WHAT IS CYBERCRIME? A CRIMINOLOGY PERSPECTIVE*

Dawei Song[1]

It is a commonplace idea that cybercrime has been a growing problem in the whole world. Cybercrime is perplexing and seriously harmful. It seems that every country in the world has formulated some regulations and rules dealing with cybercrimes. At the international level, there are many treaties or conventions on cybercrimes. When referring to the term cybercrime, because of the different legislation, cultural backgrounds, and social choices, the connotation and denotation of cybercrime are dramatically different in different countries. For the discussion of cybercrime from a macroscopic and global angle, it is important to unify the universe of discourse of cybercrime and figure out the concept and nature thereof. This article will conclude with a concept of cybercrime developed using criminological methods, based on the analysis of two kinds of existing definitions.

1. The Reasons for Criminology Perspective

The definition of cybercrime should be divided into two parts to be defined separately. One is "cyber," and the other is "crime." The meaning of cyber should be more apparent than that of crime. So, we should talk about the meaning of crime first. In law, crime is the contravention of a norm or set of norms which is backed up by the deterrence of the criminal sanctions (Case – Manlow – Johnson 2017). A crime must be an act or omission. Then arises the question: what kind of action could be criminalized? What if a person expresses intense criticism of the government in his blog, should this act be criminalized?

There is a classification which distinguishes behaviors into normal behaviors and deviance (Durkheim 1966). Deviance is any violation of social norms, values, and expectations. It does not have a fixed meaning; it morphs in different environments and contexts. For example, homosexuality was considered deviance or even a crime before the 1960s in England and Wales. However, it is not seen as deviance or crime anymore, and gay couples can get married in England legally (Case – Manlow – Johnson 2017, 57). The extension of deviance has shown a difference. On this basis, the extension of the crime is also different, or arguably more complicated. We can ascertain that all crimes are deviance, but not all forms of deviance are crimes in the eyes of the law. It is a necessary but not sufficient requirement. Some behaviors are seen as deviance in some countries, but not in other countries. In the same vein, some forms of deviance are considered crimes in some countries, but not in other countries.

Returning to the concept of cybercrime, if we want to determine the meaning of the element of "crime", we should consider two dimensions: the first is what kind of cyber-behavior is deviance and the second is what kind of cyber-deviance is a crime?

* DOI 10.21868/PGnG.2018.2.2.
[1]*Dawei Song*, PhD student, Géza Marton Doctoral School of Legal Studies, University of Debrecen, Faculty of Law

To answer the first question, we should bear in mind that it is often a localized concept. It depends on the different culture, historical customs and fundamental moral rules of a specific area. Different societies have different values and practices, and for the members of a certain society, keeping these norms is a way of identifying themselves as belonging to that society, so it is challenging to change their mindset. For instance, a man who is over 20 years old watching porn online may be normal in Europe as long as he does not watch child pornography or does so at a public place (or both), but it is deviant in China because all obscene material is seen as illegal and immoral.

To answer the second question, we should apply the "Harm Principle," i.e. that crime is deviance that jeopardizes others' interests, such as physical integrity, privacy, autonomy, and freedom from humiliation or degrading treatment (Von Hirsch – Jareborg 1991). Despite the detailed content of the harm principle, the requirement that crime must be a harmful act is the same around the world. However, in different countries, the definition of a harmful act is not identical, so some acts may simply be considered deviance in some countries but a crime in others. For instance, three persons have sex in a hotel. Although the place they had sex in is closed, all three persons have consented to the act, and none of them engage in prostitution, it is considered a crime in China, and their acts are treated as harmful.

According to the two answers given above, we can conclude that, if we want to have a comprehensive understanding of the element of "crime" in the word cybercrime, it is a difficult task to assemble and summarize all the related charges in different conventions or treaties or countries' legislations due to the non-identical societal backgrounds. So, if we wish to keep researching the concept of cybercrime, we should abandon the detailed regulations and pave a road by using the harm principle commonly utilized in criminology. By utilizing the harm principle, we could find the greatest common divisor, which is the common characteristic, among all the different treaties or legislations of cybercrime in the world from a macroscopic and global angle.

2. Two Kinds of Definitions: Computer Crime and Cybercrime

Looking up the word "cyber" in the dictionary, we can find it defined as something "of, relating to, or involving computers or computer networks" (Macmillan Dictionary 2010). Cybercrime, when it first came into attention of legislators, was not known by this name. It took a long time for cybercrime to get its current name, and before this – or even nowadays – some scholars call it computer crime (Licalzi, C. 2017) or Internet crime (Curran 2007). Indeed, the word "cyber" first saw use in 1992 (Macmillan Dictionary 2010). This article will only discuss two definitions: computer crime and cybercrime.

It is essential to keep in mind that the classifications of "computer crime," "Internet crime" or "cybercrime" are based on the classifying approach of criminology. The terms "computer crime," "Internet crime" or "cybercrime" are not actual charges but sets of many related ones.

The first official national definition of cybercrime might be the one appearing in Senate Bill S.240, the Federal Computer System Protection Act of 1979, of the United States. In this act, cybercrimes are called "computer crimes." Though this act did not pass in the end, it tried to give a somewhat accurate concept of computer crimes. In this bill the computer crimes are considered to be:

a) any use of a computer for a fraudulent purpose,

b) intentional, unauthorized use, access or alterations of computer programs or data.

Some scholars fiercely opposed this bill and argued it had no meaning to be promulgated because the existing law could address all the problems referred to in the articles (Taber 1979). However, in 1984 the United States passed the Computer Fraud and Abuse Act (CFAA)[2], and the content of CFAA showed similarities with the previous bill.

Then, by the technological development brought on by computer science and the improvement of the Internet, the term computer crime could no longer cover all the circumstances of new crimes. For example, consider the emergence of the mobile phone. In China, more and more people use the smartphone especially to access the Internet instead of the PC (CNNIC 2018). So, we arrive to the "cybercrime" era.

However, the word cybercrime is too broad to describe the different behaviors accurately. It seems that all incidents happening in the cyberspace or having a minor connection with computers or the Internet can get classified under the umbrella of cybercrime. There are two methods to define what is understood by the term cybercrime:

One is the method of particularization. Take the Budapest Convention on Cybercrime as an example. The Budapest Convention on Cybercrime was opened for signature in 2001 and entered into force in 2004. In Chapter 1 of the Convention, titled "Terms of Use", Article 1, titled "Definitions", did not give any clear statement or description of cybercrime but listed nine kinds of specific behaviors which should be treated as crimes in the subsequent nine articles.[3]

The other approach is the method of generalization. The majority of scholars tend to use this method to summarize the contents of the term cybercrime. A representative view of cybercrime is that the cybercrime is (1) the crime which has the computer and computer network as the target, for example, hacking; (2) the conventional crime which occurs in the virtual reality world, for instance, cyber-fraud; (3) the crime where the computer or Internet plays an incidental role in committing them (Clough 2011).

The advantage of particularization is that it can be easy to understand the specific behaviors which are more harmful to be a crime. While it is definitely more comfortable to use in judicial practice, the disadvantage is that it cannot contain the entire, rapidly growing list of criminal acts, e.g. cyber-terrorism was not included in the Convention on Cybercrime and necessitated amendments to fix the issue. Because of the time cost of legislation or concluding a treaty, even if the newest crimes are regulated in the new law or treaty, even newer forms of crimes appear before its conclusion. The preventive function of criminal law would not be produced effectively.

Reflecting on the generalization method, sometimes, the too broad definition of the cybercrime might hinder people in understanding the concept of cybercrime very well, especially some non-professionals; and, the risk of abuse of discretion should be a flaw when applying this definition. So, with regards to this issue, the generalization method requires some revising.

[2] See: Computer fraud and abuse act, 18 U.S.C. 1029 (1984).

[3] Convention on cybercrime: Budapest, 23. XI. 2001, (2002). The 9 behaviors which should be treated as crimes are: Illegal access; Illegal interception; Data interference; System interference; Misuse of devices; Computer-related forgery; Computer-related fraud; Offences related to child pornography; Offences related to infringements of copyright and related rights.

However, by contrast, the generalization is better than the particularization. It appears to have a significant advantage in academic research. Scholars, politicians, policy-makers, and practitioners can use their discretion to make sense of the term cybercrime. It gives more discretion to the institutions of society, such as the legislative and the judicial system. It is also able to reply to new crimes rapidly by providing interpretations.

3. Concluding remarks

In criminology, to define a crime is necessary for explaining it, and the explanation should form the basis of the response to the crime. An appropriate definition of crime would be convenient to easily explain to the public what is understood by crime. The pinpointed explanation underlies the rationale of responses to crimes and vice versa. The definition of, explanation of, and responses to crime are reciprocal, mutually-dependent and mutually-reinforcing (Case – Manlow – Johnson 2017, 32).

According to the discussion of both advantages and disadvantages of the two methods for summarizing the concept of cybercrime, I prefer the generalization method. Meanwhile, for the sake of narrowing down the broad boundary of the general concept of cybercrime and to make it more suitable for building the rationale of effective and efficient responses to crime, I would like to redefine cybercrime on the basis of the general classification with the consideration of the relationship between crime and deviance, and the characteristics of computer technologies and the Internet.

So, in my opinion, cybercrime is a harmful deviant behavior that is taken for procuring improper interests which are forbidden by law or common social values, by use of the features of data and the online transportation thereof, which abuses the advanced technologies and the information asymmetries that stem from positional advantages.

List of References:

- Case, S., Manlow, D., & Johnson, P. (2017). Criminology. New York, NY: Oxford University Press
- Clough, J. (2011). Cybercrime. *Commonwealth Law Bulletin*, 37(4): 671-680.
- CNNIC (2018). The 42nd china statistical report on internet development. China Internet Network Information Center. http://www.cnnic.com.cn/hlwfzyj/hlwxzbg/hlwtjbg/201808/P020180820630889299840.pdf [accessed October 3, 2018]
- Computer fraud and abuse act, 18U.S.C. 1029 (1984).
- Convention on cybercrime: Budapest, 23. XI. 2001, (2002).
- Curran, J. F. (2007). Internet crime victimization: Sentencing. *Mississippi Law Journal* 76(3): 909-922.
- Durkheim, É. (1966). *The rules of sociological method.* New York: Free Press.
- Licalzi, C. (2017). Computer crime. *American Criminal Law Review* 54(4): 1025-1072.
- Macmillan Dictionary (2010). Retrieved from https://www.merriam-webster.com/ [accessed October 3, 2018]

- Taber, J. K. (1979). On computer crime. *Computer Law Journal* 1: 517-544.
- Von Hirsch, A. & Jareborg, N. (1991). Gauging criminal harm: A living-standard analysis. *Oxford Journal of Legal Studies*, 11(1): 1.