Transnational Cybercrime: The Dark Web

Barbara Jane Holland

INTRODUCTION

The world and human behavior have changed so quickly through the use of technology. China and India have the largest population of internet users though only 55 percent and 34 percent have total access (Internet live stats 2016). The United States, Brazil, and Japan come next. The proliferation of technology has clearly led to changes in how individuals engage with the world around them. Today people shop and communicate in digital format.

Most people born in the mid-eighties have never lived without a computer. The endless development of human behavior has created unparalleled opportunities for crime and misuse.

Over the past thirty years, there has been a substantial increase in the use of technology by street criminals and new forms of crime that did not previously exist.

Technology is at the core of information security. It can enable crime, and but also prevent it. Every country has its own police agency that enforces its own laws. The growth of global transportation systems, international trade, computerized financial transactions, and worldwide availability, of information through the internet have facilitated the expansion of the international economy. These factors simultaneously provided the basis for transnational crime. There is a distinction between profit-seeking transnational crime and international crimes. Which are acts of terrorism, genocide, human rights abuses and other crimes that violate international law (Albanese 2011). Transnational crimes, by contrast, include theft, fraud, counterfeiting, smuggling and other violations of individual countries’ criminal laws that involve trans-border activities.

BACKGROUND

Cybercrime involves the use of computers and the internet to commit acts against people, property, public order or morality (de Villiers 2011). Some may occupy a computer to steal funds, information or resources. These thefts can be aimed at stealing money, company trade secrets, chemical formulas, and other information that could be valuable to a competing business. Others may commit destructive acts by releasing a malicious virus or worm to harm a computer system.

Cybercrime is an evolving form of transnational crime. The complex nature of the crime as one that takes place in the border-less realm of cyberspace is compounded by the increasing involvement of organized crime groups.

DOI: 10.4018/978-1-5225-9715-5.ch007
Transnational Cybercrime can be grouped into three categories. (Albanese, 2011).

**The First Category:** Provision of illicit goods such as drug trafficking, moving stolen automobiles and artwork, from one country to another for sales, is difficult to trace back to its original owner. (Alderman, 2012). Also included is the transportation and sale of counterfeit goods such as prescription drugs, medication and designer clothing.

**The Second Category:** Provision of illegal services, includes human trafficking, with the transportation of sex workers or undocumented immigrants illegally into the country (Shamir, 2012). Also included are fraudulent investments and child pornography.

**The Third Category:** Infiltration of business or government. (Albanese, 2011). This category includes the widely publicized conclusion by American Intelligence agencies that Russians under the direction of the Russian Government, sought to affect elections in the United States by hacking into American computers and selecting revealing information that would help or hurt certain political candidates. According to the United Nations, the annual profits from Transnational organized crime amounts to 870 billion annually with drug trafficking producing the largest segment of that amount.

Law enforcement official faces huge challenges in combating transnational crime.