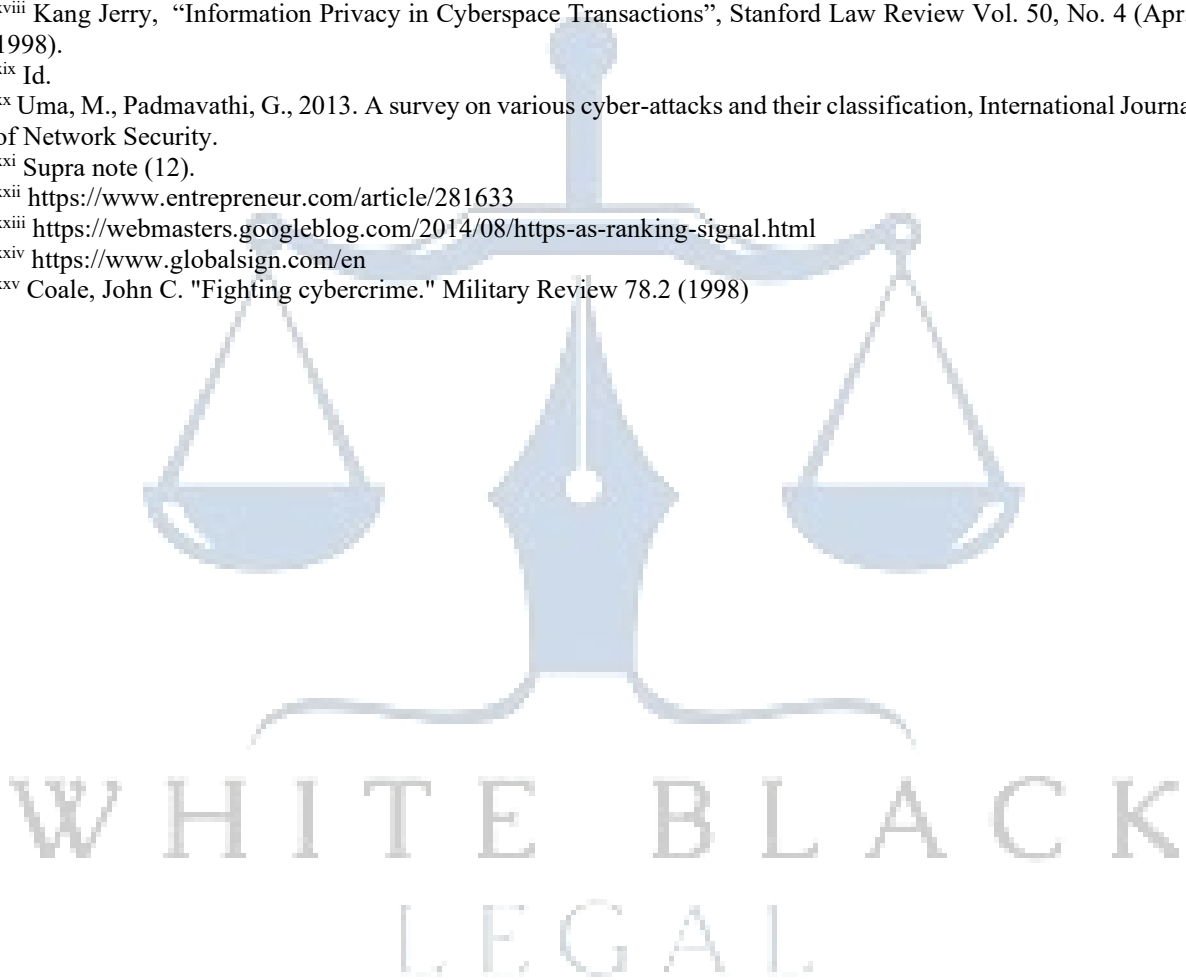
ⁱⁱⁱ Wall, David S. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." Police Practice & Research 8.2 (2007): 183-205.

^{iv} Hunton, Paul. "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model." Computer Law & Security Review 25.6 (2009): 528-535.

^v <https://www.csoonline.com/article/3210912/is-cybercrime-the-greatest-threat-to-every-company-in-the-world.html>

^{vi} <https://www.newworldencyclopedia.org/entry/cybercrime>

- vii https://www.bukisa.com/articles/206_internet-security-concepts
- viii <https://www.techopedia.com>
- ix Sharma, Vakul; Information Technology; Universal Law Publishing; 2017.
- x <http://www.cybercrime.org.za/definition>
- xi <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>
- xii Kallender Kyle Paul, "Waking Up to a New Threat: Cyber Threats and Space", JSASS Aerospace Tech. Japan Vol. 12, No. 12, 2019.
- xiii Rushinek, A, Rushinek, SF. "Using Experts for Detecting and Litigating Computer Crime". Managerial Auditing Journal. 8.7(1993).
- xiv Sharma, Vakul; Information Technology; Universal Law Publishing; 2017.
- xv Information Technology ACT, 2002 - It is the law that deals with cybercrime and electronic commerce in India.
- xvi Graham Roderick, "Cybercriminology", Oxford University Press.
- xvii <http://www.uidai.gov.in/>
- xviii Kang Jerry, "Information Privacy in Cyberspace Transactions", Stanford Law Review Vol. 50, No. 4 (Apr., 1998).
- xix Id.
- xx Uma, M., Padmavathi, G., 2013. A survey on various cyber-attacks and their classification, International Journal of Network Security.
- xxi Supra note (12).
- xxii <https://www.entrepreneur.com/article/281633>
- xxiii <https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html>
- xxiv <https://www.globalsign.com/en>
- xxv Coale, John C. "Fighting cybercrime." Military Review 78.2 (1998)



WHITE BLACK
LEGAL