Chapter 35
Towards Black Box Forensic Cybercrime Investigation Model (BBFCIM): Beyond the Rule of Thumb

Oyewole Simon Oginni
Pan African University, Cameroon

ABSTRACT

Although internet has emerged to bridge digital divides and improve how things are done across diverse spheres of life, its explosion has also brought unexpected threats, risks and loss of valuables over a decade. Consequently, there seems to have been plethora of cybercrime investigation models but the proliferation of these models has not substantially reduced the frequency of cyber attacks globally. Given that the recent development in cyberspace seems to follow same trends of how survivable Black Box (Flight Data Recorder) emerged, this chapter proposes a Black Box Forensic Cybercrime Investigation Model (BBFCIM). BBFCIM sets a new agenda for cybercrime investigation process by focusing on survivability and reliability of existing and would-be models rather than evolving as a distinct model of itself. It adopts soft innovative skills in the development of Black Box components to shape proactive cybercrime investigation process through sequential tests on each networking layers.

INTRODUCTION

The dawn of the 21st Century met with the advent of globalization and internet technology. During the past decade, the explosion of technology innovation has produced mixed outcomes: expanding access to global markets, narrowing digital divides, and an increasing complex series of crimes – especially cyberspace crimes. Technology innovation has improved access to market information, products, and services. It has also lent credence to better consultative public policy processes, advocacy, activism, and geographical interconnectedness. Simultaneously, technology innovation has expanded the scope and sophistication of crimes to cyberspace. At first, cybercrime was mainly perpetrated by individuals

DOI: 10.4018/978-1-5225-9273-0.ch035

against other individuals. However, recently cybercrime has assumed a greater dimension than ever as the number of cybercrime victims has increased from individuals to small businesses, multinational corporations (MCNs), international organizations, and states (Alperovitch, 2011).

The recent cyberwarfare between the United States (U.S.) and China over economic cyberespionage presents a unique dimension of cybercrimes for and/or against the state. Several times the U.S. has accused China of economic cyberespionage and, in return, China has accused the U.S. of the same crime (Eunjung & Nakashima 2010; Perlroth, 2013). In the concluding part of a piece entitled, *China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain*, Cate maintains the U.S. only conducts cyberoperations against government for military and other commercial information, while the Chinese are hacking businesses for trade secrets and commercial information (Lindsya, Ming, & Reveron, 2015). In September, 2015, the U.S. and China resorted to diplomatic agreement in order to address the reoccurring cyberwarfare (Austin, 2015). Nevertheless, the use of diplomacy to tackle cybersecurity espionage still depends on if the two countries will continue to operate according to the agreed rules.

One would reason that since the U.S. has the strongest military strength in the world, the country would have opted to use such capability to attack cyberespionage. Unfortunately, the control of cyberspace is not confined to militarization or the use of security operatives such as the Central Intelligence Agency (CIA). Although internet technology emerged from the U.S., the uninterrupted knowledge expansion in the applications of internet technology globally has limited the capabilities of the U.S. laying claim to sole ownership and control of cyberspace. The preamble of the National Commission for the Review of the R&D Programs of the United States Intelligence Community (2013, p. 3) reads as follows:

The global spread of scientific and technical knowledge challenges U.S. national security. It threatens to erode essential capabilities of the U.S. Intelligence Community (IC) and the strength of the U.S. R&D base.

Moreover, considering the elaborative policy of the European Union (EU) on cybercrime, it is expected normally that the supranational institution has adequate security guard against cyberespionage. However, on the contrary, the EU has once been victim of a cyberattack. A secret malware was discovered on the EU computer systems in 2014 designed to disguise itself as authorized Microsoft software and steal data from the infected systems. Marquis-Boire, Guarneri, and Gallagher (2014) reported the malware to the U.S. National Security Agency (NSA) and the British Intelligence surveillance. This demonstrates that cybercrime has moved beyond targeting individuals to state and regional actors.

Besides the history of cyberespionage against the state, there is also evidence of syndicates jointly launching cyberattacks against MNCs. The great bank robbery, referred to as the Carbanak Attack, is one of the world's largest crimes committed by cybercriminals against multinational banks (Kaspersky, 2015). A syndicate of cybercriminals employed Carbanak to infiltrate more than more than 100 banks, e-payment systems, and financial institutions across 30 countries and stole approximately US$1 billion between 2013 and 2015. Carbanak is a remote backdoor designed for data infiltration, espionage, and remote access to infected machines. The Kaspersky Lab Report (2015) provides detail accounts on the methods used by the syndicate:

…the initial infections were achieved using spear phishing emails that appeared to be legitimate banking communications, … once the attackers successfully compromise the victim´s network, the primary internal destinations are money processing services, Automated Teller Machines (ATM) and financial accounts. In some cases, the attackers used the Society for Worldwide Interbank Financial Telecommunication