Chapter 25

A Routine Activity Theory-Based Framework for Combating Cybercrime

Dillon Glasser
The Richard Stockton College of New Jersey, USA

Aakash Taneja
The Richard Stockton College of New Jersey, USA

ABSTRACT

Since the government began tackling the problems of cybercrime, many laws have been enacted. A lack of a comprehensive definition and taxonomy of cybercrime makes it difficult to accurately identify report and monitor cybercrime trends. There is not just a lack of international agreement on what cybercrime is; there are different laws in every state within the United States, reflecting the inconsistency of dealing with cybercrime. There is also concern that many times lawyers and information technology professions are unable to understand each other well. The deficiency of cyber laws is an obvious problem and development of effective laws is emerging as an important issue to deal with cybercrime. This research uses the routine activity theory to develop a unified framework by including the motivation of the offender to use a computer as a tool/target, suitability of the target, and the presence (or absence) of guardian. It could help states that want to update their existing laws and cover areas that were previously uncovered.

INTRODUCTION

Originally the Internet was considered the Wild West, but legislators and law enforcement have made significant strides in tackling cybercrime. However, cybercrime has changed in recent years due to the growth of new phenomena in internet environments, such as peer to peer networks, social networks, organized cybercrime groups, and powerful new “smart” viruses (Berg, 2007). Cybercrime has “historically referred to crimes happening specifically over networks, especially the Internet, but that term has gradually become a general synonym for computer crime.” (Alkaabi, 2011). Cybercrime is different from other crimes because of the way it changes rapidly along with the technology that it uses or abuses.

Cybercriminals today are becoming more sophisticated and organized. They are now using botnets to accomplish crimes such as spamming and denial of service attacks. Technology and cybercrime are moving targets and there should
be concern that the slow nature of our government may not be keeping pace. It is therefore not a surprise that old laws are being applied to new age crime. For example, Indiana has no laws pertaining to fraud or theft using a computer. Unfortunately, Indiana is not the only state that is lacking in cyber laws. It has been hard in the past to come to an agreement on what exactly constitutes cybercrime. As lack of a comprehensive definition and taxonomy of cybercrime makes it difficult to accurately identify report and monitor cybercrime trends. The deficiency of cyber laws is an obvious problem and development of effective laws is emerging as an important issue to deal with and combat cybercrime.

According to the routine activity theory, three specific criteria must exist for a crime to take place. There must be a motivated offender, a suitable target, and the absence of a capable guardian. The objective of this research is to use routine activity theory by including the suitability of target and motivation behind cybercrime for creating a unified framework which can be used to develop capable guardians (appropriate laws and policies) to effectively coordinate cybercrime regulation and legislation.

The rest of the paper is organized as follows. Section 2 of the paper describes the background in the areas of cybercrime, federal and state laws related to cybercrime. Section 3 discusses the routine activity theory followed by the unified framework in section 4. Lastly, we present our conclusions and the work ahead.

**BACKGROUND**

**Cybercrime**

Cybercrime is a very broad term that has “historically referred to crimes happening specifically over networks, especially the Internet, but that term has gradually become a general synonym for computer crime. Cybercrime is different from other crimes because of the way it changes rapidly along with the technology that it uses or abuses. There is a lack of international agreement on what cybercrime is, which the UN has stated as one of the reasons for the lack of international cooperation on tackling cybercrime (Alkaabi, 2011). That is not to say that there is a complete lack of cooperation. When it comes to spam, there has been a significant amount of international cooperation on creating laws to combat it. The Tripartite Memorandum of Understanding on Spam Enforcement cooperation is one example of this. This is a law internationally agreed upon between the United States, Australia, Canada, and the European Union for the purposes of fighting spam (Kigerl, 2012). However, many other areas of cybercrime legislation do not have the same level of cooperation that spam receives, including such things as intellectual property, identity theft, and fraud. This lack of cooperation is a serious problem when considering the international nature of the internet. It is quickly becoming our most important tool, responsible for many different aspects of our everyday life. Technology is always expanding into more parts of our lives.

Not just internationally, there are different laws in every state within the US, reflecting the inconsistency of dealing with cybercrime. For example, New Jersey, the United States 7th largest state by GDP, does not have laws for Content Violations, Unauthorized alteration of data or software for personal or organization gain, or improper use of communications; Alaska, 46th, lacks laws pertaining to interruption of Services such as the infamous Denial of Service attacks that plague the internet. “By far the greatest number of state cybercrime statutes are concerned with computer intrusions and damage caused by intrusions” (Brenner, 2001). This is an epidemic of cybercrime that cannot simply be solved with an expansion of previous non-cybercrime related laws. Given the nature of the cybercrime, these gaps and legal contradictions can cause many issues.