INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

International Journal of Criminal Jurisprudence

(Free Publication and Open Access Journal)

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

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

Volume 1 and Issue 1 (Access Full Issue on - https://ijcj.iledu.in/category/p-volume-1-and-issue-1-of-2023/)

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

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

CYBER CRIME: START OF A WAR

Author -RIMPLEPREET KAUR, Student at SCHOOL OF LAW, CHRIST (DEEMED TO BE) UNIVERSITY, BANGALORE.

Best Citation - RIMPLEPREET KAUR, CYBER CRIME: START OF A WAR, INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE, 1 (1) of 2023, Pg. 7-14, ISBN (P) - 978-81-960702-2-9.

ABSTRACT

The Internet is frequently praised as a great resource, an entertaining environment, and a liberating experience, but for whom? There is a chance that many of us will fall prey to the increasing number of criminals who are adept at using the Internet. Cyberspace, also referred to as the Web, is a dynamic and intangible environment. This essay makes the case that cybercrime, often known as e-crime, introduces a new type of company and hi-tech criminals.

This essay examines a general overview of cybercrimes, as well as the criminals' motivations. I want to go into great detail about various cybercrimes, how they're developing, and how to tackle them.

1. INTRODUCTION

There isn't any technological crime. It is a creation of our minds. It is merely a convenient way to refer to a collection of ideas, routines, frames, and knowledge that influence how we think about issues related to how technology affects crime, criminals, and our responses to crime - and how crime, criminals, and reactions also modify technology. Technocrime includes offenses against computers, offenses committed using computers, cybercrimes, offenses involving credit cards, automated teller machines, communications equipment (such as satellite signal theft), or offenses that violate security measures (such as alarm systems and CD/DVD copy protection schemes).

2. BACKGROUND

What Exactly Is Cybercrime? Others argue that cybercrime is a new category of crime requiring a comprehensive new legal framework to address the unique nature of emerging technologies and the unique set of challenges that traditional crime does not address, such as jurisdiction, international cooperation, intent, and the difficulty of id. Some experts believe that cybercrime is nothing more than ordinary crime committed by high tech computers where computers are either a tool or target, or both.

2.2 The Perpetrators – Hackers & Crackers

2.2.1 Hackers

A "computer user who intends to obtain unauthorized access to a computer system" is usually referred to as a "hacker." A hacker is defined by IT Act 2000 section 66 as *"a person who, with the intent to cause or knowing that he is likely to cause the public to suffer unjustified loss or damage, or any person, destroys, deletes, or modifies any information stored in a computer resource, lessens its value or utility, or adversely affects its integrity using any method."*[19]

2.2.2 Crackers

A hacker with criminal intentions is called a "cracker." This word is used to separate "benign" hackers from those who intentionally harm targeted computers, according to the Jargon Dictionary. For financial gain or political gain, crackers deliberately damage computers, steal data from secure computers, and disrupt networks.

3. CHILDHOOD: THE INTERNET

[19] Section 66, IT Act, 2002

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-2-9
Published by
Institute of Legal Education
https://iledu.in

It is commonly known that the military industrial complex, as President Dwight D. Eisenhower referred to it, was a component of the creation of the Internet. The first computer network was being developed in the late 1960s, and it was being worked on by the Defense Advanced Research Projects Agency (DARPA, also known as ARPA at the time of the invention of the Internet, as in "Arpanet"). One of the pioneers of the Internet, Joseph Carl Robnett Licklider, desired to link several computers to enable information sharing (see Waldrop 2002). The research resulted in the development of the TCP/IP protocol, which allowed computer systems to "converse" with one another. Such networks proliferated quickly through US government agencies and academic institutions to become the norm. But the US military was one of computer network science's biggest advocates. The military was among the first to understand the potential of computer networking. Linking devices across space, for instance, might revolutionize command and control in military operations. These new capabilities were also utilized by some military-civilian hybrid organizations like NASA (North American Security Association).

The military's control over computer networks, however, was short-lived. Computer networks started to emerge in several nations as computer science gained popularity in colleges throughout the world, providing scientists unparalleled power to communicate. The military was forced to give up control of the networks it had created in order for academic research on computer networking to be useful.

4. ADOLESCENCE: THE WORLD WIDE WEB

With the entry of commercial Internet service providers, the internet entered its adolescence (ISPs) . ISPs obviously signaled the start of a significant democratization of the Internet, which was further accelerated by the availability of hypertext and graphically user-friendly World Wide Web standards (developed in Europe in 1989). From that moment on, the majority of computer users could join a global network and get information in an approachable style. The short-lived oligopoly of academia and the military in cyberspace came to an end as more private entities made the decision to be present online. When commercial Internet service providers appeared, cyberspace entered its adolescent phase (ISPs) . ISPs definitely heralded the beginning of a significant democratization of the Internet, along with the accessibility of hypertext and graphic-friendly World Wide Web standards (developed in Europe in 1989). From that moment on, a significant portion of computer users may join a global network and access data in an intuitive manner. The short-lived oligopoly of academia and the military in cyberspace came to an end as ISPs proliferated and an increasing number of private entities made the decision to be active online.

5. ADULTHOOD: CYBERSPACE AS STRATEGIC SPACE

The many cyberspace security doctrines that have been created have a tendency to perceive this new environment as becoming more significant from a strategic standpoint. This has given rise to novel concepts regarding the military's function in cyberspace. Military organizations are beginning to view cyberspace as a potential new theater of operations and a region where strategic dominance must be attained. Robert J. Bunker's essays, particularly one that appeared in Parameters, a prestigious journal on US strategy, persuasively prove this:

The traditional physical realm of human perception that armed forces operate in is called "humanspace." On the other hand, cyberspace represents both the electromagnetic spectrum and the realm where armed troops hide for defensive objectives.

Humanspace may not be dominant in comparison to cyberspace. The Army's ultimate objective in future conflicts will be the dominance of whole cyberspace rather than

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

just a small digital battle. From a strategic perspective, cyberspace has drastically changed positions and has emerged as a new arena for the projection of state supremacy.

6. THE NEAR FUTURE: OLD MODELS IN NEW ENVIRONMENTS

The internet is subject to quick, unforeseen change, but two recent developments in national cybersecurity can be noted: the adoption of a Cold War strategic model and the ensuing demand for greater nation-state sovereignty in cyberspace. The White House's National Strategy to Secure Cyberspace demonstrates the continuation of Cold War values and perspectives:

For the first time, our country was exposed to air and missile strikes in the 1950s and 1960s. In response, the federal government established a national system to: coordinate the defenses of our fighter aircraft during an attack; monitor our airspace with radar to detect unusual activity; analyze and warn of potential attacks; and restore our Nation through civil defense programmes after an attack. Critical national assets are now vulnerable to cyber attacks. Detecting potentially harmful activities in cyberspace, analyzing exploits and alerting prospective victims, coordinating incident responses, and repairing key services that have been compromised now require a different form of national response system for the United States. Although the text specifically mentions the Cold War era, it asks for new strategies to counter threats from Uberspace. The fact that this kind of thinking continues to shape how policies are created has clear repercussions. As can be seen from the publication's title above, it has caused the US government and its security agencies to adopt a nationalistic perspective on cyberspace. However, the space it alludes to is absolutely virtual, non-national, flexible, and dynamic even though the strategy is laid out in the same territorial, sovereign, nation-state language that predominated Cold War doctrine. The cyberspace that computers support does not share their location in any appreciable way, despite the fact that they are physically located on sovereign territory and are geolocatable. The creation of a state-centric understanding of the Internet and its threats is indicative of the US attempt to expand the notion of the nation state to uncharted and obviously poorly understood territory. The key phrase "national cyberspace" is repeated more than 40 times in the document. The text also emphasizes the distinction between "us" and "them," or between our cyberspace and their cyberspace, by "delimiting cyberspace" in social and cultural terms. It is assumed that in order to protect our cyberterritory from threats from other entities asserting their sovereignty over other cyberterritories, we must first establish a "framework for the contributions that we all can make to secure our areas of cyberspace" (or, worse, over the same one).

7. TYPES OF CYBER CRIME

For practically all cybercrimes, a computer is a necessary instrument. The arsenal of techniques available to hackers is certain to grow as more devices are made capable of communicating with the Internet.

A computer may be the object of the crime, the instrument used in the crime, or it may hold the evidence of the crime. Criminal statutes will develop from the many uses of computers.

The criminal intent is to steal information from or harm a computer, computer system, or computer network when a computer is the intended victim of the crime. Computer-targeting crimes include hacking, cracking, espionage, cyberwarfare, and malicious computer viruses. Teenagers, college students, professionals, or terrorists could be the culprits. The computer might also be the offender's tool. The cybercriminals use the computer to carry out more conventional crimes, such as printing counterfeit money on high-tech color printers.

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

Although they may be unrelated to the crime, computers are nevertheless significant since they hold the evidence of a crime. For instance, computers used by child pornographers may have child pornography that was created, owned, received, and/or distributed. Instead of depending on paper accounting records, money launderers might utilize a computer to keep information about their laundering operation.

7.1 Malicious Code – Viruses, Worms and Trojans Viruses

A computer programme that alters other computer programmes is called a virus. These adjustments make sure that the virus is replicated by the infected programme. Not all viruses harm their hosts. Typically, a virus is transferred from one computer to another using e-mail or an infected disc. However, until the application is run, a virus cannot infect another machine. When a computer user is duped into opening a file attached to an email, believing the file to be a harmless software coming from a reliable source, that is a popular way for viruses to spread. The Melissa virus, which first appeared in March 1999, is the most well-known instance of a virus. A Microsoft Word attachment that appeared to be from someone the recipient knew contained the Melissa virus. The software started a macro that sent emails to itself at the first fifty addresses it found in the Microsoft Outlook email client. Damage from the virus was estimated to have cost $80 million.

7.2 Worms

A worm is a self-replicating standalone software. In contrast to viruses, worms can spread throughout a network system without needing to be attached to a file. For instance, the loss caused by I love You Worm in 2001 was estimated to be $US 10.7 billion.

7.3 Trojan horses

An innocent-looking computer application with secret features is known as a Trojan Horse. They were downloaded to the computer's hard disc and ran concurrently with the default programme. However, a sub-program that will carry out an unapproved function is concealed in the good software. The most frequent method used to inject viruses into computer systems is through a Trojan horse. For instance, Back Orifice 2000 is an application made to be used improperly and attack a different machine.

7.4 Denial of services

A Denial of Service ("DoS") is an attack or incursion that targets computers connected to the Internet and allows one user to prevent service from being provided to other legitimate users by flooding the website with so much traffic that no other traffic can enter or exit. The hacker may just try to restrict people from accessing their own network for reasons only they know, such as retaliation, economic or political gain, or just plain nastiness, rather than actually trying to break into the system or steal data.

7.5 Cyberstalking

When someone is tracked and pursued online, it is called cyberstalking. Their privacy is violated, and everything they do is tracked. It is a sort of harassment that can interfere with the victim's life and make them feel extremely intimidated and threatened. The problem of stalking or being "following" is one that many people, particularly

women, have experienced. These issues (stalking and harassment) might occasionally take place online. This is referred to as online stalking. The internet is a reflection of reality. Therefore, it also depicts real life and genuine people who are dealing with real problems. Even though it is uncommon, cyberstalking does happen. Usually, women who are stalked by men or children who are stalked by adult predators or pedophiles engage in cyberstalking. Because he believes he cannot be touched physically in cyberspace, a cyber stalker does not need to leave his house in order to find or bother his targets. He also has no fear of physical violence. He can be a neighbor, a relative, or even on the opposite side of the planet! A stalker could be either a man or a woman.

The victim of a cyber stalker is frequently new to the internet and uninitiated in matters of netiquette and online safety. They primarily prey on women, kids, emotionally fragile or unstable people, etc. Although it's estimated that women make up over 75% of the victims, men can also become the targets of stalking.[20]

7.6 Financial crimes

This would involve deception such as fraud using credit cards, money laundering, etc. To give an example from the recent past, a website advertised Alphonso mangoes for cheap. Few customers responded to or provided the website with their credit card information since they mistrusted such a transaction. The Alphonso mangoes were actually sent to these people. The word about this website suddenly spread like wildfire. Numerous thousands of people reacted from all around the nation and placed orders for mangoes using their credit card information. To the dismay of the cardholders, the owners of the website—which was later shown to be fraudulent—flew after stealing the many credit card details and using them to make large purchases.

7.7 Cyber pornography

Pornographic websites, magazines created utilizing computers to publish and print the content, and pornographic websites on the Internet would all fall under this category (to download and transmit pornographic pictures, photos, writings etc). The Air Force Balbharati School affair is among recent cyberpornographic events in India. All of the other students at the Air Force Bal Bharti School in Delhi taunted a student for having a scarred face. He decided to avenge his tormentors since he was sick of their nasty pranks. He uploaded them to a website that he hosted for free using a free web hosting service after scanning photos of his classmates and teachers, morphing them with naked photos, and posting the results. Any action was only taken until the father of one of the classmate girls who was displayed on the website voiced his disapproval and filed a police report.

In a different incident, a Swiss couple would round up youngsters from the slums in Mumbai and force them to stand for pornographic photos. After that, they would post these images on pedophile-specific websites. The pair was detained by the Mumbai police for pornography.

7.8 Sale of illegal articles

[20] Cyber stalking India, www.indianchild.com.

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

This would involve the selling of illegal substances, firearms, and wildlife, among other things, by placing advertisements on websites, auction platforms, and message boards or just by emailing people. For instance, it's thought that numerous auction sites, especially in India, offer cocaine under the guise of "honey."

7.9 Online gambling

Online gambling is available on millions of websites, all of which are hosted on foreign servers. Many of these websites are genuinely thought to be fronts for money laundering, in fact.

7.10 Intellectual property crimes

These include the theft of computer source code, copyright violations, trademark violations, and software piracy.

7.11 Email spoofing

An email that looks to come from one source but was actually sent by another is spoofed. For instance, Pooja can be reached at pooja@asianlaws.org. Sameer, her adversary, spoofs her email and sends vulgar messages to all of her friends. Since the emails seem to have come from Pooja, her friends might be offended, and relationships might be permanently damaged.

Email spoofing can potentially inflict monetary damage. An American kid who had shorted shares of several firms won millions of dollars by disseminating untrue information about them. Share brokers and investors were notified that the companies were performing horribly via faked emails purporting to be from news organizations like Reuters.

7.12 Forgery

Sophisticated computers, printers, and scanners can be used to forge counterfeit cash notes, postage and revenue stamps, mark sheets, and other documents. Touts selling bogus transcripts and certificates can be seen outside numerous colleges all throughout India. Computers, as well as high-end scanners and printers, are used to create them. In reality, giving student gangs hundreds of rupees in exchange for these fake but genuine-looking certificates has turned into a lucrative business.

8. CYBER LAWS IN INDIA

The Information Technology Bill was approved by the Indian Parliament's two chambers in May 2000. The Information Technology Act of 2000 was created after the President gave his assent to the bill in August 2000. The IT Act of 2000 contains laws relating to cyberspace.[21]

The purpose of this Act is to set up the legal framework for online shopping in India. Additionally, the cyber regulations significantly affect India's new economy and e-businesses. Therefore, it's critical to comprehend the IT Act of 2000's many views and what it has to offer.

The Information Technology Act of 2000 also intends to establish the legal framework necessary to give all electronic records and other actions conducted via electronic means legal sanctity. According to the Act, a contract acceptance may, unless otherwise agreed, be expressed using electronic means of communication and shall have full legal force and effect. The following is a list of the Act's highlights:

Any subscriber may authenticate an electronic record by attaching his digital signature, according to Chapter-II of the Act. Furthermore,

[21] IT Act, 2000

it stipulates that anyone can use a subscriber's public key to verify an electronic record.

The Electronic Governance section of Chapter III of the Act states, among other things, that where a law requires that information or another matter be in writing, typewritten, or printed form, that requirement shall be deemed to have been satisfied if the information or other matter is: Rendered or made available in an electronic form; and Accessible so as to be usable for a subsequent reference. The legal recognition of digital signatures is likewise covered in the aforementioned chapter.

The stated Act's Chapter-IV lays out a plan for regulating certifying authorities. The Act calls for the appointment of a Controller of Certifying Authorities, who will be responsible for overseeing the actions of the Certifying Authorities, establishing the rules and guidelines that will govern them, and defining the various formats and contents of Digital Signature Certificates. The Act specifies the various requirements for the issuance of a license to issue Digital Signature Certificates and acknowledges the necessity of recognising foreign Certifying Authorities.

The idea of secure electronic records and secure digital signatures is presented in Chapter-V of the act.

The act's Chapter-VI outlines the certification authority' procedures, norms, and functions.

The Act's Chapter-VII provides information on the overall structure of the Digital Signature Certificates system. The aforementioned Act also specifies the obligations of subscribers.

The responsibilities of the subscribers are covered in Chapter VIII of the statute.

The aforementioned Act's Chapter IX discusses fines and judgements for various offenses. The punishment for damaging computers, computer systems, etc. has been set as damages, with the affected parties receiving compensation of up to Rs. 1,000,000. The Act mentions the appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of State Government as an Adjudicating Officer who shall determine whether anyone has violated any of the rules made under the said Act or the provisions of the said Act. The aforementioned adjudicating officer has been given civil court authority.

The Cyber Regulations Appellate Tribunal will be an appeals body where appeals against the decisions made by the Adjudicating Officers would be preferred, according to Chapter-X of the Act.

Chapter XI of the Act lists a number of offenses, and only police officers with the rank of Deputy Superintendent of Police or higher are allowed to look into these offenses. These offenses include hacking, disseminating obscene information in electronic form, and tampering with computer source documents.

The Act also calls for the establishment of the Cyber Regulations Advisory Committee, which will advise the government on any rules or other matters related to the aforementioned Act. In order to bring them into compliance with the terms of the IT Act, the said Act also intends to change the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934.[22]

9. CONCLUSION

When the tendencies covered in this chapter are taken into account, three conclusions may be made. The (re-)militarization of cyberspace is the first. Although the Internet was born into a military family, it quickly evolved towards civilian organization and oversight.

[22] Cyber crime a new challenge for CBI, www.rediff.com, March 12, 2003 12:27 IST

At the height of this transformation, the military virtually lost its ability to carry out serious cyberspace operations. Military organizations are attempting to reclaim their strategic capacity in cyberspace as we enter the new millennium, though. Second, the war against cybercrime is becoming more militarized. The best illustration of this is arguably the current developments in the USA. A strong indication of the direction the government is headed in in its fight against cybercrime is the shifting balance between the DoD and DHS regarding which one should be in charge of cybersecurity.

Finally, despite the fact that such actions are expressly prohibited by regulations, cybersecurity companies are becoming more and more willing to commit cybercrimes in order to achieve their goals.

It's interesting that these trends exist in China and the USA, two quite different nations. The United States presently holds "cyber hegemony" over the internet, but China is gaining ground. The changing of the guard, if and when it occurs, might not be such a significant change, though. Whatever occurs, it is very likely that the two countries will have an impact on how other states shape their future presence in cyberspace because they are such significant actors in the field. We can be confident that the militarization of the web will continue in that future, based on current patterns, and that committing cyber crimes for cybersecurity objectives will become the norm.

REFERENCES

- Benedikt, M. (ed.) (1992) Cyberspace First Steps, Cambridge, MA: MIT Press.
- Bunker, R.J. (1996) 'Advanced battlespace and cyber maneuver concepts: implications for force XXI, Parameters, 26: 108-20.
- Central Intelligence Agency (2008) Rank Order - Internet Users https:/ / www. cia.gov/library /publications / the-world-factbook/rankorder/2153rank. html).
- Fallows, J. (2005) 'Success without victory', The Atlantic Monthly, January-February: 80-90.
- Federal Trade Commission (2007) About the Bureau of Consumer Protection, (http://www.ftc.gov/bcp/about.shtm).
- Federation of American Scientists (2007) National Security Presidential Directives, (http://www.fas.org/irp/offdocs/nspd/index.html).
- Etter,B. (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.
- Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.
- Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2.
- Gengler, B. (2001), Virus Cost hit $20bn, The Australian, 11 September p.36.
- The IT Act 2000.
- Cyber stalking India, www.indianchild.com.
- Cyber crime a new challenge for CBI, www.rediff.com, March 12, 2003 12:27
- Richard Raysman & Peter Brown (1999), Viruses Worms, and other Destructive Forces N. Y. L. J.