Modus Operandi in Cybercrime

1

Bettina Pospisil
https://orcid.org/0000-0002-8854-9764
Danube University Krems, Austria

Edith Huber
https://orcid.org/0000-0003-3373-0870
Danube University Krems, Austria

Gerald Quirchmayr
University of Vienna, Austria

Walter Seboeck
Danube University Krems, Austria

INTRODUCTION

Every person has their own way of doing something, from simple-to-interpret routinized actions to significant acts, which are difficult to observe. Even though we are not aware of it most of the time, we often recognize our counterparts opposite because of their *modus operandi* before we can see their face. This "particular way or method of doing something" (English Oxford Living Dictionaries, n.d.) is called the *modus operandi*. Behind this term lies a vast and heterogeneous field of definitions and interpretations. Especially in the context of crime studies, the *modus operandi* represents an important concept to learn about offenders. This concept is used to raise the existing knowledge about the defendant and his/her approach to criminal activity, in order to predict, prevent and deter future crimes. While analysing the *modus operandi* is already well-established practice used to detect offenders in traditional forms of crime, it is not yet commonly used in cybercrime. The most important reason is the lack of insight into the approach of a cybercriminal. His/her playground is cyberspace, where it is difficult to gather all the details needed to construct a complete picture of a *modus operandi*. This difficulty arises because not all data in cyberspace is easily accessible, and even criminals with basic technical knowledge can hide themselves and camouflage their activities without much of a problem. Hence, this lack of insight leads to a lack of knowledge about the activities perpetrated before the victim recognizes the damage.

In this article the concept of *modus operandi* will be discussed within the context of the phenomenon of cybercrime. In the first chapter, the terms cybercrime and *modus operandi* will be defined. In the second chapter, the article will explore the nature of cybercrime as a topic situated at the interface of different disciplines. In particular, the challenges and topics of the three most important disciplines will be outlined. When talking about the idea of *modus operandi* in the context of cybercrime, technical aspects that represent the framework conditions warrant further consideration. The third chapter of the article will examine these in two steps. First, the technical aspects of the *modus operandi* concept in cybercrime will be set down. Next, different classifications of potential criminals will be discussed

DOI: 10.4018/978-1-5225-9715-5.ch013

and one classification type selected as an example of how the *modus operandi* in cybercrime could be analysed. In the closing chapter, the authors make recommendations concerning the need for greater awareness, knowledge, prosecution, and cooperation, and argue for the necessity of future research.

One of the objectives of this article is (1) to illustrate that valid definitions of cybercrime and of the *modus operandi* have to take the interdisciplinary nature of both concepts into account. The second objective is (2) to highlight the issues and challenges the various disciplines have to face when talking about cybercrime. This article will continue (3) with an explanation of what a *modus operandi* in cybercrime could look like in practice. This will be achieved through the use of different studies that developed a classification of the motivation of cybercriminals, with a focus being on a recent study of defendants in Austria. Last but not least, the aim of this article is (4) to present recommendations and a conclusion pertaining to the key issues to be kept in mind when talking about the *modus operandi* in cybercrime.

BACKGROUND

Before addressing the topic in more detail, the basic terms of this article, namely "cybercrime" and "*modus operandi*" will be defined as follows.

Defining Cybercrime

Researchers from all disciplines commonly understand cybercrime as a sort of crime that involves, uses or is related to the computer or to information technology (Furnell, 2003; Varghese, 2016; Wilson, 2008). "Cybercrime differs from crime primarily in the way it is committed: Criminals use guns, whereas cybercriminals use computer technology." (Brenner, 2010, p. 10)

The most basic distinction in defining cybercrime can be made by splitting it in two categories, "computer-assisted cybercrime" and "computer-focused cybercrime" (Furnell, 2001). This distinction has be made by various researchers from different disciplines. While Furnell (2001) characterizes the terms as already mentioned, Gordon and Ford (2006) critically discuss "Type I" and "Type II" cybercrime. McGuire and Dowling (2013) call their categories "cyber-dependent crime" and "cyber-enabled crime". The United Nations (2000) makes the distinction between "cybercrime in a narrower sense" and "cybercrime in a broader sense", while also conveying the same core meaning as the terms used before.

1. Computer-focused cybercrime, Type I cybercrime, cyber-dependent crime, cybercrime in a narrower sense:

This type of cybercrime relates to offences that can only be committed online. These offences do not exist offline in any way; they occur within the confines of cyberspace. This type of cybercrime includes the violation of confidentiality, integrity and availability of networks, as well as of devices, data and services connected within these networks. Examples for this type of cybercrime range from the spreading of malware to hacking, and attacks on network infrastructure or websites.

2. Computer-assisted cybercrime, Type II cybercrime, cyber-enabled crime, cybercrime in a broader sense: