Chapter 3
Towards a Theory for Explaining Socially-Engineered Cyber Deception and Theft

Paul Danquah
Heritage Christian College, Ghana

Olumide Babatope Longe
American University of Nigeria, Nigeria

Jojo Desmond Lartey
Heritage Christian College, Ghana

Peter Ebo Tobbin
Center for IT Professional Development, Ghana

ABSTRACT

Socially engineered cyber deception and theft seems to have gained prominence in cybercrime. Given the contextual background of inadequate theoretical explanations of socially engineered cyber deception and theft cybercrime, there is the need for theory to better explain and possibly predict activities involved in socially engineered cyber deception and theft. This chapter proposes a theory of socially engineered cyber deception and theft (SECT), with routine activity theory, crime displacement theory, the space transition theory, and empirical review as its foundation. It iteratively combines deductive and inductive approaches to infer the occurrence of socially engineered cyber deception and theft. While the deductive approach serves the deduction leading to the inference, the inductive approach extracts and suggests empirical evidence for a deterministic prediction of the crime occurrence. It is recommended that the theory is further validated to test its applicability.

DOI: 10.4018/978-1-7998-3149-5.ch003

INTRODUCTION

Cybercrime is a generic terminology used for all sorts of crimes committed with computers (Katyal, 2001). Srinivasan (2008) defines cybercrime as criminal activities that are executed by the use of communication networks such as the Internet, satellite, mobile networks, telephone and wireless networks. Service interruption, virus transmission, and denial-of-service attack are a number of ways in which cyber criminals can invade systems and cause damage. Yar (2005) categorizes cybercrime into four different types, namely *cyber deception and theft*, *Cyber trespass*, *cyber violence and cyber pornography*. Cyber-trespass occurs when a perpetrator intentionally intrudes or enter computer resource, asset or property belonging to other people, without their expressed approved authorization or authentication, in order to gain right of access and privileges available on the computer with a motive to harm or steal (Reynolds, 2015; Yar, 2005). Typical examples are website defacement, spread of viruses and hacking. Cyber-deception and Theft also involves the use of computer technology to deceive and steal, usually electronically, and typical examples are theft of assets or money, such as intellectual property (IP) breach or violation, IP piracy and credit card fraud (Reynolds, 2015). Cyber-pornography refers to activities that breach laws on obscenity and decency. An example is child pornography. Cyber violence on the other hand involves the use of the Internet and related technologies to cause psychological harm or incites physical injury against others, thereby breaking laws relating to the protection of the individual. Typical instances of cyber violence are hated-speech, denial of service attack and cyber mistreatment and bullying (Reynolds, 2015).

Ngo and Jaishankar (2017) further highlighted Wall (2005, revised in 2010, p. 82) which addressed cybercrime from four perspectives. These include crime against machines, crimes using machines, and crimes within computer/system, content-related crimes, which may encourage viciousness and further stimulate relatively traditional crimes like stalking and personal pestering.

These different crimes, arguably, bear striking resemblances that are characteristically different from other known crimes. Among the unique characteristics of such cybercrimes include transnational, through the Internet, whereby the attack originates from a different country to another than that of the victims with clearly different jurisdiction, laws and perhaps culture (Brenner 2004; Reynolds, 2015). “Such modus operendi from foreign lands makes it difficult to detect and consequently retaliate them” (Reynolds, 2015). Also, these crimes do not require proximity, and neither are they limited by physical constraints; it has the potential to scale at a high velocity with multiple victimization, while the perpetuator may possibly maintain perfect anonymity. It was identified by Assarut, Bunaramrueang and Kowpatanakit (2019) that freedom and anonymity are key factors in the behavioural intention to commit cybercrime. Al-Suwaidi, Haitham and Jabeen (2018) argued the need for collaboration of space tradition theory and criminal opportunity theory to explain cybercrime since they incorporate not only cyber space but also population characteristics in different countries.

There are several applicable cybercrime related theories, notable ones are the Routine Activity Theory (RAT) by Cohen and Felson (1979), Crime Displacement Theory (CDT) by Cox, Johnson & Richards (2009), and the Space Transition Theory (STT) by Jaishankar (2008). Much as these theories are applicable to cybercrime They all generalize their applicability for the purpose of either explaining the phenomena or predicting it. The STT focuses on cybercrime but again generally postulates as applicable to all the mentioned types of cybercrime. Socially engineered cyber deception and theft (SECT) is a subset of the cyber deception and theft category of cybercrime, a form of cybercrime that involves a perpetrator using computer system to leverage on gained-trust from a victim and subsequently fraudulently exploiting the