

Developing An Analytical Definition Of Cybercrime

Ajoy P.B. Ph.D

Advocate, High Court Of Kerala

Abstract

The ever-increasing use of internet and cyberspace for committing crimes has resulted in the emergence of a separate category of crime called cybercrime. In order to develop an analytical definition of cybercrime which distinguishes cybercrime from real-world/traditional crime, the concepts of mens rea and actus reus are used. Since, mens rea always occurs in the mind of the individual, it is always located outside cyberspace. Consequently, for a crime to be classified as cybercrime, the actus reus must occur in cyberspace. Based on this assumption, it is proposed that a crime will be considered as cybercrime only if both of the following conditions, namely: (a) any one or more of the several acts constituting actus reus occur within the cyberspace; and (b) the actus reus is completed in cyberspace, are satisfied. While developing such a definition it is also assumed that merely because evidence regarding a crime is stored in cyberspace, the crime will not be considered as cybercrime.

Keywords: Cyberspace; Cybercrime; Crime; Mens Rea; Actus Reus.

Date of Submission: 10-01-2024

Date of Acceptance: 20-01-2024

I. Introduction

The advent of internet and cyberspace has resulted in criminals using the same for committing various forms of deviant behaviour, some of which have been criminalized by the competent national legislatures. Such crimes are called cybercrimes. This article after defining crime and identifying its consistent elements (mens rea and actus reus) attempts to develop an analytical definition of cybercrime which distinguishes the same from real-world/traditional crimes.

II. Defining Crime

The word 'crime' has its origin in the Latin word '*crimen*' which means 'accusation'.¹ Crimes are those special class of deviant behaviour in society which the state through law, has prohibited and provided punishment for. Thus, if any person commits an act which has been criminalized by law, the state/its agencies will lay an accusation against that person and would put him to trial before a competent criminal court. However, if a person commits a deviant behaviour which has not been prohibited by criminal law, he cannot be charged for any offence. He would at the most face social sanctions. Thus, crime is a public wrong, i.e., a wrong against the State.²

The Criminalizing Decision

The decision by the State to criminalize a deviant conduct is a complex one. Several factors have to be taken into consideration before such a decision is made by the State. That is because such a decision has serious implications for the life and liberty of its citizens. Consequently, the said question has always vexed law-makers, academicians and researchers. Traditionally, commentators agree that if a behaviour/conduct satisfies the following two conditions, namely: (i) the behaviour/conduct is harmful to individuals or society; and (ii) the behaviour/conduct is immoral, then that behaviour/conduct can be criminalized.³

However, merely satisfying the harm principle and the immorality principle will not result in the legislature criminalizing a behaviour/conduct. This is because life in modern society is complex and several other factors have to be taken into consideration. It is in this context that the eight additional conditions suggested by

¹ T. Sowmya, *Crime: A Conceptual Understanding*, 4 INDIAN J. APPL. RES. 196–198 (2011), http://www.theglobaljournals.com/ijar/file.php?val=March_2014_1393846361_38326_58.pdf.

² ANDREW ASHWORTH & JEREMY HORDER, *PRINCIPLES OF CRIMINAL LAW* (7 ed. 2013), <http://oxfordlawtrove.com/view/10.1093/he/9780199672684.001.0001/he-9780199672684>.

³ MIKE MOLAN, DENIS LANSER & DUNCAN BLOY, *PRINCIPLES OF CRIMINAL LAW* (4th ed. 2000), <https://www.worldcat.org/title/bloy-parrys-principles-of-criminal-law-principles-of-criminal-law/oclc/437154677>.

Herbert Packer in 1968 becomes relevant. The said conditions are⁴ (i) the behaviour/conduct is considered by most people without any social dissent as immoral; (ii) the behaviour/conduct is not condoned by a significant section of the society;⁵ (iii) criminalization is not inconsistent with the goals of punishment; (iv) suppressing the behaviour through criminal sanctions will not inhibit a socially desirable conduct; (v) the behaviour can be dealt with even-handedly without any type of discrimination; (vi) controlling the behaviour through the criminal process will not expose that process to severe qualitative or quantitative strains; (vii) there are no reasonable alternatives to the method of criminal sanction for dealing with the behaviour; and (viii) the cost of enforcement is not prohibitive.⁶

These additional eight conditions help to understand the process of criminalization of behaviour much better. But it must not be forgotten that decision to criminalize a particular deviant behaviour is taken by a legislative body which is basically a political body. Consequently, each and every decision to criminalize a particular behaviour is influenced by the dominant political culture or morality prevailing in the country. Thus, taking a realistic view, it can be safely said that every decision to criminalize a behaviour is also controlled to a great extent by political opportunism and power.⁷

Definition of Crime

Simply put, crime is a human conduct or behaviour which is prohibited and its occurrence is made punishable by law. A number of famous commentators and legal luminaries have given more elaborate definitions of crime, a study of some of which will be useful for the purpose of understanding the complex concept of crime.

- (i) Glanville Williams in 1983 defined crime as a 'legal wrong that can be followed by criminal proceedings which may result in punishment'.⁸
- (ii) The 3rd edition of Halsbury's Laws of England (1980) defined crime as 'an unlawful act or default which is an offence against the public and renders the person guilty of the act or default, liable to legal punishment'.⁹
- (iii) J.W. Cecil Turner in Kenny's Outlines of Criminal Law (1962) has defined crime through the description of its three characteristic features, namely: (a) it is a harm brought about by human conduct which the sovereign power in the state desires to prevent; (b) that one among the measures of prevention selected, is the threat of punishment; and (c) that legal proceedings of a special kind are employed to decide whether the accused person did, in fact, cause the harm, and is, according to the law, to be held legally punishable for doing so.¹⁰

These three definitions point to the fact that, for a behaviour to be called crime, there must be four elements, namely: (i) the behaviour must cause some harm; (ii) the State must prohibit the behaviour; (iii) the occurrence of the behaviour must attract punishment; and (iv) the punishment must be imposed by a special proceeding.

Constituent Elements of Crime

For an act to be legally considered as a crime, common law requires that there must be two basic elements namely (i) *actus reus* (wrongful act); and (ii) *mens rea* (wrongful intention).¹¹ These two elements must be present at the same time i.e. there must be temporal coincidence.¹² This fundamental principle of criminal liability is embodied in the Latin maxim '*actus non facit reum nisi mens sit rea*', which means that an act does not make one guilty unless the mind is also legally blameworthy.¹³ The concepts of *actus reus* and *mens rea* have to be analyzed

⁴ Martha S. Yerkes, *The Limits of the Criminal Sanction*, by Herbert L. Packer, 2 LOYAL. LOS ANGELES LAW REV. 176-178 (1969), <https://digitalcommons.lmu.edu/ljr/vol2/iss1/12>.

⁵ MIKE MOLAN, DENIS LANSER & DUNCAN BLOY, PRINCIPLES OF CRIMINAL LAW (4th ed. 2000), <https://www.worldcat.org/title/bloy-parrys-principles-of-criminal-law-principles-of-criminal-law/oclc/437154677>.

⁶ *Id.*

⁷ ASHWORTH AND HORDER, *supra* note 2.

⁸ GLANVILLE WILLIAMS, TEXTBOOK OF CRIMINAL LAW (2nd ed. 1983), <https://www.worldcat.org/title/textbook-of-criminal-law/oclc/10167284>. Also see Mouaid Al Qudah, *The Moral Foundations of Criminal Liability*, 2 INTELLECT. PROP. RIGHTS 1-9 (2014), <http://www.esciencecentral.org/journals/the-moral-foundations-of-criminal-liability-ipr.1000116.php?aid=26446>.

⁹ LORD SIMONDS, HALSBURY'S LAWS OF ENGLAND (VOLUME 10) (3rd ed. 1964), <https://www.wildy.com/id/157381/halsbury-s-laws-of-england-3rd-ed-volumes-1-43-hardback-43-volumes-lexisnexis-butterworths>. For details See VIBHUTE, PSA PILLAI'S CRIMINAL LAW (12th ed. 2015), <https://lexisnexis.in/p-s-a-pillai-criminal-law>.

¹⁰ See VIBHUTE, *supra* note 9.

¹¹ CATHERINE ELLIOT & FRANCES QUINN, CRIMINAL LAW (9 ed. 2012), <https://www.pearson.com/uk/educators/higher-education-educators/program/Elliott-Criminal-Law-9th-Edition/PGM1025870.html>.

¹² *Id.*

¹³ VIBHUTE, *supra* note 9.

separately for fully understanding the concept of crime.

Actus Reus

Actus reus refers to the wrongful act that has been prohibited by law.¹⁴ It is also called as the external element of crime.¹⁵ It is the overt act or the physical result of human conduct.¹⁶ The wrongful act must be committed voluntarily.¹⁷ Experience show that the wrongful act can take three different forms, namely: (a) positive act by the accused; (b) in some circumstances, omitting to act; and (c) in rare circumstances, being involved in a state of affairs.¹⁸ Various commentators have pointed out that *actus reus* consist of three elements, namely: (a) conduct prohibited by law; (b) its attendant circumstances; and/or (c) result.¹⁹

The third element, namely, result, need not be present in all cases. In cases, where it is present, the crime is called as result crime.²⁰ For example, murder is a result crime where all the three elements are present. The firing of a gun to kill the victim is the conduct element. The attendant circumstance in murder is that the victim is a human being (shooting and killing a crow with a gun will not amount to an offence of murder). The third element is the death of the victim. Had the victim not died, the crime of murder would not have been committed.²¹ When the third element 'result' is not required to be present in a crime, the crime is called as conduct crime.²² For example, rape is a conduct crime. The mere vaginal or other statutorily defined forms of penetration of the victim by the accused is sufficient to constitute the offence of rape. The effect /impact of the *actus reus* on the victim is not an element of the offence. The attendant circumstance in the offence of rape is the non-consent on the part of the victim.²³

Mens Rea

Mens rea refers to the blameworthy mental condition of the accused that contemporarily accompanies the *actus reus*.²⁴ It is an umbrella concept which covers a wide range of mental states and conditions of the accused which form part of the definition of most offences.²⁵ *Mens rea* being a mental state, is an element of crime which is known only to the accused. So, it is very difficult to prove the existence of *mens rea* by positive direct evidence in a court of law during the trial of any offence.²⁶ Consequently, in most cases, the court must infer the presence or absence of *mens rea* from the facts and circumstances of the case. *Mens rea* can be considered as the internal element of crime.²⁷ It is also called as the fault element of crime.²⁸

The legislatures across the world have identified various shades of the mental state of the accused that prompts him/her to commit offences. The wide range of mental states of the accused can be roughly classified into two categories, namely: (a) specific intent *mens rea*; and (b) general non-specific intent *mens rea*.²⁹

The specific intent *mens rea* is a particular type of state of mind of the accused that is required to commit crimes. Such forms of *mens rea* are defined in criminal statutes using words like intention, recklessness, willfulness, knowledge, belief, reasonable cause to believe, maliciousness, fraudulent, dishonesty, etc.³⁰ The general, non-specific intent *mens rea* refers to a general state of guilty mind of the accused where there is no

¹⁴ IRYNA MARCHUK, THE FUNDAMENTAL CONCEPT OF CRIME IN INTERNATIONAL CRIMINAL LAW (1st ed. 2014), <http://link.springer.com/10.1007/978-3-642-28246-1>.

¹⁵ MOLAN, LANSER, AND BLOY, *supra* note 5.

¹⁶ VIBHUTE, *supra* note 9.

¹⁷ Gerhard O W Mueller, *On Common Law Mens Rea*, 42 MINN. LAW REV. 1043–1104 (1958), <https://scholarship.law.umn.edu/mlr/1384>.

¹⁸ MOLAN, LANSER, AND BLOY, *supra* note 5.

¹⁹ MARCHUK, *supra* note 14.

²⁰ MOLAN, LANSER, AND BLOY, *supra* note 5.

²¹ ELLIOT AND QUINN, *supra* note 11.

²² MOLAN, LANSER, AND BLOY, *supra* note 5.

²³ MARCHUK, *supra* note 14.

²⁴ Arshdeep Ghuman, *Elements of Crime*, 1 INT. J. LAW, MANAG. HUMANIT. 1–18 (2017), <https://www.ijlmh.com/wp-content/uploads/2019/03/Elements-of-Crime.pdf>.

²⁵ MOLAN, LANSER, AND BLOY, *supra* note 5.

²⁶ VIBHUTE, *supra* note 9.

²⁷ Abhirup Bangara, *Determinism and the Annihilation of Mens Rea*, 4 NIRMA UNIV. LAW J. 37–47 (2014), <http://docs.manupatra.in/newslines/articles/Upload/C721060E-D748-4B0E-B2F9-4E0CB0FA83CB.pdf>. Also see Eugene J. Chesney, *The Concept of Mens Rea in the Criminal Law*, 29 J. CRIM. LAW CRIMINOL. 627 (1939), <https://www.jstor.org/stable/1136853?origin=crossref>.

²⁸ MOLAN, LANSER, AND BLOY, *supra* note 5.

²⁹ Mueller, *supra* note 17.

³⁰ MARCHUK, *supra* note 14.

specific intent. In some crimes, only a general state of mind is sufficient. The legislature normally uses the word 'unlawfully' to describe such a state of mind in the definition of offences.³¹

III. Defining Cybercrime

Cybercrime is a term of comparative recent origin. It is a term which now attempts to replace the term 'computer crime' that was in use since the early 1970s.³² In that era, as personal computers were being invented, crimes relating to computers came into existence and the term "computer crime" was the phrase used by the press/media to describe and report those crimes. However, even before the term computer crime could attain an acceptable legal definition, internet emerged and stand-alone computers ceased to exist. When internet became very popular and people began to use it for various purposes, including interpersonal communication and interaction, the concept of cyberspace emerged. Simultaneously, some persons began to use internet as a means to commit/perpetuate crimes. Consequently, media began to use the term 'cybercrime' instead of 'computer crime'. At the same time, the media also used other terms like network crimes, high tech crimes, internet crimes, virtual crimes, etc. to define the same phenomenon.³³

For a wide variety of reasons, no single acceptable definition of cybercrime has emerged so far.³⁴ Some of the reasons are the use of large number of terms to describe the offence committed in cyberspace, the infancy of internet and its technologies, the rapid advancements in information and communication technology, emergence of newer forms of cybercrimes, etc. Only when a cybercrime is properly defined, can a proper classification scheme for same be arrived at.

Definition of Cybercrime

Developing a definition for cybercrime is not a difficult task, once the definition of crime has been identified. From a legal point of view, the definition of crime as an act prohibited by law through penal sanctions, can easily be extended to the cyberspace domain. Similarly, the analytical definition of crime that considers crime as consisting of *actus reus* and *mens rea* can also be extended to the cyberspace without much difficulty. However, just like ordinary crime, in some situations, cybercrime is a social problem as well.³⁵ It has always been difficult to define crime from a social point of view. The same difficulty exists with cybercrime as well. Consequently, the term 'cybercrime' carries with it some degree of contextual mutability.³⁶ With the background, it is useful to analyze six of the most important definitions of cybercrime suggested by different authors/institutions/commentators.

(i) During the 10th UN Congress on the Prevention of Crime and the Treatment of Offenders (2000) two definitions of cybercrime were provided in a background paper for a workshop on crimes related to the computer network.³⁷

a. Cybercrime in a narrow sense (computer crime)

It is 'any illegal behaviour directed by means of electronic operations that target the security of computer systems and data processed by them'.

b. Cybercrime in a broader sense (computer-related crime)

It is 'any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of computer system or network'.

³¹ Mueller, *supra* note 17.

³² Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VIRGINIA J. LAW TECHNOL. 1–52 (2004), https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles.

³³ David Wall, *What are Cybercrimes?*, 58 CRIM. JUSTICE MATTERS 20–21 (2004), <http://www.tandfonline.com/doi/abs/10.1080/09627250408553239>.

³⁴ See Aleš Završnik, *Cybercrime: Definitional Challenges and Criminological Particularities*, 2 MASARYK UNIV. J. LAW TECHNOL. 1–29 (2008), <https://journals.muni.cz/mujlt/article/viewFile/2506/2070>. Also see Regner Sabillon et al., *Cybercrime and Cybercriminals: A Comprehensive Study*, 4 INT. J. COMPUT. NETWORKS COMMUN. SECUR. 165–176 (2016), http://openaccess.uoc.edu/webapps/o2/bitstream/10609/78507/1/p1_4-6.pdf.

³⁵ Mary Aiken et al., *A Consideration of the Social Impact of Cybercrime: Examples from Hacking, Piracy, and Child Abuse Material Online*, 11 CONTEMP. SOC. SCI. 373–391 (2016), <https://www.tandfonline.com/doi/full/10.1080/21582041.2015.1117648>.

³⁶ STEFAN FAFINSKI, WILLIAM H. DUTTON & HELEN ZERLINA MARGETTS, *Mapping and Measuring Cybercrime*, OXFORD INTERNET INSTITUTE FORUM DISCUSSION PAPER NO 18 (2010), <https://www.foresightfordevelopment.org/sobipro/54/1163-mapping-and-measuring-cybercrime>.

³⁷ UNITED NATIONS, *Crimes Related to Computer Networks*, 10TH UNITED NATIONS CONGRESS ON THE PREVENTION AND THE TREATMENT OF OFFENDERS (2000), https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf.

The said background paper also provided for a general definition of cybercrime and defined it as ‘any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment’.³⁸

- (ii) Some others have come up with functional definitions of cybercrime for the purpose of including various types of cybercrimes within one definition. In such functional definitions, cybercrime is defined by reference to ways in which computers can be involved in the crime. In such a definition, cybercrime is ‘described as any activity (prohibited by law) in which computers or networks are a tool, a target or a place of criminal activity’.³⁹ In fact, cybercrimes are classified based on such functional definitions. Near similar functional definitions of cybercrime has been adopted by the cybersecurity strategies of many countries like New Zealand (2011), European Union (2013), Germany (2013) etc.⁴⁰
- (i) The Stanford Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (2001) prepared by Abraham D. Sofaer, Gregory D. Grove and George D. Wilson gives a very broad definition for cybercrime.⁴¹ Article 1.1 of the said draft convention defines cybercrime as ‘conduct with respect to cyber-systems’ which are classified as offence and made punishable by the convention.
- (ii) A more socially oriented definition of cybercrime is provided by Chris Hale (2002). He defines cybercrime as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.⁴²
- (iii) Sarah Gordon and Richard Ford (2006) provided a techno-legal definition of cybercrime. They define cybercrime as ‘any crime that is facilitated or committed using a computer, network or hardware device’.⁴³
- (iv) Samuel C McQuade III (2009) defines/views cybercrime as a broad term ‘covering all the ways in which computers and other types of portable electronic devices such as cell phones and PDAs (Personal Digital Assistants) capable of connecting to the internet are used to break laws and cause harm’.⁴⁴
- (v) Nir Kshetri (2009)⁴⁵ defines cybercrime in a practical manner as a ‘criminal activity in which computers or computer networks are the ‘principal’ means of committing an offence or violating laws, rules or regulations’.⁴⁶

All the above discussed definitions attempt to give a comprehensive all-encompassing definition of cybercrime. However, as can be seen, there is considerable variation in those definitions. This is understandable considering the nascent as well as diverse nature of cybercrime.

IV. An Analytical Definition of Cybercrime

There is no consensus of opinion among the various commentators regarding an all-purpose all-weather definition of cybercrime⁴⁷. The primary reason for this failure is the inability of academicians to lay down acceptable criteria to delineate the boundary lines between concepts of real-world crime and cybercrime.

From a theoretical point of view, it is possible to draw a tentative line between the said two concepts by adopting a postulate that a crime will be considered cybercrime only if any one of the constituent elements of the crime occurred in cyberspace. Susan W. Brenner has very aptly, through the following equation, presented the

³⁸ *Id.*

³⁹ INTERNATIONAL TELECOMMUNICATION UNION, UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE (2012), <https://www.itu.int/ITU-D/cyb/cybersecurity/docs/CybercrimelegislationEV6.pdf>

⁴⁰ TIM MAURER & ROBERT MORGUS, *Compilation of Existing Cybersecurity and Information Security Related Definitions*, NEW AMERICA (2014), <https://www.jstor.org/stable/resrep10487>.

⁴¹ Abraham D. Sofaer, Gregory D. Grove & George D. Wilson, *Draft International Convention to Enhance Protection from Cyber Crime and Terrorism*, in THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM 249–265 (Abraham D. Sofaer & Seymour E. Goodman eds., 1st ed. 2001), <http://web.stanford.edu/~g-wilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf>.

⁴² INTERNATIONAL TELECOMMUNICATION UNION, *supra* note 39.

⁴³ Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUT. VIROL. 13–20 (2006), <http://link.springer.com/10.1007/s11416-006-0015-z>.

⁴⁴ Samuel C. McQuade III, *Cybercrime*, in ENCYCLOPEDIA OF CYBERCRIME 43–44 (Samuel C. McQuade III ed., 1st ed. 2009), <https://www.nlb.gov.sg/biblio/13168971>.

⁴⁵ Nir Kshetri, *Positive Externality, Increasing Returns, and the Rise in Cybercrimes*, 52 COMMUN. ACM 141–144 (2009), <https://dl.acm.org/doi/10.1145/1610252.1610288>.

⁴⁶ NIR KSHETRI, THE GLOBAL CYBERCRIME INDUSTRY (2010), <http://link.springer.com/10.1007/978-3-642-11522-6>.

⁴⁷ For details see: Kirsty Phillips et al., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, 2 Forensic Sci. 379–398 (2022).

conceptual relationship between crime and cybercrime.⁴⁸

Cybercrime = Cyberspace + Crime

It is a widely accepted proposition that the basic constituent elements of crime are *mens rea* and *actus reus*.⁴⁹ It can also be reduced to the following equation

Crime = *Actus Reus* + *Mens Rea*

If the two equations are combined together, the following equation will be generated

Cybercrime = Cyberspace + (*Actus Reus* + *Mens Rea*)

Mens rea represents the mental state of the criminal. Theoretically, it is always located in the mind of the criminal which is within him. Consequently, it is not possible for *mens rea* to occur in cyberspace. Thus, for a crime to be classified as cybercrime, *actus reus* must occur in cyberspace. On most of the occasions, *actus reus* consist of several acts. It is, hence, proposed that a crime will be considered a cybercrime only if both of the following conditions, namely: (a) any one or more of the several acts constituting *actus reus* occurred within the cyberspace; and (b) the *actus reus* is completed in cyberspace, are satisfied.

This analytical approach towards understanding cybercrime can be better understood by considering the examples of online fraud/theft and online defamation. Suppose in a case of online fraud/theft, a criminal unlawfully obtains the login information of the internet enabled bank account of the victim from the physical notebook in which the victim had written the same. The said unlawful act of obtaining the login information is a constituent element of the *actus reus* of the offence. However, it occurs in the territorial space and not in the cyberspace. Suppose the criminal, thereafter, uses that stolen information to electronically login into the internet bank account of the victim and transfers some money from that account to another account. This act of transferring money, which is also a constituent element of the *actus reus* of the offence, occurs in cyberspace. Further, the said wrongful act of transferring money was completed within cyberspace. This is because the offence was complete when the money was transferred. That occurred within cyberspace. Hence, according to the proposed postulate this particular crime is a cybercrime.

Considering the example of online defamation, suppose the accused person posts a defamatory message about the victim in a social media platform like Facebook. The mere posting of the defamatory message in Facebook will not constitute the offence of defamation. The offence of defamation is completed when right thinking members of the society read that message and feel bad/ill about the victim.⁵⁰ Right thinking members of society read the defamatory post from terminal devices which are located outside cyberspace. It must also be noted that when the accused person was authoring the defamatory post, he was typing the post from a keyboard located outside cyberspace. Consequently, all the constituent elements of *actus reus* of the offence of online defamation occurred outside cyberspace. Further, the act of posting message on Facebook became a wrongful act (*actus reus*), only when the right-thinking men in society read the message and felt bad about the victim. Thus, the *actus reus* in this crime was completed outside cyberspace. Hence, this particular crime of online defamation is not a cybercrime. However, the evidence of the defamatory post is located in cyberspace. Since, it is a fundamental assumption of the proposed definition of cybercrime that merely because evidence regarding a crime is stored in cyberspace, the crime will not be considered a cybercrime.

A crime of online identity theft will qualify as a cybercrime, since the stolen identity of the victim is used to impersonate the victim in cyberspace. Consequently, in case of online identity theft, not only are some of the elements of *actus reus* located in cyberspace, but the *actus reus* is also completed in cyberspace, where the impersonation took place.

If the proposed postulates and its assumptions are accepted, a large number of offences that are hitherto classified as cybercrime will fall outside the new definition of cybercrime proposed by the postulate. This will result in the narrowing down of the definition of cybercrime and the elimination of several categories of crime which are hitherto considered as cybercrime. Such a narrow definition of cybercrime, based on the conceptual differences between real-world crime and cybercrime will be useful for defining the jurisdiction of special cybercrime courts that may be established in the future.

V. Suggested Statutory Definition

Very few statutes enacted by sovereign legislatures around the world defines cybercrime for the purpose of distinguishing it from traditional real-world crimes. Such a definition of cybercrime is crucial for deciding the

⁴⁸ SUSAN W BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE (2010), <http://choicereviews.org/review/10.5860/CHOICE.48-0685>.

⁴⁹ Angira Singhvi, *Corporate Crime and Sentencing in India : Required Amendments in Law*, 1 INT. J. CRIM. JUSTICE SCI. 1–17 (2006), <http://www.sascv.org/ijcjs/angira.pdf>.

⁵⁰ Odianonsen Francis Iyoha, Olusola Joshua Olujobi & Olabode A. Oyewunmi, *Application of the Laws of Defamation and Sedition in Nigeria's Jurisprudence: Still Relevant?*, 8 J. ADV. RES. LAW ECON. 59–68 (2017), <https://journals.aserspublishing.eu/jarle/article/view/1130>.

jurisdiction of special courts to try cases of cybercrime. This is relevant, considering the fact that many cybercrimes particularly those relating to cheating, fraud, etc. are still charged and prosecuted under the general criminal law. A definition of cybercrime is necessarily to be included in the cybercrime law of every country. The following is a suggested definition in the context of India's Information Technology Act, 2000:

Cybercrime means 'any offence defined in any statute in force in India where any transaction as a whole or one or more act in a series of acts that constitute a single transaction, which is an ingredient of the offence, occurs within one or more computer/digital resource(s) and the offence or its effect is fully complete within that computer/digital resource(s) or any other computer/digital resource(s) without any further human intervention' and includes any offence specifically defined in the Information Technology Act, 2000.

VI. Conclusion

The attempt in this article is to come up with a tentative definition of cybercrime which distinguishes it from real-world/traditional crime. It is suggested that a conceptually clear definition of cybercrime can be developed if only those crimes whose actus reus occur and are completed within cyberspace. This suggested definition of cybercrime or a more refined version of the same that may be developed in the future will go a long way in not just understanding the nature of cybercrime but also in developing a comprehensive classification scheme of cybercrime.

References

- [1]. Abhirup Bangara, Determinism And The Annihilation Of Mens Rea, 4 *Nirma Univ. Law J.* 37–47 (2014), [Http://Docs.Manupatra.In/Newsline/Articles/Upload/C721060e-D748-4b0e-B2f9-4e0cb0fa83cb.Pdf](http://docs.manupatra.in/newline/articles/upload/C721060e-D748-4b0e-B2f9-4e0cb0fa83cb.pdf).
- [2]. Abraham D. Sofaer, Gregory D. Grove & George D. Wilson, Draft International Convention To Enhance Protection From Cyber Crime And Terrorism, In *The Transnational Dimension Of Cyber Crime And Terrorism* 249–265 (Abraham D. Sofaer & Seymour E. Goodman Eds., 1st Ed. 2001), [Http://Web.Stanford.Edu/~Gwilson/Transnatl.Dimension.Cyber.Crime.2001.P.249 .Pdf](http://web.stanford.edu/~gwilson/transnatl.dimension.cyber.crime.2001.p.249.pdf).
- [3]. Aleš Završnik, Cybercrime: Definitional Challenges And Criminological Particularities, 2 *Masaryk Univ. J. Law Technol.* 1–29 (2008), [Https://Journals.Muni.Cz/Mujlt/Article/Viewfile/2506/2070](https://journals.muni.cz/mujlt/article/viewfile/2506/2070).
- [4]. Andrew Ashworth & Jeremy Horder, *Principles Of Criminal Law* (7 Ed. 2013), [Http://Oxfordlawtrove.Com/View/10.1093/He/9780199672684.001.0001/He-9780199672684](http://oxfordlawtrove.com/view/10.1093/he/9780199672684.001.0001/he-9780199672684).
- [5]. Angira Singhvi, Corporate Crime And Sentencing In India : Required Amendments In Law, 1 *Int. J. Crim. Justice Sci.* 1–17 (2006), [Http://Www.Sascv.Org/Ljcsj/Angira.Pdf](http://www.sascv.org/ljcsj/angira.pdf).
- [6]. Arshdeep Ghuman, Elements Of Crime, 1 *Int. J. Law, Manag. Humanit.* 1–18 (2017), [Https:// Www.Ijlmh.Com/Wp-Content/Uploads/2019/03/Elements-Of-Crime.Pdf](https://www.ijlmh.com/wp-content/uploads/2019/03/Elements-Of-Crime.pdf).
- [7]. Catherine Elliot & Frances Quinn, *Criminal Law* (9 Ed. 2012), [Https:// Www.Pearson.Com/Uk/Educators/Higher-Education-Educators/Program/Elliott-Criminal-Law-9th-Editi On/Pgm1025870.Html](https://www.pearson.com/uk/educators/higher-education-educators/program/elliott-criminal-law-9th-edition/pgm1025870.html).
- [8]. David Wall, What Are Cybercrimes?, 58 *Crim. Justice Matters* 20–21 (2004), [Http:// Www.Tandfonline.Com/Doi/Abs/10.1080/09627250408553239](http://www.tandfonline.com/doi/abs/10.1080/09627250408553239).
- [9]. Eugene J. Chesney, The Concept Of Mens Rea In The Criminal Law, 29 *J. Crim. Law Criminol.* 627 (1939), [Https://Www.Jstor.Org/Stable/1136853?Origin= Crossref](https://www.jstor.org/stable/1136853?origin=crossref).
- [10]. Gerhard O W Mueller, On Common Law Mens Rea, 42 *Minn. Law Rev.* 1043–1104 (1958), [Https://Scholarship.Law.Umn.Edu/Mlr/1384](https://scholarship.law.umn.edu/mlr/1384).
- [11]. Glanville Williams, *Textbook Of Criminal Law* (2nd Ed. 1983), [Https://Www.World Cat.Org/Title/Textbook-Of-Criminal-Law/Oclc/10167284](https://www.worldcat.org/title/textbook-of-criminal-law/oclc/10167284).
- [12]. International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges And Legal Response* (2012), [Https://Www.Itu.Int/Itu-D/Cyb/Cybersecurity/Docs/Cybercrimelegislation Ev6.Pdf](https://www.itu.int/itu-d/cyb/cybersecurity/docs/cybercrimelegislation-ev6.pdf)
- [13]. Iryna Marchuk, *The Fundamental Concept Of Crime In International Criminal Law* (1st Ed. 2014), [Http://Link.Springer.Com/10.1007/978-3-642-28246-1](http://link.springer.com/10.1007/978-3-642-28246-1).
- [14]. Kirsty Phillips Et Al., Conceptualizing Cybercrime: Definitions, Typologies And Taxonomies, 2 *Forensic Sci.* 379–398 (2022).
- [15]. Lord Simonds, *Halsbury's Laws Of England* (Volume 10) (3rd Ed. 1964), [Https://Www.Wildy.Com/Id/157381/Halsbury-S-Laws-Of-England-3rd-Ed-Volumes-1-43-Hardback-43-Vol Umes-Lexisnexis-Butterworths](https://www.wildy.com/id/157381/halsbury-s-laws-of-england-3rd-ed-volumes-1-43-hardback-43-vol-umes-Lexisnexis-Butterworths).
- [16]. Martha S. Yerkes, The Limits Of The Criminal Sanction, By Herbert L. Packer, 2 *Loyal. Los Angeles Law Rev.* 176–178 (1969), [Https://Digitalcommons.Lmu.Edu/Llr/Vol2/Iss1/12](https://digitalcommons.lmu.edu/llr/vol2/iss1/12).
- [17]. Mary Aiken Et Al., A Consideration Of The Social Impact Of Cybercrime: Examples From Hacking, Piracy, And Child Abuse Material Online, 11 *Contemp. Soc. Sci.* 373–391 (2016), [Https:// Www.Tandfonline.Com/Doi/Full/10.1080/21582041.2015.1117648](https://www.tandfonline.com/doi/full/10.1080/21582041.2015.1117648).
- [18]. Mike Molan, Denis Lanser & Duncan Bloy, *Principles Of Criminal Law* (4th Ed. 2000), [Https://Www.Worldcat.Org/Title/Bloy-Parrys-Principles-Of-Criminal-Law-Principles-Of-Criminal-Law/Oclc/437154677](https://www.worldcat.org/title/bloy-parrys-principles-of-criminal-law-principles-of-criminal-law/oclc/437154677).
- [19]. Mouaid Al Qudah, The Moral Foundations Of Criminal Liability, 2 *Intellect. Prop. Rights* 1–9 (2014), [Http://Www.Esciencecentral.Org/Journals/The-Moral-Foundations-Of-Criminal-Liability-Ipr.1000116.Php?Aid=26446](http://www.esciencecentral.org/journals/the-moral-foundations-of-criminal-liability-ipr.1000116.php?aid=26446).
- [20]. Nir Kshetri, Positive Externality, Increasing Returns, And The Rise In Cybercrimes, 52 *Commun. Acm* 141–144 (2009), [Https://Dl.Acm.Org/Doi/10.1145/1610252.1610288](https://dl.acm.org/doi/10.1145/1610252.1610288).
- [21]. Nir Kshetri, *The Global Cybercrime Industry* (2010), [Http://Link.Springer.Com/ 10.1007/978-3-642-11522-6](http://link.springer.com/10.1007/978-3-642-11522-6).
- [22]. Odianonsen Francis Iyoha, Olusola Joshua Olujobi & Olabode A. Oyewunmi, Application Of The Laws Of Defamation And Seditious In Nigeria's Jurisprudence: Still Relevant?, 8 *J. Adv. Res. Law Econ.* 59–68 (2017), [Https://Journals.Aserspublishing.Eu/Jarle/Article/View/1130](https://journals.aserspublishing.eu/jarle/article/view/1130).
- [23]. Regner Sabillon Et Al., Cybercrime And Cybercriminals: A Comprehensive Study, 4 *Int. J. Comput. Networks Commun. Secur.* 165–176 (2016), [Http://Openaccess.Uoc.Edu/Webapps/O2/Bitstream /10609/78507/1/P1_4-6.Pdf](http://openaccess.uoc.edu/webapps/O2/bitstream/10609/78507/1/P1_4-6.pdf).
- [24]. Samuel C. Mcquade Iii, Cybercrime, In *Encyclopedia Of Cybercrime* 43–44 (Samuel C. Mcquade Iii Ed., 1st Ed. 2009), [Https://Www.Nlb.Gov.Sg/Biblio/13168971](https://www.nlb.gov.sg/biblio/13168971).
- [25]. Sarah Gordon & Richard Ford, On The Definition And Classification Of Cybercrime, 2 *J. Comput. Virol.* 13–20 (2006),

- [Http://Link.Springer.Com/10.1007/S11416-006-0015-Z](http://link.springer.com/10.1007/S11416-006-0015-Z).
- [26]. Sowmyya T., Crime: A Conceptual Understanding, 4 Indian J. Appl. Res. 196–198 (2011), [Http://Www.Theglobaljournals.Com/ljar/File.Php?Val=March_2014_1393846361_38326_58.Pdf](http://www.theglobaljournals.com/ljar/file.php?val=March_2014_1393846361_38326_58.pdf).
- [27]. Stefan Fafinski, William H. Dutton & Helen Zerlina Margetts, Mapping And Measuring Cybercrime, Oxford Internet Institute Forum Discussion Paper No 18 (2010), [Https://Www.Foresightfordevelopment.Org/Sobipro/54/1163-Mapping-And-Measuring-Cybercrime](https://www.foresightfordevelopment.org/Sobipro/54/1163-Mapping-And-Measuring-Cybercrime).
- [28]. Susan W Brenner, Cybercrime: Criminal Threats From Cyberspace (2010), [Http://Choicereviews.Org/Review/10.5860/Choice.48-0685](http://choicereviews.org/Review/10.5860/Choice.48-0685).
- [29]. Susan W. Brenner, Cybercrime Metrics: Old Wine, New Bottles?, 9 Virginia J. Law Technol. 1–52 (2004), [Https://Www.Researchgate.Net/Publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles](https://www.researchgate.net/publication/265032559_Cybercrime_Metrics_Old_Wine_New_Bottles).
- [30]. Tim Maurer & Robert Morgus, Compilation Of Existing Cybersecurity And Information Security Related Definitions, New America (2014), [Https://Www.Jstor.Org/Stable/Resrep10487](https://www.jstor.org/stable/resrep10487).
- [31]. United Nations, Crimes Related To Computer Networks, 10th United Nations Congress On The Prevention And The Treatment Of Offenders (2000), [Https://Www.Unodc.Org/Documents/Congress/Previous_Congresses/10th_Congress_2000/017_Aconf.187.10_Crimes_Related_To_Computer_Networks.Pdf](https://www.unodc.org/documents/congress/previous_congresses/10th_congress_2000/017_aconf.187.10_crimes_related_to_computer_networks.pdf).
- [32]. Vibhute, Psa Pillai's Criminal Law (12th Ed. 2015), [Https://Lexisnexis.In/P-S-A-Pillai-Criminal-Law](https://lexisnexis.in/P-S-A-Pillai-Criminal-Law).