Social Media and Online Gaming: A Masquerading Funding Source

Pedro Ramos, Florida International University, Miami, USA
Pierre Funderburk, Florida International University, Miami, USA
Jennifer Gebelein, Florida International University, Miami, USA

ABSTRACT
This article describes how the rise in technological innovation has allowed for transnational criminal organizations (TCOs) to expand their operations using virtual platforms such as social media and online video games. These virtual platforms are utilized by TCOs to conduct some of their traditional forms of crimes, such as money laundering. These criminal practices have found solace in technological innovation, mainly through the exploitation of rising technologies, such as online video games, video game consoles and peripherals, such as Virtual Reality headsets, inconspicuous electronic devices for children, Near-Field Communication (NFC), and finally, social media as tool for recruitment and immediate communication. TCOs have managed to utilize these mediums to conduct their criminal activities in part due to the lack or nonexistence of new or proper legislation that regulates how these new mediums can function without facilitating illicit activities and the germination of illicit markets.

KEYWORDS
Bitcoin, Money Laundering, Near-Field Communication, Online Video Games, Social Media, Terrorism, Transnational Criminal Organizations

1. INTRODUCTION
Crime and technology share a complex relationship. Crime thrives on innovation and ingenuity. Illicit markets and activities germinate where new legislations are in place, where proper legislation is lacking or nonexistent, or where there is a high demand for these illicit markets and their products. Despite strong regulation, transnational criminals are highly resilient and are always adapting to these new regulations and availability of better technologies. Based on the National Security Council’s definition, “transnational criminal organizations (TCOs) are criminal groups that operate across national borders and utilize corruption and violence to exploit transnational commerce and communications in order to disguise their illegal activities” (Harris, 2014). Innovation is an important aspect of TCOs that engage in criminal activities. Criminal organizations need to innovate in the interest of expanding and improving their operations. One of the several forms of illegal activities that TCOs engage in is the laundering of money obtained through criminal activities or corruption and concealing it through legitimate, legal means (Investopedia, 2017). Incidentally, money laundering helps finance other forms of illicit activities that range from drugs and illegal arms trade to terrorist activities.

Traditional forms of money laundering include cash smuggling, gambling, black market currency exchange, and other forms of fraudulent business operations (Richet, 2013). Nonetheless TCOs have progressively adopted new forms of money laundering in recent years. Due to the rapid technological

DOI: 10.4018/IJCWT.2018010103

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
development and the integration of financial transactions through online mediums such as social media and online gaming, criminal organizations have harnessed the ease of use provided by these virtual platforms and the light legislation focused on money laundering through such mediums.

This recent form of money laundering is the reason why crime is sometimes symbiotically dependent on technological development. Beyond digital money laundering, technology has enabled the proliferation of TC0s operations through the feasibility of online communication networks enabled by social media. Initially, online communication was facilitated by messaging services like AIM or Messenger where two or more individuals could communicate with each other by connecting to a server through their computers.

The detriment of these early online messaging services was that users were anchored to their computers in order to communicate with each other. Subsequently, this all changed with the introduction of newer technologies like cellphones that allowed text messaging. This was also further amended with the revolutionary introduction of smartphones, specifically the BlackBerry. Considered as the first “smart” device, the BlackBerry offered emails on the go as well as instant communication between other BlackBerry devices through BlackBerry Messenger (BBM) (O’Boyle, 2016). All these innovations in instant messaging became an integral part of smartphones since the introduction of the BlackBerry. Succeeding smartphones like iPhones and Android-based handhelds like Samsung Galaxy devices all adopted their own forms of instant messaging. WhatsApp (WA) is the clear example of the evolution of mobile instant messaging. This particular application has facilitated communication across the globe in ways never before imagined. Relying on both mobile data and WiFi, WA allows users to instantaneously send messages to other WA users. Long distance phone calls utilizing mobile data plans is also possible through WA. Furthermore, WA now offers end-to-end encryption when communicating with other users.

This is particularly important given the “golden age of leaks” presently afflicting issues of national security and whistleblowers (Sanders, 2017). There has been an increase in encrypted instant messaging applications that even government officials utilize to communicate with each other. Applications such as “Signal” allow for highly encrypted end-to-end communication (Sanders, 2017). Similar applications like “Confide” are even used by staffers in the White House. In addition to WhatsApp, other popular applications that offer instant messaging include Facebook Messenger, Viber, Line, Snapchat, and even Instagram.

2. BACKGROUND

Pursuing this further, in order to understand the feasibility of money laundering through social media and online video games, it is important to first assess the importance of these two mediums. It is also necessary to address these concepts to better understand the relationship between social media and online gaming. Social media can be defined as any medium that allows users to connect with each other and share content, ideas, culture, entertainment, and other social forms of expression. These social media platforms include popular outlets such as Facebook, Twitter, Tumblr, Reddit, Pinterest, Instagram, and Snapchat.

Although user interfaces vary significantly between these outlets, the main function remains the same: Social interconnectivity through shared content. Social media has the capacity to create complex networks and communities in ways that were not possible before due to geographical and technological restraints. Compared to other forms of communication like emailing or virtual chat rooms, it is easier for users in one country to quickly connect with users in other countries via social media through shared interests such as movies, television series, sports, and online video games.

Forums, like Reddit, have created vast, living communities that participate in the discourse of several topics that range from sports to complex philosophical and political theories. Social media’s popularity consists of its ability to appeal to all the different types of internauts that visit social media outlets like Reddit or Twitter. In that sense, there are also detrimental aspects produced by the same ease of social interconnectivity. Individuals seeking to participate in criminal activities are able to
In Internet’s Way: Radical, Terrorist Islamists on the Free Highway
www.igi-global.com/article/in-internets-way/86075?camid=4v1a