


Transnational Cybercrime: The Dark Web

Barbara Jane Holland

 <https://orcid.org/0000-0003-3729-0147>

Brooklyn Public Library, USA

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.

Figure 1. Cybercrime



Table 1. World wide web

Surface Web Google, Bing Facebook LinkedIn, eBay, Amazon Illicit online pharmacies Anonymous forums	Deep Web Medical Records Legal documents scientific Reports Academic documents Government documents	Dark Web Mirrored Websites Private Communication Illicit Activity
---	---	---

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.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/transnational-cybercrime/248035

Related Content

Gender and Access to Justice and Uganda's Criminal Justice System

Winfred Kyobiika Naigaga (2022). *Comparative Criminology Across Western and African Perspectives* (pp. 232-257).

www.irma-international.org/chapter/gender-and-access-to-justice-and-ugandas-criminal-justice-system/305506

Case Study: South Africa

(2023). *Comparing Black Deaths in Custody, Police Brutality, and Social Justice Solutions* (pp. 121-168).

www.irma-international.org/chapter/case-study/323587

Borders and Rights: Human Smuggling vs. Human Trafficking

Ana M. Fuentes Cano (2024). *Modern Insights and Strategies in Victimology* (pp. 93-117).

www.irma-international.org/chapter/borders-and-rights/342797

How Nigerian Junior Secondary School Students Perceive Internet Child Exploitation

Talatu Salihu Ahmaduand Hafsat Lawal Kontagora (2021). *Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities* (pp. 95-116).

www.irma-international.org/chapter/how-nigerian-junior-secondary-school-students-perceive-internet-child-exploitation/270490

The Victimization and Disparate Treatment of Racial and Ethnic Minorities

Rhiannon Oakes, Annie K. Oakeleyand Rola Goke-Pariola (2021). *Invisible Victims and the Pursuit of Justice: Analyzing Frequently Victimized Yet Rarely Discussed Populations* (pp. 353-382).

www.irma-international.org/chapter/the-victimization-and-disparate-treatment-of-racial-and-ethnic-minorities/281365