T

Transnational Crime

Louise Shelley
George Mason University, Arlington, Virginia, USA

Transnational crime has expanded dramatically in the past two decades as criminals have benefited from the speed and anonymity of the cyber world and encrypted social media. Developments in technology have facilitated the growth of many forms of traditional crime as well as introduced cyber-dependent crime in which the crime is linked to pernicious items sold primarily on the dark web, such as ransomware, botnets, and trojans. These new tools deployed by criminals have permitted the theft of billions of private records, the theft of identities, and the enormous growth of illicit e-commerce. This criminal activity has expanded even more during the COVID-19 pandemic when individuals are isolated and spend greater amount of time on the Internet and on cell phones. The increase in this crime has required cyber security firms and law enforcement to rely more on large-scale data analytics to stop this crime and to locate and aid its victims and bring criminals to justice.

Transnational criminals have capitalized on the possibilities of the Internet, the deep and the dark web, and social media, especially its end-to-end encryption to expand their activities globally. Criminals are among the major beneficiaries of the anonymity of this new world of big data, providing them greater speed and outreach than previously. This phenomenal growth has occurred over the last two decades but has intensified particularly during the COVID-19 pandemic as individuals are more isolated and use their computers and cell phones more to engage with the outside world.

The use of big data for criminal uses can be divided into two distinct categories: cyber-enabled crime and cyber-dependent crime that can exist only in the cyber world. Cyber-enabled crimes include existing forms of crime that have been transformed in scale or form by criminal use of the Internet, dark web, or social media. Included in this category are such crimes as drug trafficking, credit card fraud, human trafficking, and online sales of counterfeits, wildlife and antiquities. For example, dark websites have allowed bulk sales of narcotics facilitating impersonal interactions of drug traffickers and buyers. Silk Road, the first large online dark web drug marketplace, did billions of dollars in sales in its relatively short existence. Its replacement have continued to sell significant supplies of drugs online (Shelley 2018). During the COVID-19 pandemic, such cyber-enabled crimes as online fraud, dissemination of child abuse and pornography imagery, and sale of counterfeit medical products needed for the medical emergency have grown particularly.

Cyber-dependent crimes are defined as criminal activity in which a digital system is the target

L. A. Schintler, C.L. McNeely (eds.), *Encyclopedia of Big Data*,
https://doi.org/10.1007/978-3-319-32001-4_543-1

as well as the means of attack. Dark websites, accessed only by special software (e.g., Tor), sell these criminal tools such as ransomware, trojans, and botnets. Under this category of crime, information technology (IT) infrastructure can be disrupted, and data can be stolen on a massive scale using malware and phishing attacks. Many online cyber products are sold that can be used to extract ransoms, spread spam, and execute denial of service attacks. These same tools can lead to massive numbers of identity thefts and the theft of personal passwords facilitating intrusion into bank and other financial accounts and loss of large sums by victims. Ransomware sold online has been used to freeze the record systems of hospitals treating patients until ransom payments are made. Year-on-year growth is detected in cyber-dependent crimes and tens if not hundreds of millions of individuals were affected in 2020 through large-scale hacks and data breaches (Osborne 2020).

The availability of the Internet has provided for the dramatic expansion of customer access to purchase commercial sex and for exploiters to advertise victims of human trafficking. A major US government-funded computer research program, known as Memex, reported identified advertisement sales of approximately $250 million spent on posting more than 60 million advertisements for commercial sexual services in a 2-year period (Greenmeier 2015). The Memex tool that provides big data analytics for the deep web is now used to target the human trafficking criminals operating online. One human trafficking network, operating out of China, indicted by federal prosecutors was linked to hundreds of thousands of escort advertisements and 55 websites in more than 25 cities in the USA, Canada, and Australia. This case reveals how large-scale data analytics is now key to understanding the networks and the activities behind transnational organized crime (the USA et al. 2018).

Online and dark web sales as well as that conducted through social media are all facilitated by payment systems that process billions of transactions. The growth of global payments and the increased use of crypto currencies, many of them anonymized, make the identification of the account owners challenging. Therefore, finding the criminal transactions among the numerous international wire transfers, credit card, prepaid credit card, and crypto-currency transactions is difficult. Understanding the illicit activity requires the development of complex data analytics and artificial intelligence to ascertain the suspicious payments and link them with actual criminal activity.

Transnational criminals have been major beneficiaries of globalization and the rise of new technology. With their ability to use the Internet, deep and dark web, and social media to their advantage, capitalizing on anonymity and encryption, they have managed to advance their criminal objectives. Millions of individuals and institutions globally have suffered both personal and financial losses as law enforcement rarely possesses or keeps up with the advanced data analytics skills needed to counter the criminals' pernicious activities in social media and cyberspace.

Further Readings

Global Initiative Against Transnational Organized Crime. (2020). Crime and contagion: The impact of a pandemic on organized crime. https://globalinitiative.net/wp-content/uploads/2020/03/CovidPB1rev.04.04.v1.pdf. Accessed 22 Dec 2020.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. New York: Doubleday.

Greenmeier, L. (2015). Human traffickers caught on hidden Internet. https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/. Accessed 22 Dec 2020.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Cambridge, MA: Harvard University Press.

Osborne, C. (2020). The biggest hacks, data breaches of 2020. https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/. Accessed 22 Dec 2020.

Shelley, L. (2018). *Dark commerce: How a new illicit economy is threatening our future*. Princeton: Princeton University Press.

United States of America, Chen, Z. a.k.a. Chen, M., Zhou, W., Wang, Y. a.k.a. Sarah, Fu, T., & Wang, C.. (2018, November 15). https://www.justice.gov/usao-or/press-release/file/1124296/download. Accessed 22 Dec 2020.