JIED Journal of Illicit Economies and Development

Albanese, J. 2021. Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. *Journal of Illicit Economies and Development*, 3(2): pp. 160–166. DOI: https://doi.org/10.31389/jied.111

POLICY COMMENTARY

Cybercrime as an Essential Element in Transnational Counterfeiting Schemes

Jay Albanese
Virginia Commonwealth University, US
jsalbane@vcu.edu

Transnational counterfeiting conspiracy cases often link the developing and the developed world in illicit ways. In many of these cases, a forged copy of name-brand merchandise is produced cheaply, and transported and shipped to a destination market where it is sold to consumers at a high mark-up, producing multiple harms. An overlooked element of these counterfeiting schemes is the essential role that cybercrime plays in their operation. Several transnational organized crime and cybercrime prosecutions are examined here to assess the role of counterfeiting in these criminal operations. The three conspiracies involve electronics, pills, and perfume—all illustrating the centrality of cybercrime in their commission. The implications for investigation, policy and practice are noted.

Keywords: counterfeiting; cybercrime; organized crime; conspiracy; illicit products; trafficking

Introduction

Cybercrime is closely linked with computer intrusions, identity fraud, sexual exploitation, malware and ransomware attacks, and cyberstalking. Its role in counterfeiting schemes has not drawn as much attention, but it will be shown here that cybercrime is an essential element of counterfeiting. Cybercrime enables the adding of high value to counterfeit/fake merchandise. Without good quality branding with fake labels, shipping, and logos, counterfeiting schemes would not work because customers would not be deceived. Without the deception required for counterfeit product distribution, criminal schemes could not survive. This analysis provides evidence that cybercrime is an essential element of more "traditional" forms of organized crime, beyond computer and information attacks, such as counterfeiting conspiracies and the trafficking in illicit goods.

What is Cybercrime?

Cybercrime can be seen as a method of crime commission, but it is also a substantive criminal offense in many jurisdictions. The central idea behind all the various types and definitions of cybercrime is the use of information technology to commit criminal acts (UNODC, 2013; Viano, 2017). Cybercrime is not limited to cases involving intrusion of computers, but it is the larger misuse of computer and information technology to commit crimes, whether or not the computer is the instrument or the object of the offense (Albanese, 2015; Levine, 1987).

The central principle of counterfeiting is using another person's intellectual property without permission in order to make an illicit profit. Patents, copyrights, and trademarks protect the creations (intellectual property) of inventors, artists, musicians, and authors from having their work copied and altered without permission.

The harms produced by counterfeiting are of two general types: financial fraud victimization and the danger posed to victims. Fraud victimization involves the receipt of inferior products and the payment of funds for a product or document not received. The dangers posed by counterfeiting and forgery are the unsafe nature of inferior products (e.g., medicines, toys, toothpaste, automobile parts) and the deleterious impact on the economy (e.g., loss of jobs in legitimate manufacturing companies, impact on the balance of trade

around the world, and on the development of new product ideas which are often stolen and used to make imitations).

Interest in cybercrime has been dominated by cases involving computer intrusions, identity theft, ransomware attacks, and cyberstalking—all with clear cyber implications, often with a computer or network as the target of the crime. In many cases of transnational organized crime, however, the computer is an instrument in the conspiracy, so the cyber element of crime is a method rather than a criminal objective.

Three counterfeiting conspiracies

Three types of counterfeiting cases were selected to illustrate how widely divergent forms of manufacturing and trafficking in counterfeit goods can each employ some form of cybercrime as essential to their commission. The three types of cases chosen were counterfeit electronics, pills, and perfume. Each of these three cases will be summarized, followed by an assessment of their common cyber components.

It is important to recognize that many other specific cases could have been chosen for this analysis. These three cases were selected because of their large scope and wide differences in the products counterfeited. In addition, these cases had more extensive available documentation, given their size, with each involving at least three countries, creating ideal case studies.

Information for this analysis was obtained from indictments and other court and public records of each case. The criminal prosecutions for these cases occurred in the United States, as the end point of each conspiracy. However, it is possible that other criminal cases against these schemes could be made in other jurisdictions in which the counterfeit products were sourced, manufactured, transported, or sold.

Electronics

A foreign national, living in the United States on a student visa, pleaded guilty for his role as a counterfeit distributor in a scheme to traffic and smuggle counterfeit electronics purporting to be Apple iPhones and iPads from China into the United States. The principal, Jeff Li, age 43, worked through his company "Dream Digitals" (based in Hong Kong), conspiring with others to smuggle and traffic into the US, from China, more than 40,000 electronic devices and accessories, including iPads and iPhones, along with labels and packaging bearing counterfeit Apple trademarks.

Mr. Li also received payments totaling over $1.1 million in sales proceeds into his bank accounts in the US as well as those of his co-conspirators in Hong Kong and China. His co-conspirators also pleaded guilty. Mr. Li shipped devices separately from the labels and logos bearing counterfeit trademarks and assembled them later, a tactic designed to avoid detection by U.S. Border officials. The devices were then shipped to conspirators throughout the US. Proceeds from the sales of the devices were funneled back to the co-conspirators' accounts in the US via structured cash deposits (making deposits of under $10,000 USD to avoid bank reporting requirements). A portion of the proceeds was then transferred to conspirators in Italy, further disguising the source of the funds (U.S. Department of Justice, 2018).

The operation of the scheme is summarized in **Figure 1**. It shows how the scheme operated in the US, but had facilitators in China and Italy for electronics supply and money laundering purposes, respectively.

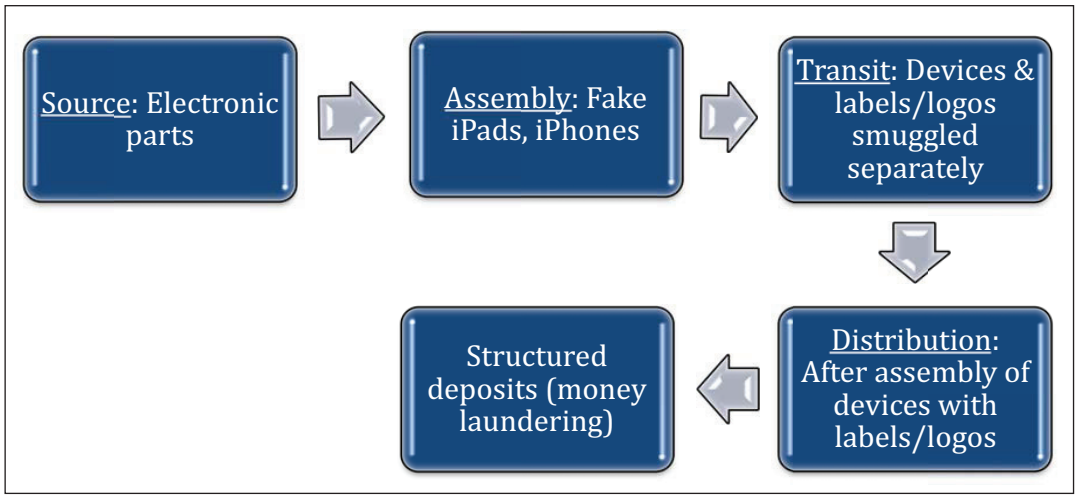

Figure 1: Counterfeit Apple products conspiracy.

This scheme, like others of this type, was prosecuted as a counterfeiting case.

It was discovered through a joint investigation from US Homeland Security Investigations (at the US border), the Bergen County (US) Prosecutor's Financial Crimes Unit, Europol, and Italy's Guardia di Finanza. This international cooperation was necessary in tracking the source of the counterfeit goods and the disposition of the proceeds of the criminal scheme.

The offenders in this scheme were charged with trafficking and smuggling counterfeit electronics with counterfeit labels, but cybercrime, which was a central element of the illicit enterprise, was not pursued. Specifically, an essential element of the scheme was the need for high quality labels bearing counterfeit trademarks. It is this labeling (i.e., good quality counterfeits) that is crucial to the success of the scheme. An unknowing consumer would not realize that the counterfeit iPads and iPhones were of poor quality until long after the purchase (when the devices did not operate with the same quality that authentic devices do). This delayed realization of the fraud by the victims protected the traffickers and the distributor from detection by customers, because the products *looked* genuine.

An essential part of the counterfeiting process is the need for labeling that looks exactly like the real thing, including counterfeit shipping labels. This task requires cyber-capability to design, manufacture, and distribute high quality counterfeit labeling able to deceive both consumers and border inspectors. It is the visual branding capacity, made possible by misusing cyber tools, that provides value to the counterfeit product. Without high quality fake labels and logos, distributors and consumers would not be interested.

As the indictment in this case stated, an important part of the scheme was to "intentionally traffic in labels, stickers, boxes, and packaging for such goods, knowing that a counterfeit mark had been applied thereto" in addition to "knowingly using a counterfeit mark on and in connection with such goods" in manufacturing the fake Apple products. The participants in this scheme shared via email a "listing of the prices for stickers, boxes, and packaging, all purporting to bear counterfeit Apple marks, which he was offering for sale" (U.S. v. Becerra, et al., 2015). This information indicates that the counterfeit labeling process was a separate criminal enterprise, which was required to distribute the counterfeits electronics successfully. A three-year prison sentence was imposed in this case (U.S. Department of Justice, 2019).

Without cybercrime (through the misuse of computer technology to create high quality counterfeit labeling and products and shipments), criminal schemes like this one cannot be successful over the long term. They cannot develop into a large illicit enterprise involving many counterfeit products and shipments without high quality false labels and trademarks. So, the question to be asked is whether counterfeiting schemes rely on cybercrime capabilities as an essential element?

Pills

A second common form of counterfeiting scheme is the manufacture of fake pills popular among consumers. Popular pills include: steroids, fentanyl, and Viagra.

In a scheme involving counterfeit Viagra, testing on samples of the seized drug found it to contain less than the 100 mg of active pharmaceutical ingredient (API) indicated on the labels. Counterfeit Cialis was also seized and tested, revealing small quantities of the Viagra API and no Cialis at all. In addition, some of the counterfeit Viagra tablets were found to contain the unrelated compound 2-MBT. The counterfeit Viagra and Cialis tablets looked like the authentic products and included labels and packaging that closely resembled the registered trademarks of either Eli Lilly and Company or Pfizer Inc. (U.S. Attorney, 2016).

The counterfeits bore the same mark, shape, and appearance as the genuine Viagra tablets. The tablets were shipped transnationally from Asia to North America. According to the indictment, on each pill, "counterfeit marks were identical with and substantially indistinguishable" from the genuine marks registered for this manufacturer (U.S v. Khattab et al., 2012; U.S. Department of Justice, 2013). Similar to other conspiracies involving false medications, members of the criminal scheme purchased counterfeit labeling and packaging from overseas suppliers, as well as the raw materials to manufacture the drugs, either by using money remitters or by shipping U.S. currency to foreign suppliers (US Attorney, 2017; U.S. Attorney, 2017a).

Similar to the previous case involving counterfeit electronics, this criminal enterprise relied on a separate cyber-criminal operation to generate the counterfeit labeling, logos, and packaging (U.S. Department of Justice, 2016a; 2021). Cyber- criminal operations are an essential element of counterfeiting enterprises because it is the *appearance* of the genuine product which makes the counterfeiting criminal enterprise possible and ongoing.

Perfume

The "Counterfeit Perfume Ring" was a group of individuals who imported generic liquid fragrances, separately importing boxes and packaging bearing counterfeit trademarks, from China. They packaged the generic liquid fragrances into the branded and trademarked packaging, and then sold counterfeit perfumes to wholesalers in New York and at least six other states in the US (U.S. Department of Justice, 2016).

It is noteworthy that the imported counterfeit packages were marked with false representations of the products inside. At the U.S border, inspectors discovered many bottles of unlabeled fragrances which had the same size, shape, color, and features of trademarked, brand name perfume bottles. Other boxes were labeled as Dolce & Gabbana Light Blue perfumes, which were determined not to be the authentic product. Additional shipments contained 20,000 counterfeit Chanel No. 5 product boxes, 4,000 Prada brand, 2,600 Lacoste, 2,000 Versace, and 1,000 Coco Chanel brand perfume boxes—all of which were counterfeit (U.S. v. Badal, et al., 2016).

Through physical surveillance, searches, and review of written records, a chain conspiracy was revealed. The scheme involved moving generic liquid fragrances and counterfeit packaging separately from China to Port Newark in the US. These shipments were supplemented by others containing unmarked bottles in the shape of well-known fragrances. Packaging occurred in New York, combining the generic fragrance, bottles, with counterfeit labels and packaging. The items were then shipped to multiple locations for distribution and sale. **Figure 2** diagrams the criminal scheme.

Similar to the earlier electronics and pill counterfeiting schemes, the perfume ring had a separate criminal agreement with a supplier who manufactured the high-quality counterfeit labeling and shipping documents. Other cases of this type appear to have a similar method of operation (U.S. Department of Justice, 2018a). This suggests that the cyber scheme to create the labeling was an integral, yet separate, part of the counterfeiting and distribution scheme.

Discussion

The cybercrime element in counterfeiting schemes can take several different forms. In some cases, the counterfeiter can scan a logo into a computer to create a digital file. This file can then be transferred into a computerized embroidery machine, for example, using the digital image to recreate the design on garments or bags. However, it is often more complicated than this to make high-quality fakes, so counterfeit labels are usually made by illicit specialists in their own factories, with specialized scanners, printers, and imprinting tools (Abagnale, 2002; UNODC, 2019). A separate fake labeling, brand name, and logo enterprise was seen in every one of the three counterfeiting schemes presented here. It is also present in related schemes that have been prosecuted (several noted above; see also Foltz, 2008; Guarnieri & Przyswa, 2013).

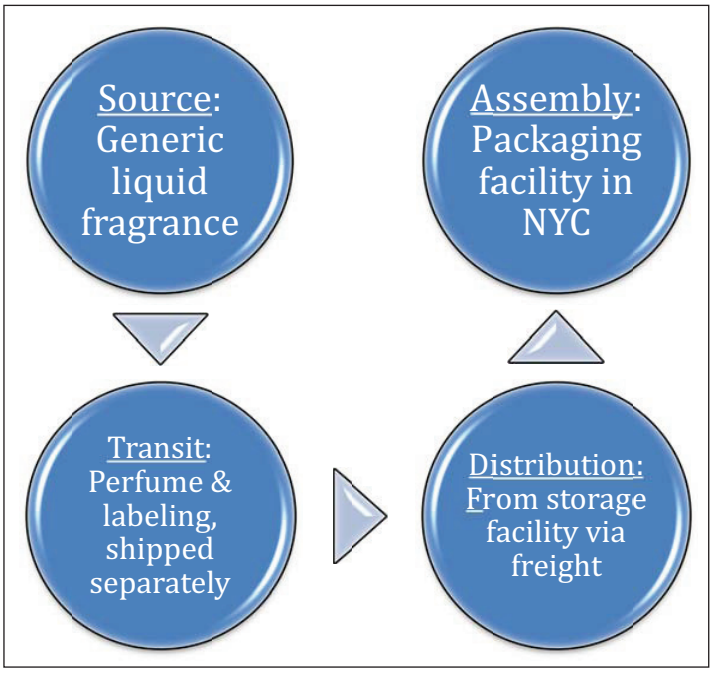

Figure 2: "Counterfeit Perfume Ring".

The implications for policy and practice of this counterfeit-cyber connection are several: 1) The growing use of two-dimensional barcodes, watermarks, micro text, holograms, RFID tags, and forensic taggants are all designed to make counterfeiting more difficult as well as to authenticate the real thing (Anti-Counterfeit Labels, 2017; Safeguarding, 2017). 2) These deterrents to counterfeiting, spurred by industries to protect their brands more effectively, increasingly require illicit specialists to defeat them, using cyber technology to do so.

This analysis also suggests that the prosecution of counterfeiters and their distributors addresses only part of the problem. A separate, and often overlooked, key feature of counterfeiting schemes is the essential element of cybercrime specialists who work to defeat brand names, labels, and logos. These criminal entrepreneurs are the ones who make counterfeiting possible through the creation of high-quality fakes that are indistinguishable to most consumers. This is a crucial insight for policy and practice.

Figure 3 illustrates the central elements to each of the three counterfeiting schemes described here. It is suggested that these elements are required for any large counterfeiting enterprise. The fake products were shipped separately from the false labeling and logos, which were supplied by a different conspirator. Therefore, the manufacturers of counterfeit labels are the hidden players in counterfeiting cases, who often avoid detection and prosecution. This is a significant observation for those developing counterfeiting and fraud cases, and those designing policy to obstruct these schemes.

Conclusion

Cybercrime is often associated with computer intrusions, identity theft, ransomware attacks, and cyberstalking. This analysis provides evidence that cybercrime is also an essential element of more "traditional" organized crime, including counterfeiting conspiracies and the trafficking in illicit goods.

The question asked above is whether counterfeiting schemes rely on cybercrime capabilities as an essential element. It appears from these three transnational cases, and many others, that cybercrime is an essential element of counterfeiting schemes. In every case, a "hidden" participant was the creator and manufacturer of the high-quality fake labels, logos, and trademarks. Increased attention to the cyber-capability to produce high quality counterfeits that mimic brand names, packaging, and shipping labels are key to defrauding customers, deceiving inspectors at ports of entry, and frustrating investigations. This is an important perspective to consider in counterfeiting investigations.

Greater emphasis on the misuse of cyber capabilities as an essential element connected to the trafficking in counterfeit goods would increase the difficulty of operating successful criminal schemes involving the trafficking of fake goods. It is the visual branding capacity, made possible by misuse of cyber tools, created by illicit counterfeiting specialists, that gives value to the counterfeit product. Without high quality fake labels and logos, distributors and consumers would not be interested in the products, and counterfeiting schemes would not thrive.

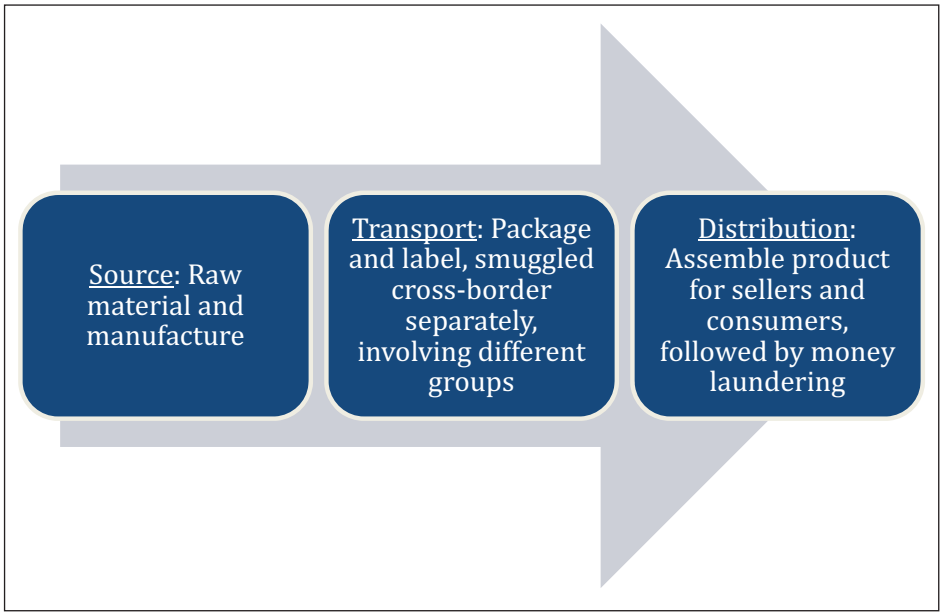

Figure 3: The essential elements of counterfeiting schemes.

Competing Interests

The author has no competing interests to declare.

References

Abagnale, FW. 2002. *The art of the steal: How to protect yourself and your business from fraud*. New York: Crown Publishing.

Albanese, JS. 2015. *Organized crime: From the mob to transnational organized crime*. New York: Routledge.

Consolidated Label Co. 2017. *Anti-Counterfeit Labels and Packaging Are Key To Brand Protection*. Available at https://www.consolidatedlabel.com/label-articles/anti-counterfeit-labels/ [Last accessed day month year].

Foltz, JE. 2008. Global crime case: Cybercrime and counterfeiting. *The Futurist*, 42(6).

Guarnieri, F and **Przyswa, E.** 2013. Counterfeiting and cybercrime: Stakes and challenges. *The Information Society*, 29: 219–226. DOI: https://doi.org/10.1080/01972243.2013.792303

Hampshire Label. 2017. *Safeguarding Your Brand With Anti-Counterfeit Labels*. Available at http://hampshirelabel.com/safeguarding-brand-anti-counterfeit-labels/ [Last accessed day month year].

Levine, DE. 1987. *Crooked computers or computer crooks? An examination of the development and treatment of computer crime*. Master's thesis, New York University.

United Nations Office on Drugs and Crime. 2013. *Comprehensive study on cybercrime*. Vienna: UNODC.

United Nations Office on Drugs and Crime. 2019. *Combating falsified medical product-related crime: A guide to good legislative practices*. Vienna: UNODC.

U.S. Attorney. 2016. *Two sentenced for trafficking in counterfeit Viagra and Cialis*. Southern District of Texas. December 6.

U.S. Attorney. 2017. *Gardner man charged with conspiracy to traffic counterfeit steroids*. District of Massachusetts. May 27.

U.S. Attorney. 2017a. *Joint law enforcement operation leads to conviction of East Bay counterfeit drug manufacturer. David Beckford sentenced to 123-month prison term for operating counterfeit Xanax pill operation*. Northern District of California. February 9.

U.S. Department of Justice. 2013. *Two men charged in Texas and arrested for smuggling counterfeit Viagra*. Office of Public Affairs. August 6.

U.S. Department of Justice. 2016. *Five charged in national counterfeit perfume ring*. Southern District of New York. May 25.

U.S. Department of Justice. 2016a. *Two Pakistani nationals sentenced for conspiring to illegally ship pharmaceuticals into the United States*. Washington, DC: Office of Public Affairs. November 4.

U.S. Department of Justice. 2018. *Chinese national pleads guilty to conspiracy and trafficking of counterfeit Apple goods into the United States*. Washington, DC: Office of Public Affairs. February 2.

U.S. Department of Justice. 2018a. *Twenty-two charged with smuggling millions of dollars of counterfeit luxury goods from China into the United States*. Washington, DC: Office of Public Affairs. August 16.

U.S. Department of Justice. 2019. *Chinese national sentenced to over three years in prison for trafficking counterfeit Apple goods into the United States.* Washington, DC: Office of Public Affairs. July 30.

U.S. Department of Justice. 2021. *Man convicted of conspiracy to import and distribute Fentanyl.* Washington, DC: Office of Public Affairs. July 9.

U.S. v. Badal, Shah, Ni, Kasher, and Shazzed. 2016. *Complaint* 16 MAG 3210. Southern District of New York. May 18.

U.S. v. Becerra, Marca, Li, and Volpe. 2015. *Indictment*. Crim. No. 15- 178-KM. U.S. District Court for the District of New Jersey.

U.S. v. Khattab, Al-Jabri, and Al-Jabri. 2012. *Indictment* 12 CR 514. Southern District of Texas. August 22.

Viano, EC. 2017. Cybercrime: Definition, Typology, and Criminalization. In *Cybercrime, Organized Crime, and Societal Responses*. Switzerland: Springer. DOI: https://doi.org/10.1007/978-3-319-44501-4

How to cite this article: Albanese, J. 2021. Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. *Journal of Illicit Economies and Development*, 3(2): pp. 160–166. DOI: https://doi.org/10.31389/jied.111

Submitted: 22 July 2021 **Accepted:** 27 August 2021 **Published:** 23 November 2021

LSE Press

Journal of Illicit Economies and Development is a peer-reviewed open access journal published by LSE Press.

OPEN ACCESS