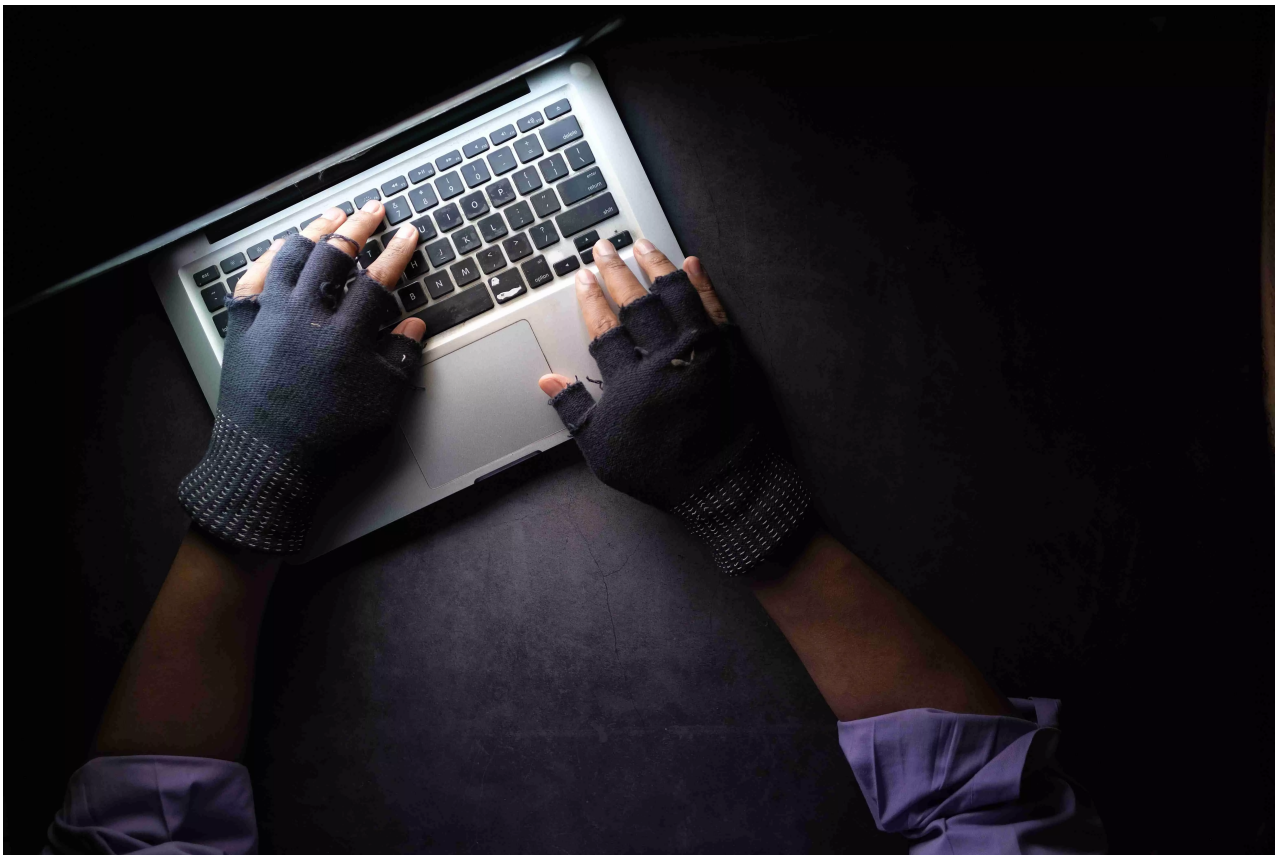
Perplexing touch of novelty

millenniumpost.in/opinion/perplexing-touch-of-novelty-527259

Nikhil Naren July 28, 2023

A descriptive, nuanced definition of cybercrime, emphasising proportionately on hardware, networks and information, is essential to deal with such crimes in the prevailing technological clime

BY Nikhil Naren28 July 2023 6:45 PM



The advancements made in the realm of digital technology today are immense. Such advancements have also impacted [and transformed] the ways in which day-to-day communication and businesses are carried out. I agree with Jonathan Clough when he writes: “crime follows opportunity, and virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes”. Hence, it becomes quintessential for the legislators to define crimes being committed using advances made in the realm of digital space. This would not only help identify and segregate the very ‘nature’ of crime but also help in policy-making and address the varying concerns around the misuse of computers.

Also Read - Epistle of harmony

As the proposed Digital India Act also discusses the need to adopt cyber laws that are fit for global standards, it does suggest amendments in the Indian Penal Code, 1860, for cybercrimes. Furthermore, as per the proposal, the Information Technology Act, 2000, has limited recognition of harms, and new forms of cybercrimes. In this article, I aim to discuss the need to define cybercrimes, and the key aspects to be considered in doing so.

The House of Commons Standing Committee On Justice and Legal Affairs, in their 1983 report, discussed the early description of cybercrimes which were referred to as either computer crime, computer-related crime, or crime by computer. Sheridan Morris emphasised that it was the advent of the internet that brought ‘cybercrime’ or ‘net’ crime into usage. What we need to understand before beginning to define cybercrime is the mix of different components involved in the commission of cybercrimes and that should not be mutually exclusive of each other. For instance, a definition of crime that emphasises on computers may not incorporate the role of networks. Today, it is immensely difficult to imagine the commission of cybercrime without a string of networks and only using a stand-alone computer. Similarly, the Oxford Dictionary, while defining cybercrime, places reliance on the Internet. Therefore, while giving a definition of cybercrime, we should make sure that our approach towards these terms is descriptive and not literal.

Also Read - Talking Shop: India’s last village

It is understood that there is no agreed definition of what constitutes a cybercrime, and there have been debates about whether such a definition could even hold meaning. Prof. Ian Walden, in his book, has pointed out the broad acceptance within literature that cybercrime involves traditional crimes committed in a new environment as well as new crimes made possible in the new environment. A similar distinction was drawn by Prof. Anne Flanagan, where she bifurcated cybercrimes into two types: ‘issues of degree’ and ‘issues of kind’. The issues of degrees are the commission of traditional crimes with the help of technological tools, and issues of kinds are the ones where the offence is fundamentally new. However, such definitions may still call for a more nuanced approach because the veracity of a traditional crime being committed by technological tools could be greater, and the issues of overlap may come up when traditional crimes are committed using new tools. For instance, consider an example of cloning a credit card and making fraudulent transactions. Such an offence could be fraud under the ‘issue of degree’ approach, but the very act of cloning a credit card could make a new offence altogether.

Also Read - Deepfake

One of the most essential purposes of the Council of Europe Convention on Cybercrime was to ensure international cooperation and harmonisation of laws for enforcement, because the very nature of cybercrime is transnational. Prof. Walden distinguishes the substantive offences of cybercrime into three categories: computer-related crime, content-related crime, and computer-integrity offences. He refers to computer-related crime as the traditional type of criminal offence that can be committed using computers as the primary tool. Hence, computer-related offences could be an extensive category. The offence of

fraud or forgery could be a good example. Content-related crime focuses on how the use of computers and communication technologies can aid in the transmission of unlawful content. The cases concerning Intellectual Property Rights infringement, or the circulation of pornographic content or sexual image-based abuse, could fall well within this category. Both categories of crimes consist of computers as the instrument for the commission of a crime, but in computer-related crime, it is not only the computer which is the instrument but also the information that is being processed for committing the criminal act. While in the case of content-related crime, the information itself is the crime and not merely a tool or an instrument. The third category, computer-integrity offences, are the offences that attack the integrity of the computer itself, such as installing malware or distributing viruses.

Also Read - Encyclopedic in character

Another important aspect to look upon while defining cybercrime is to consider the objective of information processing. Several crimes committed do not merely pertain to the computer or the network systems, but the information they store or carry. Graeme Newman and Ronald Clarke in their paper, *'Superhighway Robbery: Preventing e-Commerce Crime'*, have emphasised that information may be the perpetrator's prime, convertible, or transitional target. There are hardly any laws that protect information, but we are gradually progressing in adopting measures for protecting the technological tools that are processing such information. Therefore, we should not only focus on the end result or the commission of the act itself but also on the very nature of the information that was compromised while committing an offence.

The need to define and strictly enforce the laws around cybercrime is also based on different factors that may not only concern after a cybercrime has been committed but also instil fear in the minds of the perpetrators. Unlike more traditional forms of communication, the Internet has opened the doorways to communicate with a larger audience — cheaply and easily. Gone are the days when computers were only seen in big offices and government institutions, the commission of crime could be done by anyone using a touch of a finger by devices that are accessible to both offenders and victims today. Under the garb of anonymity, committing an offence has become a cakewalk, but the investigation has become increasingly difficult. The ways of perceiving criminal laws as being local in nature also need to change, as modern-day technologies have built a fertile land for offenders to be present and cause harm from anywhere in the world.

After all, the very purpose of any criminal law is not only to assess whether a particular act is criminal or not but is also about law enforcement and the investigation and prosecution of those who commit criminal acts, a process that gets way more challenging when offences have been committed in a digital environment.

The writer is a Chevening Scholar, Author, Assistant Professor at Jindal Global Law School and Of Counsel at Scriboard, New Delhi. Views expressed are personal

millenniumpost mpostdigital mpostopinion cybercrime Internet technology computer

@mpostdigital @mpostdigital @mpostdigital

Nikhil Naren