5

Business Models

HISTORICAL TRANSFORMATION OF ILLICIT ENTREPRENEURSHIP AND TRADE

A great transformation of commerce is presently under way. More and more commerce is moving online, and trade is increasingly conducted through personal communication devices. As the location of trade shifts into the cyberworld, we are not facing an entirely alien phenomenon. Rather, the new illicit traders, like their predecessors and their counterparts in the legitimate economy, seek sales and profits to sustain their businesses. To operate successfully, they search for targets of opportunity, strategic alliances, and forms of trade with worthwhile profit markets. To grow, participants in illicit commerce must find capital for their businesses, as well as develop a market niche and a marketing strategy for their goods. As illicit traders grow their businesses, they are confronted with new challenges—recruiting and retaining employees, experts, and contractors; mitigating risk while retaining good profit margins; managing competition; and incorporating new technology into their sales and marketing models. If they are successful, they must choose whether to withdraw profits, reinvest their profits in existing trade products, or diversify. Sometimes illicit traders may

move their profits into the legitimate economy, either partially or entirely.

The Stages of Illicit Trade

Three large-scale criminal cases illustrated in table 5.1 reveal how illicit trade, entrepreneurship, and financial flows have changed dramatically with the development of the new technology of the internet, cell and smart phones, the Dark Web (the part of the web accessible by Tor and similar software that hides your location and identity), credit cards, and cryptocurrencies.[1] The cases will also be used to illustrate fundamental principles of the dynamics of illicit business.

Table 5.1 outlines the primary transformation of illicit trade. The first stage, which existed for at least 3,750 years, involved concrete objects traded by known individuals, using currency and tangible financial instruments, often backed by states, and items of value such as gold and silver. This form of trade, which has been with us since the dawn of written legal history, is still with us today, as we will see in the first case of a long-lasting American car theft ring.

Stage 2, illustrated by the Pharmaleaks case, represents the transitional form of illicit trade that has arisen as the new medium of the internet has allowed illicit sellers to rapidly grow their businesses and expand their customer base. Just as we saw the Smirnovs in chapter 1 scaling the age-old profession of fencing to its online version, the transitional phase is not unique to computers or to computer crime. Throughout much of history, technological innovation has merely extended existing modus operandi into a new medium.[2] In the Pharmaleaks case, Russian online criminals sold large quantities of counterfeit pharmaceuticals to American, western European, and Australian customers. In the impersonal world of stage 2, there are no longer personal connections between buyer and seller. In contrast to stage 1, stage 2 introduces the new tools of the global financial system—credit cards and wire transfers. This is cyber-assisted crime.[3]

The third stage, represented by the Avalanche case, includes not just illicit trade but illicit entrepreneurship. The sellers produce and market virtual and intangible products to sabotage computers and

TABLE 5.1. THE STAGES OF ILLICIT TRADE

Time Frame	Products	Financial Payments
Stage 1: Hammurabi to the mid-1990s—trade in stolen goods and tangible items	People dealing in tangible property (e.g., Operation Dual Identity)	Cash, trade-based money laundering, barter, Western Union and other wire transfer businesses
Stage 2: Mid-1990s to the present—computer-facilitated crime	People dealing in tangible property but selling online, usually through the web (e.g., Pharmaleaks, counterfeits, antiquities, wildlife parts)	Payment systems tied to the global financial economy (credit cards, prepaid credit cards, wire transfers, trade-based money laundering);efforts made to hide identity of buyers and sellers
Stage 3: Late 1990s to the present—crime linked solely to computers	People dealing in intangible property through the web and the Dark Web (e.g., Avalanche) in crimes such as malware, Trojans, spam, botnets, phishing tools, fake antiviral software, hacking tools, ransomware, denial-of-service attacks, and other malicious computer products; theft of identities, credit card numbers, and intellectual property such as songs, videos, and products in development; and employing people to deploy pernicious cyber-tools	Payment systems tied to the global economy and to cryptocurrencies (e.g., Bitcoin, Liberty Reserve); online gaming used to launder money; transactions often anonymized

computer systems, such as botnets, malware, and Trojans, and services such as denial-of-service attacks. Seller-buyer relationships and payments are intentionally anonymized in the Dark Web, as encryption is used to hide the identities of sellers and purchasers.[4] Some of the currency has gone virtual and is not tied to any currency or metal of value.

The evolution from stage 1 to stage 2 took almost four millennia. Yet the evolution from stage 2 to stage 3 was extremely rapid—only

a few years. This illustrates the transformative property of the new technology. Unfortunately for the global community, all three stages of illicit trade now coexist.

Stage 1: Operation Dual Identity—Illicit Trade in Tangible Goods and Currency

In Tampa, Florida, a few cars had been stolen from a local car dealership, and local detectives needed help. An FBI agent who assisted them was directed by his superiors to devote his efforts to more substantial cases. But he kept on investigating the car theft part-time, convinced that he was on to something bigger. His perseverance paid off: a couple of years later, fifty law enforcement agencies across the United States were investigating car thefts in Florida, Texas, and Illinois committed by a group of Cuban American thieves.

Operation Dual Identity, as the criminal operation was subsequently named, revealed one of the largest car theft rings in the United States, operating for over twenty years, during which time more than a hundred people stole a thousand expensive cars. A potential buyer would ask one of the ring members to obtain a specific type of high-end vehicle. The criminal would satisfy the request by either drawing on stock or committing vehicle thefts on order in other states. Key to the deal was obtaining a legitimate vehicle identification number (VIN) from a car of the desired brand. Mexican criminals served as service providers producing counterfeit VIN plates and labels, as well as phony title documents that would facilitate resales.[5] The cars were marketed through underground networks throughout the United States, especially in Chicago and Texas, for cash or its equivalent.[6] As the criminal operation evolved and more criminal activity was conducted in online marketplaces, the car thieves evolved and, consistent with activity in stage 2, sold some vehicles through eBay and Craigslist.[7]

Press releases on Operation Dual Identity reported only on the disruption of the $25 million car theft ring. None reported on what the investigators found when they followed the money.[8] The investigators did not find an offshore bank account, but rather investments

of the criminals' proceeds in another illegal activity—marijuana farms. Running a marijuana facility is a tough business. Lights are on all night, and the plants must be monitored twenty-four hours a day to produce good yields. Not many people perform this work voluntarily for a minimum wage. But working on a marijuana farm was then illegal and remains so today in most states. Undocumented migrants would not labor in such farms voluntarily, as doing so would enhance their risk of deportation. Legal workers would avoid such difficult jobs that paid little and might lead to their arrest.

To secure workers, the Spanish-speaking leaders of the car theft ring pursued a logical business strategy—they imported hundreds of smuggled Spanish-speaking workers from Mexico. Forcing smuggled Mexicans to work in illegal employment for long hours, the marijuana farm operators then transitioned from smuggling to trafficking individuals. Operation Dual Identity may be the best example of convergence between the drug trade and human trafficking in the United States, but it is far from unique.

Similar patterns are observed in the marijuana farms of Great Britain. The exploited there are Vietnamese, often children, as illegal marijuana cultivation is controlled by members of the Vietnamese diaspora community. Similarly inhumane conditions are recorded there, as the laborers work long hours under glaring lights without any protective glasses.[9]

Stage 2: Pharmaleaks—Tangible Property Sold on the Web through the Global Financial System

The Pharmaleaks case, representing stage 2, illustrates many of the defining aspects of the illicit online marketplace.[10] Unlike the long-existing car theft business representative of stage 1, which delivered good profits over an extended period, the cyber-pharmaceutical business scaled rapidly and delivered an excellent rate of return for the three-year period in which it functioned. Analysis of the cybercriminals' financial transactions reveals that they netted more than $25 million over this period—about the same revenues collected by the Operation Dual Identity criminals over twenty years. The

cybercriminals behind Pharmaleaks, however, earned far less than Dread Pirate Roberts (discussed in chapter 3), who sold narcotic drugs on the Dark Net market Silk Road. Nevertheless, the criminals of Pharmaleaks enjoyed a very significant rate of return for a limited investment.

The Pharmaleaks investigation unmasked three online black market pharmaceutical sites—GlavMed, SpamIt, and RXPromotion—each of which operated out of Russia on the World Wide Web between 2007 and 2010, generating $185 million in sales of Viagra as well as unregulated or counterfeit medicines for heart disease, infections, obesity, pain, and mental health.[11] Fortunately for the purchasers of Pharmaleaks products, when tested, some of these counterfeit medicines, sold without requisite prescriptions, did have the appropriate active ingredients in the correct proportions.[12] But other purchasers of some online pharmaceuticals were not as fortunate, as we will see in chapter 6.[13]

Pharmaleaks's financial data could be analyzed because rival online illicit pharmaceutical companies hacked into their competitor's business records and then distributed these leaked documents "very broadly on under-ground forums and file-sharing sites, and other times distributing to a variety of journalists, e-crime researchers, law enforcement agencies as well as a broad range of underground actors." These methods mimicked the exposures of WikiLeaks—hence the name Pharmaleaks.[14] In contrast to WikiLeaks, Pharmaleaks also issued physical threats, undermining the presumption that the criminal trade in the cyberworld is devoid of the violence of street-level commerce.

Viagra was a product of choice for the cybercriminals because of its high profit margins. A decade earlier, the street value of Viagra had already created a distinct financial advantage for traffickers over trading narcotics. Heroin could be marked up 66 percent, cocaine 4,600 percent, and opium 27,400. Yet the markup figure for Viagra was an astonishing 166,700 percent.[15] The comparative profit advantage of the counterfeit pharmaceutical trade helps explain its explosive growth. Interpol evaluates the annual turnover from pharmaceutical crime at $75 billion.[16]

Surprisingly, the masterminds behind Glavit and Spamit, Igor Gusev and Pavel Vrublevsky, did not fully capitalize on the price advantage of counterfeit Viagra for two reasons—high advertising budgets and costly corruption that limited their profits to approximately 16 percent.[17]

Legitimate online sellers such as Amazon use independent contractors called "affiliates" to drive customers to their websites. In the parallel world of affiliates for criminal traders and sellers of pirated digital content, diverse techniques are used, such as spam, chat forums, blogs, social media, and SMS messages.[18] The cost of advertising in the criminal online world is much higher than in legitimate commerce because of the risks and the high cost charged to develop and disseminate spam. Highly competent affiliates working for criminals can make $5,000 daily, or $300,000 monthly.[19]

The managers of Pharmaleaks paid commissions to affiliates of 25 to 60 percent, depending on the service provided.[20] In return, the spammers working for Gusev and Vrublevsky blanketed people's email in many countries, becoming some of the largest propagators of spam on the internet. Spam may be costly for the company but highly profitable for the spammer. As a New Scotland Yard specialist explained in 2012, "A spammer only needs a 0.0001 percent response rate to be in profit."[21] The companies behind Pharmaleaks at their height were responsible for almost half of the spam sent in the world; therefore, they drew many customers, but payments to spammers reduced their profit margins significantly.[22]

The Pharmaleaks companies also paid corrupt bank insiders to secure access to payment systems that linked them to global banking, permitting purchasers to charge the drugs they ordered through credit cards. Credit card charges for Pharmaleaks were processed through a few key banking hubs known for their facilitation of money laundering, such as Azerbaijan and Latvia. The banking relationship was the key for the online pharmaceutical business model in the days before cryptocurrencies. Once these bogus pharmaceuticals sellers were cut off by Western law enforcement from the financial institutions that facilitated their credit card payments, the businesses went into a nosedive. The online criminals cursed the credit card

companies, writing in Russian, "The . . . Visa is burning us with napalm."[23] But with the sales drop, the level of spam on the internet also declined dramatically.[24]

Pavel Vrublevsky was eventually sentenced to two and a half years in a Russian prison for his computer crimes when he crossed the wrong people. But after a short period of detention, he took the Russian government equivalent of an offer "you cannot refuse": work for the Russian government and "get out of jail now." Released, he was appointed the head of the Russian government's national payment system.[25] Vrublevsky's appointment may have been owed not only to his high-level computer skills but to his vast contacts with the managers of botnets whose tools are used to produce spam and propagate false news.[26] Through management of the Russia's state payment system, Vrublevsky was perfectly placed to hide irregular payments among the mass of normal payments and to pay the rogue IT community responsible for the cyber-campaigns of the Russian state.[27]

Vrublevsky personifies the cyber-buccaneer or cyber-privateer—the criminal who preys off others for profit, but simultaneously serves his government in cyberspace.[28] The Russian criminal world provides fertile recruitment for state-sponsored hackers, especially when foreign investigations point the way to the most talented criminals.

Stage 3: Avalanche: Virtual Products Sold through the Global Financial System and Cryptocurrencies

The Avalanche case, resulting from the cooperation of many police forces around the world, addressed one of the world's largest and most costly criminal enterprises operating in the Dark Web. At the time of its takedown, the network had infected computers in 189 countries, with as many as 500,000 computers affected daily.[29] The network, operated by Ukrainian and Bulgarian master criminals for almost a decade, met little challenge from law enforcement in their home countries.[30]

In 2016, a key figure in the network, Krasimir Nikolov, was arrested after Western investigators, following payments from victims of ransomware attacks, were led to Bulgarian accounts associated

with Nikolov.[31] Shortly afterwards, in December 2016, the police in Poltava, a central Ukrainian city, arrested Gennady Kapkanov, another key figure behind Avalanche, after a violent struggle with a commando squad that came to arrest him. Unfortunately, his detention was short-lived. After Kapkanov was released by a judge, the police soon lost track of him, reflecting either the corruption or incompetence of regional Ukrainian law enforcement.[32]

The Avalanche network caused global harm because it "hosted more than two dozen of the world's most pernicious forms of malicious software" sold to customers worldwide.[33] Customers have no equivalent to a Google search engine in the Dark Web. Therefore, the cybercriminals behind Avalanche found customers by advertising their products and their locales on postings on exclusive underground online criminal forums that operate in the Dark Net.

Malware sold by the criminals of Avalanche infected the computers of both individuals and companies and could be used as weapons in cyberspace. The superstar of the malware world, GozNym, was sold on the Avalanche platform and used to target twenty-two financial institutions in the United States. In Germany alone, the criminals caused damage estimated at 6 million euros (approximately $7.5 million) to just the online German banking system.[34] They also sold Corebot, a Trojan used to steal banking and credential information in order to access online bank accounts.[35]

Ransomware sold to criminals resulted in victims' losses in the hundreds of millions of dollars.[36] Those purchasing the Nymaim malware were able to encrypt the computer files of their victims, blocking access to the contents of their computer systems. Victims would pay significant sums to their ransomware attackers to obtain a key that would allow them to decrypt their files. Many online heists via ransomware generated tens of millions of dollars. The criminals also used malware to seek revenge on law enforcement. Ransomware bought from the Avalanche network facilitated an attack on the Allegheny County District Attorney's Office in Western Pennsylvania, which admitted paying the equivalent of $1,400 in Bitcoins to recover access to its computer files, affirming the role of cryptocurrency in Avalanche payment systems.[37]

The Three Stages of Illicit Trade and the Business Dynamics of Illicit Trade

Illicit commerce has changed profoundly in the past three decades. Yet analysis of the Operation Dual Identity, Pharmaleaks, and Avalanche cases shows that despite the rapid evolution of illicit trade, such enterprises still function as businesses. Table 5.2 outlines the key differences between licit and illicit entrepreneurs and traders. Both types of traders operate with a business logic: they need to find customers, effectively market their products, manage supply chains, and use technology to the best advantage. They also need to vet their employees. Where illicit merchants diverge most significantly from their licit counterparts is that they engage in subterfuge to hide their products and supply routes, systematically engage in corruption, consistently exploit workers, pay little or minimal attention to quality control, and increasingly rely on the Dark Net rather than the internet for their activities.[38] Rather than looking for integrity, illicit traders need to ensure that employees and contractors have the appropriate bone fides of past criminal activity and cyber-skills useful to computer attackers.[39]

Like the legitimate economy, the cyberworld specializes and outsources. For instance, the masterminds of Pharmaleaks did not attempt to run their spam in-house to reach potential customers; instead, they hired large numbers of spammers with specialized capabilities to push advertising over the internet, paying them on commission and on the basis of referrals.

Other criminal tools have not, however, lose their value: violence and intimidation remain tools of illicit business in both the real and the virtual worlds.[40] Violence, as discussed in the introduction, was attempted by the Silk Road creator and operator Dread Pirate Roberts, who hired hit men to defend his financial interests. The criminals of Pharmaleaks threatened violence in the virtual world, and Kapkanov fought off the police commandos with a Kalashnikov rifle.[41]

Criminals' illicit activity intersects with the legitimate economy through their use of banks, credit cards, mail services, and legitimate transporters. The perpetrators of Pharmaleaks received payments

TABLE 5.2. ENTREPRENEURSHIP AND TRADE

	Licit Entrepreneurship and Trade	Illicit Entrepreneurship and Trade
Business logic?	Yes	Yes, but often shorter time perspective, especially in cyber-related businesses
Consumers	Seek desired products, at fair prices, that are legally available both in brick-and-mortar stores and online	Seek products that are not legally available and cheaper sources of supply; often not aware of origin
Access to capital	Easier access to capital from many legal sources, banks, crowdsourcing, stock markets, venture capital funds	Extortion, crowdsourcing; low-profit crimes may provide venture capital for more profitable ones; corrupt officials may use natural resources under their control
Personnel	Wide range of personnel to choose from, especially individuals with high skill and education levels; expected to adhere to labor standards and law; training provided; diaspora communities are important	Exploit migrants and the vulnerable, especially those without access to legitimate employment; coercion often used; web used to find personnel; training often provided; diaspora communities are important
Marketing strategies	Advertising, affiliates drive individuals to online web sites; access to sophisticated marketing and advertising companies	Online media used for marketing; criminal affiliates drive purchasers through spam to websites; Dark Net; advertising through private chat groups and forums
Growth strategies	Diversification, franchises, strategic alliances	Diversification, franchises, strategic alliances, corruption
Product development	Licit entrepreneurs need budgets for research and development; attention to quality control	Theft of new product designs and intellectual property; investment in development of malicious tools for computer; quality control not a concern
Dealing with competition	Legal means—improve pricing, emphasize competitive advantage in marketing	Use extralegal means, including violence, corporate raiding (Russia)
Transport and supply chain logistics	Seek most efficient routes to move goods; transparency of supply chains	Use traditional trade routes for illicit goods; use secondary ports and FTZs to transfer illicit goods; use subterfuge and nondirect routes to disguise commodities; merge illicit trade with licit trade

from American credit cards, and Nikolov of Avalanche used known Bulgarian banks. It is this intersection of the illicit and licit worlds that makes criminal organizations most vulnerable, however, and it helped bring down several of these criminal operations.

Business Dynamics in the Illicit and Licit Worlds

BUSINESS LOGIC

Stages 1, 2, and 3 of illicit business all operate with a business logic, although only Operation Dual Identity was long-lasting. Illicit traders often have shorter time frames than their counterparts in the legitimate world, as they do not anticipate long-term survival. The masterminds of all three cases more closely resembled entrepreneurs than mere smugglers seeking to evade taxation or regulations. They all established integrated transnational criminal businesses. The participants in Operation Dual Identity imported laborers from abroad to exploit on their farms. The Russian entrepreneurs of Pharmaleaks established numerous websites to enable their cross-border trade, and the criminals of Avalanche provided global support services to ensure effective deployment of the criminal tools they sold.

ILLICIT TRADE REFLECTS CULTURE AND HISTORY

Illicit traders, like their counterparts in the licit economy, reflect the history and culture of trade in their country or region. The traders of Operation Dual Identity continued a centuries-long tradition of illicit flows and routes across the US-Mexican border. However, the commodities involved have evolved. Highly taxed consumer products such as alcohol and cigarettes have been supplanted by people, drugs, and weapons.[42]

The Pharmaleaks case reflects Russia's history as an exporter of raw materials rather than a producer or trader of manufactured goods. There were no Russian domestic pharmaceutical products to sell. Therefore, the Russians who marketed pharmaceuticals online, needing to acquire the medicines abroad, purchased prescription drugs directly from India and China. The Pharmaleaks

businesses, while highly profitable, generated less in revenues than a vertically integrated business, where the supply chain from production through sale is controlled by the same entity. The sale of Chinese counterfeits online, for example, is a vertically integrated business.

The Russian competitive advantage, as seen in this case, is the high level of math and science education in the Soviet and post-Soviet systems; this level of knowledge among the population allows cybercrime to flourish. Unfortunately, the absence of significant legitimate cyber-companies in the Soviet successor states limits the possibilities for licit employment for those with advanced cyber-skills.

Immigration to support trade has created diaspora communities.[43] These communities, as discussed in the historical chapters, aided illicit trade in the past and continue to do so today. For example, members of the Lebanese diaspora in West Africa have played critical roles in the illicit trade that funds Hezbollah.[44] Individuals within Turkish diaspora communities in western Europe have played key roles in the distribution of heroin smuggled through the Balkan route.[45]

CONSUMERS AND MARKETS

All traders need to find purchasers. The criminals of Operation Dual Identity used their personal networks to find customers, thereby limiting their customer base. The most recent stages of illicit trade reveal significant online outreach to find purchasers of illicit goods on an international scale. An important asymmetry exists: a few illicit merchants operating from a few countries may sell to large numbers of buyers around the world.[46]

Illicit entrepreneurs and traders exploit the fact that the global marketplace is now highly competitive as to price, and that consumers are naive about the threats to their personal health and to society from counterfeit and online purchases. Fortunately, the products shipped by Pharmaleaks were generally reliable. In other cases, online purchasers were not so fortunate and were hospitalized or even died from poor-quality pharmaceuticals.

ACCESS TO CAPITAL

To start a business, traders in both the licit and illicit worlds need access to capital. Early-stage capital is hard for all businesses to acquire, and gaining access to capital is even hard for some illicit entrepreneurs and traders, who often originate from marginalized communities. Therefore, they often start small, using one form of illicit activity to generate money for another.

In contrast, well-placed officials often do not need start-up capital. Health, forestry, and labor officials in many countries have leveraged their government positions to illegally market the natural resources under their control. Access to capital is not a challenge for the residents of contested border areas where smugglers have operated for generations. Familial continuity in illicit trade alleviates the need for start-up capital. Successful smugglers pass their skills and their routes from generation to generation, whether on the US-Mexican border, at the port of Marseille, or on the borders of the Ottoman Empire, in the Balkans on the western boundary and in the Kurdish mountain areas in the east.[47]

Illicit traders generate funds through petty illicit commerce, extortion, auctions, stock shares, and more recently, new techniques are used in the online world. Often illicit traders generate capital by exploiting the most vulnerable. Criminals can coerce children to be beggars or compel women and girls to be prostitutes. Traffickers repatriate the profits from this exploitation to build large homes and invest in other businesses.[48]

Two kinds of large-scale petty crime—cigarettes and counterfeits—have been used as *venture capital* for larger-scale illicit activity. For example, Italian investigators revealed that the Camorra, the Neapolitan-based organized crime group, obtained significant profits from sales of pirated DVDs and then reinvested the profits in drugs, the arms trade, and usury.[49]

In the Czech Republic, members of the Vietnamese diaspora community generated venture capital through the low-level illicit cigarette trade. With this initial capital, they were able to become key conduits for imported counterfeit goods from Asia to western

Europe. Capital and connections allowed Vietnamese criminals to advance to the extremely profitable illicit rhino horn trade.[50]

Somalia provides an intriguing example of how working capital can be generated for illicit activity. Pirates there financed their maritime ventures through "investments" from local communities and members of the Somali diaspora community. Once capital was raised, a stock market was established in Haradheere, once a small fishing village, 250 miles from Mogadishu, to finance different pirate expeditions.[51] Auctions were also held to allocate shares in future pirate ventures. This was a far cry from Adam Smith's image of capitalism, although the illicit actors relied on known methods of the legitimate economy.

In the new digital economy, illicit entrepreneurs also generate capital through trade, crowdfunding, and crowdsourcing, as illustrated by the colorful case of a Ukrainian hacker who was eager to revenge himself on a blogger who had unmasked his identity.[52] He crowdsourced Bitcoins from his fellow fraudsters in the Dark Net to buy high-grade heroin off the Silk Road website. Then he had the purchased drugs delivered to the US-based blogger after alerting law enforcement about the drug delivery.[53] Fortunately, the hacker was revealed, and he, rather than the blogger, faced criminal charges.

PERSONNEL RECRUITMENT AND PERSONNEL POLICIES

Illicit businesses need to hire and retain personnel who can perform needed tasks. Foot soldiers for illicit trade are often displaced and smuggled people, as well as youth in areas with high unemployment rates. Employees can serve as couriers of goods and money and as sellers of drugs, counterfeits, and illicit wildlife products.

Organized criminals profile and target individuals and agencies, often investing significant time and even expense to recruit them. To achieve these results, criminal traders need psychological insight, an ability to assess vulnerability, and a willingness to utilize blackmail.[54]

Naive housewives, students, and the long-term unemployed answer online ads and become "money mules" for illicit traders shifting money between bank accounts and countries. Their pay and benefits

are negotiated through web portals. Their success in this activity is usually short-lived, since many are identified and subject to criminal sanctions, as occurred in the Avalanche case.[55]

The training of the low-level personnel of the illicit economy is immortalized in Charles Dickens's *Oliver Twist* in the character of the Artful Dodger, who trains the boys under his command as pickpockets and lowly criminals. On-the-job training has not disappeared. Trafficked young girls are often trained by their traffickers in how to satisfy customers.[56] Drug couriers are taught how to conceal the commodities they transport, and wildlife smugglers are instructed how to disguise the parts they are transporting.

Online training is also provided in launching a successful malware infection campaign. Recruits to cybercrime organizations are taught how to anonymize their identities, ensure security for the operation, and deploy cryptocurrencies successfully.[57]

Illicit entrepreneurs, unlike legitimate companies and traders, do not need to pay attention to labor conditions and worker safety. Major international companies such as Nestlé and other big chocolate companies have been accused of using cocoa from farms with child laborers.[58] Apple was criticized following multiple suicides by workers at the Chinese Foxconn factories that produce its products.[59] Walmart, Gap, and other clothing importers have bought apparel from factories in Bangladesh that failed to ensure worker safety.[60]

By contrast, illicit entrepreneurs can force workers to toil long hours in unsafe conditions without hazard pay. They can compel miners to work without protective equipment. Such labor practices, as discussed in reference to marijuana farms, cut costs and increase the competitiveness of the traders' products. These practices contravene the norms of international law, but in the world of illicit trade there is no expectation of any kind of fair labor treatment and few mechanisms by which workers can object to mistreatment. Moreover, the labor abuses of illicit entrepreneurs who produce counterfeits, mine coltan, or sell illicit timber are rarely confronted by civil society activists seeking better labor conditions for workers. The anonymity of the producers and the absence of transparency in supply chains preclude accountability.

DEVELOPING NEW MARKETS AND FINDING CUSTOMERS

Illicit entrepreneurs pursue many of the same business objectives as their legitimate counterparts—growth, desirable products, and effective marketing. There are important differences, however, in their clients and their products. Illicit entrepreneurs often market items that cannot be sold in legitimate markets, such as sex with minors, child pornography, drugs, banned substances like endangered species, and illegal computer products such as malware, spam, and botnets. Moreover, illicit traders often market in ways forbidden in legitimate markets—by generating spam, coercing buyers, or creating addictions.[61]

Drug dealers may generate customers by offering small quantities that "hook" some customers; newly addicted, they then become loyal clients. At higher levels of the drug trade, major drug traffickers develop new markets and risk mitigation strategies and deploy violence and corruption for maximum effect.[62]

Illicit traders may not have access to Madison Avenue or public relations firms, but they develop marketing strategies suitable to their customer base. Human traffickers find victims and customers through a variety of techniques. Human traffickers in the Northeast of the United States distributed business cards in locales frequented by migrant workers from Mexico and Central America, using coded symbols for sex, with telephone numbers to call.[63] Like their licit counterparts in the upper Midwest, where Hispanic customers are not online, they relied on traditional promotion through handouts.[64]

Pimps in the United States, however, find potential victims not only in malls and at bus stops but increasingly through social media. They display their material success on Facebook, Instagram, and Snapchat in images that specially target young girls, the recruitment pool sought by the traffickers.[65]

Different strategies are used to find customers for sexual services through the internet. Websites such as Craigslist and Backpage have been used in the United States to market trafficking victims and their images. After the state attorneys general cracked down on the sexual service ads of Craigslist, the ads migrated to Backpage.[66] But

Backpage was not the innocent consolidator of ads that it had falsely claimed to be.

Backpage's misrepresentation was revealed quite by accident. Like many companies, Backpage outsourced its computer services to a developing country where tech services could be hired more cheaply. By hiring a Philippine-based company called Avion to handle its sexual advertisements, Backpage could claim that it did not control sex-related ads. Backpage officials falsely believed that the location of Avion's computer system outside of the United States gave it security from scrutiny.[67]

This profit-making strategy was revealed when Filipino investigators in a totally unrelated case involving irregularities in real estate sales, seized Avion's computers. Those computers were sent for forensic analysis to the United States, where the investigators for the real estate case discovered files related to the sex trafficking of minors that connected Avion's files to Backpage.

The computer files revealed that Backpage had Avion "lure advertisers—and customers seeking sex—from sites run by its competitors."[68] Avion, while under contract to Backpage, helped create new advertisements, sometimes editing the content to hide the minor age of the girls offering sexual services and thereby disguising the criminal element of the ad.

The sexual advertisements placed on Backpage generated good profits for the pimps but massive profits for the corporate owners of Backpage.[69] Growth was at a rapid rate possible only in the tech world. Backpage revenues from its prostitution ads were $5.8 million in 2008, and that grew to $135 million in gross revenue in 2014, with 82 percent profitability. Continued growth is anticipated.[70] Prior to the arrest of Backpage's CEO in late 2016, the attorney general of California reported that Backpage's internal reports showed that from January 2013 to March 2015, 99 percent of its income was "directly attributable" to its adult advertising and more than $51 million of its revenue was derived from California in that period. Backpage's founders were each rewarded for that profitability with a $10 million bonus in 2014.[71] In early April 2018, the combined efforts of different federal law enforcement agencies resulted in the

seizure of backpage.com by the government.[72] Shortly after the seizure, seven top officials of Backpage were arrested after a ninety-three-count indictment was issued by a Phoenix grand jury, alleging conspiracy, facilitating prostitution, and money laundering. The indictment alleged that Backpage had laundered $500 million in prostitution-related revenue since 2004 and that several young girls who responded to Backpage ads were murdered.[73]

GROWTH STRATEGIES

Many start-ups fail in the legitimate economy. To survive in ever-changing markets, both licit and illicit businesses must be responsive to a challenge for sellers in both worlds—consumer demand. Counterfeiters trading in outdated or unappealing fashion can lose significantly, just as happens to legitimate retailers when their products do not appeal to purchasers. Traders in both the licit and illicit sectors can grow fast if they create a monopoly or achieve market dominance.[74]

To achieve growth online criminals must run streamlined, often lean and automated operations. Whereas trade for millennia has been based on interpersonal relations, in cyberspace criminal traders rarely, if ever, meet in person.[75] Their contacts are often established and maintained through the forums and communications of the Dark Web.

Corruption is a tool that can facilitate growth. Illicit entrepreneurs and traders avoid regulations and taxes and use corrupt officials to ensure that their commodities are purchased. Moreover, corrupt officials can help eliminate the competitors of illicit traders by selectively applying regulations. Corruption can also ensure that particular illicit businesses are not investigated.

In the online world, as in the tangible world, providers must satisfy customers to grow. In the Dark Net, as on legitimate sites such as Amazon, there are rating systems for purchases. Customers can evaluate their sellers and leave comments to advise other buyers. "The administrators take a 5–10% cut of each sale and set broad policy. . . . They pay moderators in Bitcoin to run customer forums and handle complaints." But in this illicit world, there are those

seeking to game the system. Vendors such as Mr420 offer to provide fake reviews.[76]

DIVERSIFICATION

Many businesses, in both the legitimate and illegitimate worlds, seek to diversify to ensure that they are not dependent on sales of one particular commodity. Illicit actors shift between several forms of illicit trade to optimize profits and reduce risk. Economies of scale are gained by working in diverse sectors simultaneously, achieving what is referred to as "convergence": multiple forms of crime being committed by the same groups.[77] The criminals use the skill sets they obtained in one area to enter new types of illicit trade that will prove profitable, deploying a strategy well known to the legitimate business community.

Diversification can occur rapidly because those engaging in illicit trade are more flexible and adaptable than the bureaucratic structures that oppose them. Nonstate actors can seize on market opportunities as they find them, and they can shift quickly to new income sources when revenue streams are curtailed. Mexican crime groups, for instance, have diversified from the drug trade into human smuggling and the sale of energy products.[78]

Europol has also noted increasing diversification among many European-based criminals who have recently expanded into human smuggling. They estimate that approximately five thousand international organized crime groups operate in the European Union, and that over one thousand of these are so-called poly-crime groups deriving their profits from multiple criminal activities.[79]

The criminals behind Operation Dual Identity also diversified by engaging in multiple criminal offenses, including human smuggling, identity theft, marijuana production, drug trafficking, home invasions, and even murder.[80]

Terrorist groups have also diversified the illicit commodities they trade. The Colombian terrorist organization FARC, known for its drug trafficking, acquired a new illegal funding source before the peace talks with the Colombian government—gold. Gold extraction

combines less risk with higher profits, helping to explain why over 80 percent of the gold extracted in Colombia is now mined illegally.[81] FARC's recent revenues from the illegal gold trade exceeded its revenues from the drug market. Yet FARC's business practices were transferred to this new commodity. In gold mining, as in the drug trade, intimidation, violence, extortion, and exploitation of indigenous populations are the general operating principles. Furthermore, both products harm the environment: the drug trade causes soil depletion and destruction through the use of toxic chemicals, and the illicit gold trade puts dangerous chemicals in the water and the process of extraction is harmful to human life.[82]

The terrorist group ISIS (Islamic State) sold oil but also profited from kidnapping, extortion, and the sale of contraband and antiquities.[83] Diversification has benefits beyond the financial. Pernicious nonstate actors can confound law enforcement by shifting commodities and locales, thereby reducing risk.

Criminals trading in natural resources, as we saw with the rhino horn trade, have been able to expand their businesses rapidly because they are not new to illicit commerce. Many environmental criminals were previously engaged in corruption, counterfeiting, and drug, arms, and human trafficking, as well as cyber and financial crime.[84]

Online criminals, as mentioned previously, may market different commodities in succession, as did the criminals behind Pharmaleaks. Before they entered the illicit pharmaceutical business, they had traded in child pornography. Once they lost the ability to charge for their medicines, they moved into selling fraudulent antiviral software.[85]

Online criminal markets in the Dark Net also diversify. The same site may sell drugs, weapons, malicious computer software, and tech support to deploy the pernicious tools they market. Assassins for hire are also offered on the Dark Web.[86]

STRUCTURE AND DECISION-MAKING

Italian hierarchical crime groups, such as the Cosa Nostra, Camorra, and 'Ndrangheta, are among the most studied criminal organizations in the world.[87] To survive over an extended time they have

focused on internal codes of ethics (being men of honor), respect for the chain of command, effective deployment of violence, and their reputations. As Diego Gambetta has written in *The Sicilian Mafia*, the roots of that organization lie in its certification of horses traded in the nineteenth century in an environment of distrust.[88]

Newer criminal organizations are less hierarchical than the Mafia, and illicit traders often operate with network structures. They therefore have greater flexibility than many legitimate companies, which are more bureaucratic and have more formalized decision-making. This structure enables new illicit traders to respond rapidly to emerging opportunities. This is why criminal traders, once they have depleted the natural world of plants or wildlife in one locale through over-exploitation, simply take illicit trade to another locale. The poaching of elephants, for instance, is being moved to ever more remote and conflict-ridden regions of Africa as the elephants are killed off.[89]

Different structures are found among online illicit traders such as Avalanche, which was "structured much like an IT company, with programmers, web designers, system administrators, and other roles found in legitimate enterprises." The Avalanche network survived as a business, despite increasing law enforcement scrutiny over time, because it had good leadership, successful advertising, innovative products, and good customer support.[90]

To develop, illicit businesses need strategic plans or visions for growth. Research done by cyberspecialists who have penetrated online criminal communities often reveals the transmission of strategies from the real into the virtual world. Therefore, it is hardly surprising that their plans include product development, improved logistics, development and maintenance of supply chains, and incorporation of new technology.

STRATEGIC ALLIANCES

Strategic alliances often facilitate growth in the illicit as in the licit world. Alliances in the illicit world often link highly diverse groups that transcend significant ethnic divides, geographical borders, and

even political conflicts. For example, Armenians and Azeris, sworn enemies, together extorted markets in Russia. Israelis collaborated with Bedouin human smugglers.[91] Taiwanese and mainland Chinese cybercriminals operate out of Indonesia to target Chinese speakers.[92]

Legitimate multinational trading companies establish offices and franchises globally, providing broad geographic reach, but illicit alliances, outside the cyberworld, are not often as global and are more task-focused. For example, British investigators reported on the cooperation of Jamaican and Turkish drug traffickers in the United Kingdom.

In the Dark Web, where Tor or other software allows one to enter anonymously, traders may not know the country of residence of their business associates.[93] Compounding this anonymity are digital currencies, which further obscure the identity and nationality of sellers and purchasers. In a 2014 malware case successfully prosecuted by the US Justice Department, through cooperation with foreign law enforcement, the diverse online traders were Algerian, Bulgarian, and Russian, and some resided in the United Kingdom.[94]

PRODUCT DEVELOPMENT

Legitimate companies must invest in product development if they are to grow. But this is not the case with illicit traders who prey on the products of others, whether it be fashion design, pharmaceuticals, or electronic parts.[95]

Innovations in science and technology are targeted by illicit traders at the conception stage but are particularly vulnerable to expropriation when they reach a certain economic threshold. The loss of future products is especially costly to legitimate businesses, and particularly valuable to illicit traders, as they can exploit the new technologies they acquire at minimal cost. This problem has been identified in diverse Western countries, and some of the thieves of these products are believed to be state-supported criminals.

American law enforcement has identified product theft as a key concern, particularly in such tech havens as California. Starting in 2010, Sweden also initiated a number of internet-related cases for

copyright infringement through file-sharing and crimes against industrial property rights with the help of the internet.[96] Sometimes thieves copyright stolen product designs in China, precluding their future sale in the large Chinese markets.

The dynamism and ingenuity of the synthetic drug market is revealed in the official statistics of the United Nations Office on Drugs and Crime. Between 2009 and 2016, 106 countries and territories reported the emergence of 739 new psychoactive substances.[97] The rise of the synthetic drug trade is an excellent example of illicit entrepreneurship. Synthetic drugs have seen massive growth in recent decades, reflective of the importance of technology to the growth of illicit trade. Growth has been seen in ecstasy, amphetamines, methamphetamines, and other synthetically produced drugs such as fentanyl. The trade in synthetic drugs, often referred to as "designer drugs," also reflects the trend in licit trade of premium prices being paid for fashionable consumer items.[98] In markets, lower prices are paid for items derived from agricultural labor, and this is true whether one is consuming food or drugs derived from poppies, opium, or marijuana plants.

Synthetic drugs have the additional advantage of enabling traffickers to move production closer to consumers, thereby decreasing transport costs and reducing the possibility of detection along long supply chains. Shortening the distance from production to distribution also reduces the costs of corruption, as there are fewer people to bribe before the product enters the market. Synthetic drugs such as ecstasy and crystal meth are now available in almost all markets, but striking growth rates have been recorded in Asia, Australia, and the Middle East. Captagon (a psychostimulant) is king in Saudi Arabia.[99]

Beginning in the mid-2000s, synthetic drugs began to be produced in the poorer, traditional drug cultivation countries, such as Myanmar. One synthetic drug seizure there in 2015 yielded 27 million pills.[100]

New products that target computers, such as malware, botnets, and Trojans, are among the areas of greatest growth in illicit markets.[101] They are one area in which criminals actually invest their own resources to develop new products for sale, franchising, and leasing.

QUALITY CONTROL

Many legitimate corporations, especially in markets where citizens have rights, devote significant attention to quality control in order to prevent harm to brand reputation or to prevent damaging lawsuits and fines. Television and online ads in the United States alert accident victims that they too can sue Toyota for accidents relating to defective car seat belts or seek damages from pharmaceutical companies for harmful drugs that have been placed on the market prematurely.[102]

Quality control is not a significant concern of many illicit entrepreneurs or traders who sell counterfeits, as they do not depend on brand reputation or repeat business. Moreover, if consumers take action for personal injury, the copyright holder rather than the counterfeiter will often be sued for inferior products.

Many illicit entrepreneurs do not care if they manufacture or sell defective infant formula, pesticides, medicines, and even baby toys manufactured with harmful ingredients or under very unsanitary conditions.[103] Many of the most harmful products are destined for markets with few legal regulations on product safety, such as the states of the former Soviet Union or the countries of Africa. In Soviet successor states, sales of toys produced with toxic components, disguised and sometimes sold under the labels of major corporations, are marketed to unwitting customers.[104]

ADDRESSING COMPETITION

Illicit traders have certain advantages in dealing with competitors, as they can more readily use extralegal means such as corruption, collusion, and price-fixing. These advantages help them limit competition, achieve market dominance, and fix prices.[105]

Illicit actors often threaten or use violence to ensure compliance by their suppliers, sellers, or middlemen. Violence is particularly pronounced in the drug trade, where groups battle over control of territory and routes. Drug traffickers routinely use threats and actual brutality to ensure that customers pay in a timely fashion.

Human trafficking is accompanied by violence as pimps try to take over rivals' girls. Despite the idea that online marketplaces reduce violence, the online world is not violence-free, and force is used or threatened against competitors or those who fail to make payments or produce goods.[106]

In Russia and many other post-Soviet states, a practice known as *corporate raiding* has developed to eliminate competitors; it operates very differently from the Western concept of the same name. Competitors may be targeted through corrupt and violent means, and organized crime, complicit legal officials, and fraudulent documents are deployed to deprive owners of their assets.[107]

LOGISTICS

Logistics experts are needed by both licit and illicit traders. For those in the licit world, logistics considerations include the security of supply chains and the costs and efficiency of delivery. Amazon has rapidly grown to be the eighth-largest retailer in the world because it combines online accessibility with attention to prompt and accurate delivery.[108]

Illicit traders share some of these business tenets of the legitimate world, but not all. They need to ensure delivery of their product to market. But they do not want transparency of trade or cargoes that can be tracked and traced. They seek locales where they can evade detection, bribe officials, and avoid taxes and regulations. They often rely on fake documents such as passports, driver's licenses, and ID cards to help facilitate deliveries. A whole service industry of facilitators has developed to produce these illegal documents that support illicit trade.

Like the sellers of licit goods from the internet, the illicit traders rely on numerous small packages to distribute their goods. Deliveries of counterfeit electronics, medicines, and drug packets arrive at recipients' homes by post and specialized delivery services. The postal service is particularly favored because local law enforcement in the United States does not have jurisdiction over its deliveries. Breaking down shipments into small, discrete packages makes it much more

difficult for law enforcement to detect the illicit trade.[109] Yet it also requires that illicit traders make many individual sales to achieve a profit. It is an Amazon approach to the illicit economy.

TRANSPORT

Illicit commerce travels in many different ways—by land, sea, and air. It moves with legitimate shipping and trucking companies, or its shippers operate in the world of dark commerce, ready to serve customers without asking questions. Smuggled products are even moved into highly regulated ports when criminal shippers and recipients use ingenuity and technology to aid their logistics. Corruption is key to many illicit deliveries.

Many historic trade routes have been repurposed to serve illicit traders. The ancient Silk Road now serves the northern route for the heroin trade out of Afghanistan.[110] The route that Marco Polo helped initiate between Italy and China has been repurposed to accommodate a massive counterfeit trade into Italy.[111] The slave trade route between West Africa and Brazil is now employed by the drug traffickers of Latin America and Brazil to move cocaine into Europe. The historic trade passage between East Africa, Yemen, and the Indian subcontinent is now the locale for a converging drug, wildlife, and counterfeit trade.[112]

Illicit trade need not travel along obscure or complex routes. Significant illicit shipments can still be moved into major ports through subterfuge and by hacking into the computer system of the port authority, revealing the innovativeness of some smugglers. A Suriname-based group smuggled containers' worth of drugs into Dutch and Belgian ports. The drug-filled containers were dropped at the port and then stolen before inspection. After the containers were emptied, they were returned. The drug smugglers could achieve this feat by retaining sophisticated computer security specialists who hacked into the ports' computers.[113]

The flexibility of crime networks and their absolute ruthlessness in pursuing profits are responsible for human smugglers packing many people into boats that are often not capable of staying afloat.

This practice explains the high mortality rate of contemporary human smuggling.

Legitimate shipping companies and postal services can be both witting and unwitting shippers of illicit goods. Online sales have fueled the opioid epidemic in the United States as customers buy through both the World Wide Web and the Dark Web. The ordered drugs are often delivered by American and foreign postal carriers. Finding illicit items is difficult under existing legislation, which fails to require foreign shippers to provide advanced electronic data concerning their contents and intended recipients.[114]

Legitimate global trade in tangible goods thrives where there is first-class infrastructure, communications, and commercial systems. Illicit trade often passes through many locales that are of secondary importance to global traders, such as Naples in Italy, Vladivostok in Russia, Karachi in Pakistan, Dubai in the United Arab Emirates, Cape Town in South Africa, and Miami, Florida. These are noted ports, but they are not on the "A" list of global commerce.

Poor countries, with limited enforcement capacity and high levels of corruption, have very low scores on the Illicit Trade Environment Index. These locales are key to illicit trade. It is hardly surprising that the illicit wildlife and timber trade flows through Laos, Myanmar, Vietnam, Cambodia, and Indonesia, countries with the poorest scores in Asia.[115]

Illicit trade hubs share certain attributes. They are often close to centers of organized crime, and they have high levels of corruption and limited regulatory authority. In addition to these hubs, free-trade zones (FTZs) have become critical to the movement of illicit trade, as they lack effective regulation.[116] In these murky environments, it is possible to hide the illicit in the licit. Shippers and officials surreptitiously change shipping invoices to disguise the movement of illegal commodities and avoid taxation. According to the International Chamber of Commerce:

> FTZs have provided a mechanism for counterfeiters to move illegal fake products around the world. Increasingly, counterfeiters use transit or transshipment of goods, through multiple,

geographically diverse FTZs for no other purpose than to disguise the illicit nature of the products.[117]

The Jebel Ali free-trade zone in the UAE is a major hub of the illicit trade in cigarette and counterfeits, including pharmaceuticals.[118] Through this zone move billions of illicit "white" cigarettes destined for European markets.[119]

Yet not all FTZs are located in countries that rate poorly on Transparency International's Corruption Perception Index. For example, Singapore is rated number six in the world for its low level of corruption, yet it has a different standard for its FTZ because of its eagerness to facilitate trade.[120] In its FTZ, as the *Economist* Intelligence Unit reports, "Neither Singapore Customs nor any other government authority is a consistent presence."[121]

THE ROLE OF SUBTERFUGE: ABSENCE OF TRANSPARENCY

Much human ingenuity goes into devising the disguises used to hide the contents of illegal packages. Shipments of cocaine are packed inside fish fillets heading to New York and inside pineapples headed to Spain.[122] Oriental rugs are interwoven with opium and smuggled into the Manchester airport in the United Kingdom.[123] In Zimbabwe, officials found more than 15 million cigarettes hidden within four train cars allegedly shipping full loads of timber.[124]

Illicit shipments often travel circuitous routes. For example, counterfeited goods shipped from Bangladesh and China into Europe "passed through the ports of Antwerp and Hamburg, where, thanks to the collaboration of Customs officers, the goods were unloaded and temporarily stored in warehouses. The goods were then redirected to Italy," a distribution hub for counterfeits. Transfers from the port of entry were made by Air China cargo flights headed for Milan, Brescia, and Rome.[125] This case reveals the centrality of corruption to illicit trade, even in western Europe.

Bulk shipments of drugs, timber, or elephant tusks require obfuscation. These products are often taken, with minimal oversight, through multiple trans-shipment points, particularly free-trade

zones, and locales with high degrees of corruption. For example, when shippers of an illicit cargo of ivory tusks directed the shipment through airports in West Africa, the Middle East, and then several in Asia before reaching its final destination in Thailand, they made it very difficult for law enforcement to identify them as its senders.[126]

Combining licit and illicit goods often facilitates delivery. Such combinations can be as small-scale as landscaping companies taking ferns and rocks from Shenandoah National Park to plant in clients' gardens along with plants legally obtained from nurseries. Traders of Civil War relics combine legally sourced items with those dug up illegally from government-preserved battleground sites.[127] Ivory horn travels in a shipment with legitimate trade items such as seaweed, cashew nuts, and seashells.[128]

Iranians' efforts to circumvent sanctions for their nuclear weapons program led to massive subterfuge. A German and Turkish investigation conducted between 2010 and 2012 identified nine hundred shipments of smuggled cooling devices and other apparatuses directed to five separate shell companies established by Iranians in Istanbul. Eight hundred of these shipments originated from India, and an additional one hundred came from Germany. The Istanbul-based front companies misidentified the cooling devices as valves and plumbing fixtures when they reexported them to Iran, thereby hiding the ultimate purchaser of the goods—Iran's nuclear program.[129] North Koreans have engaged in similar subterfuge for decades to build their nuclear program.[130]

The Use of Technology: The Web, the Deep Web, or the Dark Web

Traders must incorporate new technologies to stay competitive. Pernicious nonstate actors have been among the earliest and most successful adapters of new online technology. They use the searchable World Wide Web, the Deep Web (the part not accessible to conventional search engines), and the Dark Web, and some function in all three elements. The Dark Web, at five hundred times the size of the surface World Wide Web, provides a vast territory

in which massive amounts of information can be stored and made available only to a select group of users.[131] This is very conducive to its criminal abuse.

Online platforms and social media are also abused to allow individuals to buy opioids, counterfeit pharmaceuticals, and illicit wildlife products.[132] The new technology is a force multiplier for the growth of illicit trade, as seen in all three stages of illicit trade. According to a 2015 *New York Times* report:

> Ordering illegal drugs from China is as easy as typing on a keyboard. On guidechem.com, more than 150 Chinese companies sell alpha-PVP, also known as flakka, a dangerous stimulant that is illegal in the United States but not in China, and was blamed for 18 recent deaths in one Florida county.[133]

Just as false news can be disseminated through Facebook because it lacks appropriate filters to weed out erroneous communications, neither can Facebook control the posts that facilitate illicit trade. Social media has enabled arms sales to conflict-ridden areas where terrorists operate, such as Libya, Iraq, Syria, and Yemen. An analysis of Libyan Facebook accounts between September 2014 and April 2016 "documented 97 attempts at unregulated transfers of missiles, heavy machine guns, grenade launchers, rockets and anti-matériel rifles, used to disable military equipment." Facebook is hosting a virtual weapons bazaar, as are other social media platforms. Some of the weapons offered are those provided by the United States to Syrian rebels.[134]

Cybercriminals choose to operate through the World Wide Web, the Deep Web, or the Dark Web based on the visibility they want for their products, the volume of sales they seek to generate, and the level of criminality associated with their products. Therefore, products that command much more attention from law enforcement, such as narcotic drugs, child pornography, and malware, are more likely to be sold in the Dark Web. Counterfeits, even including such items as medicines, are more likely to be sold on the World Wide Web.

Affirming the criminal intent of purchasers in the Dark Web is research conducted in 2014 that determined that "four out of

five Tor hidden services site visits were to online destinations with pedophilia materials." Too many have viewed the Dark Web as a haven for privacy without understanding the extensive criminal abuse present there.[135]

In all online environments, profits can be high and products can be sold with a range of prices. In the World Wide Web and the Deep Web, illicit sellers seek an image of legitimacy and often provide options such as credit card payment processors and related payment alternatives such as debit cards, wire transfers, and digital currencies. All these traditional measures reassure customers.[136]

Sales volumes and profit margins can be significant in both the Web and the Dark Web; therefore, it is neither the price nor the number of consumers that is decisive in determining traffickers' marketing strategy. If businesses want customers to make speedy decisions, they use the Web rather than the Dark Web. They may even use spam to direct buyers to their website.

Sales in the Dark Web are based on trust, and building trust takes time.[137] Dark Web purchasers necessarily operate more slowly than those on the Web, since purchasers must obtain the appropriate certifications to acquire entry into the closed communities where the illicit trade occurs. To do this they must learn the required lingo of those who belong to these criminalized networks.[138] It is only logical, if you're buying quantities of synthetic drugs or searching for a kidney, that you would not make a quick decision because you want to be sure you trust the seller. Likewise, the sellers do not want to be entrapped by law enforcement, as happened to Dread Pirate Roberts and other large-scale illicit sellers in the Dark Web.

Corporate Social Responsibility

Corporations in the legitimate world have adopted policies to address the well-being of communities and the environment. This broad concept can include support for nonprofit social, community, and artistic groups as well as concerns about the sourcing of their products to minimize harm to the environment.[139]

Nonstate actors do not show respect for the environment; moreover, many are at the forefront of its destruction. Yet many of nonstate organizations are also at the forefront of service provision where the state is absent. They use proceeds from their criminal activity to ensure their future impunity by persuading citizens not to see them just as a negative force in the community. The *Yakuza* (members of transnational criminal organizations in Japan), after the 1995 Kobe earthquake, provided aid in the absence of state assistance. Drug traffickers offer services to those living in Brazil's *favelas*.[140] FARC, at its height, was a major provider of benefits in Colombia, including schools, medical clinics, and infrastructure support. Terrorist groups in other regions of the world also provide services to their communities, enhancing their legitimacy.[141]

Laundering Profits and Illicit Financial Flows

In a 2013 study of fifty-five developing countries by Global Financial Integrity (GFI), economists estimated that illicit financial outflows—most in the form of misinvoicing of trade—amounted to $947 billion in 2011, representing some 3.7 percent of these countries' combined GDP. Abuse of the trade system is at the heart of the asset-stripping of some of the world's poorest countries.[142]

Multinational institutions and private banks have facilitated this wealth transfer. Loans provided for national development have been siphoned off by corrupt leaders—kleptocrats—because lenders have provided inadequate oversight of the funds. Massive sums have been stolen from Nigeria in the decades since independence. Over $1 billion was allegedly stolen from the Malaysian national treasury by Prime Minister Najib Razak, who deposited much of this money in international banks around the globe, triggering investigations in many countries.[143]

The citizens of Equatorial Guinea, Turkmenistan, and Ukraine have remained impoverished while their national assets are found in the bank accounts of their leaders in many financial centers around the world.[144] The revelations of the Panama Papers and the

Paradise Papers disclose the pervasiveness of this practice among global elites.[145]

The hundreds of billions of dollars gained through the global illicit trade in drugs, humans, weapons, and other activities often enter the legitimate economy. The money is laundered through banks, wire transfer businesses, trade-based money laundering systems, currency exchange businesses, *hawala* traders (the system of underground banking based on trust), and, most recently, cryptocurrencies (currencies that exist only in the cyberworld and are not backed by any government).[146] Money from illicit trade is invested in land, expensive homes, cars, and other businesses, some of them legitimate. Real estate has been purchased with laundered funds in many locales on all continents.[147] One lucrative Turkish-run human trafficking network in the Netherlands used its victims as couriers returning the profits of the Dutch-based trade to build nightclubs in Turkey.[148] In the United States, in six jurisdictions with suspected high rates of money laundering, the financial intelligence unit of the United States, the Financial Crimes Enforcement Network (FinCEN), found that about 30 percent of real estate purchases involve a beneficial owner or representative who had previously been the subject of a suspicious activity report.[149] Profits from the fentanyl trade are laundered into Vancouver real estate by Chinese gangs.[150]

Well-established banks have moved billions in drug profits through their institutions, some of it to offshore locales.[151] Legitimate financial institutions transferred funds from illicit commerce particularly after the 2008 financial crisis, a period when banking standards declined and financial institutions were in survival mode. The multimillion-dollar penalties imposed on Citibank, HSBC, Wachovia, and Deutsche Bank indicate the key role that some bankers have assumed in facilitating illicit commerce.[152] Illustrating a recurring theme of this work—the convergence of the licit and illicit economies—this kind of cooperation is true not just of banks but also of legitimate companies.

In 2000, a group of top American companies, including Hewlett-Packard, Ford, and Whirlpool, were informed by the US Justice Department that they were implicated in a money-laundering

scheme called the "Black Market Peso Exchange."[153] Washing machines and cars were bought with drug profits without the knowledge of the sellers and then shipped to Colombia for resale. Purchasers would pay using pesos, thereby completing the cycle of converting the dollar currency proceeds earned by drug traffickers into usable assets.[154]

Financial havens, such as in Panama, have accepted funds from known traffickers aided by professionals. As the game on the website of the Panama Papers states, "Welcome to the secret world of offshore. Your goal is to navigate this parallel universe and hide your cash away. Don't worry! Lawyers, wealth managers and bankers are there to help you."[155] The documents of the Panama Papers revealed that drug traffickers and political leaders used the same law firm to hide their assets.[156]

Wire transfer businesses have moved the profits from both drug and human trafficking. In France, the leading French counter-trafficking official in 2001 implicated Western Union in the movement of money to eastern Europe by sex traffickers.[157] Arizona, a key border state for the illicit movement of drugs and people, took action against Western Union. Arizona's former state attorney general testified, "Western Union is by far the largest provider of illicit money-movement services." In 2010, Western Union entered into an agreement with the state of Arizona, paid a $94 million fine, and was placed under monitors.[158] But the problem did not end. In 2017, Western Union paid a $586 million fine in the United States for moving money resulting from fraud, drug sales, and human trafficking.[159] The large fines have sometimes been perceived as just "the cost of doing business." The problem has been transferred to the cyberworld. In Europe, intercepted email of criminals operating online revealed that they exchanged virtual currency into state-backed currencies by means of Western Union.[160]

Investigations by the tax authorities of Colombia revealed that significant drug profits were moved offshore to Panama by means of trade-based money laundering. These transfers were facilitated by significant corruption in the Colombian customs service: drug cartel members had infiltrated regional offices that allowed the

certification of exports to Panama. The products might be coffee or some other commodity for which an exaggerated value was attached to the invoice.[161] Payment would then be made for the amount in the overvalued invoice, justifying the transfer of significant sums overseas. "Over-invoicing" is a key element of trade-based money laundering, as it allows the movement of funds far in excess of what is needed to pay for what has actually been moved. Corruption at the receiving end, as seen in the Panama Papers, affirms that trade-based money laundering often requires corruption in both the source and recipient countries. Trade-based money laundering reveals the centrality of trade abuse to the movement of funds out of the developing world and the laundering of ill-gotten gains of criminals and terrorists.[162]

In the cyberworld, money is increasingly laundered through cryptocurrencies. Intercepted communications of criminals in the Netherlands have revealed that many financial companies are used by crime groups to launder their money. Although some criminals still rely on payments in traditional currencies such as PayPal and MoneyGram, others are linked to cryptocurrencies such as FBTC Exchange, WebMoney, Bitonic, and xmlgold.eu. WebMoney, founded in Russia in the late 1990s but now in use globally, works in traditional currencies as well as gold and Bitcoin by means of an e-wallet (a digital mechanism to secure one or more currency purses). Prepaid cards and vouchers are also widely employed by online criminals as well as in underground banking.[163]

Criminals are holding their money in cryptocurrencies such as Bitcoin, a sensible decision with Bitcoin rising in value. When he was arrested, Alexander Cazes, the alleged creator of the Dark Web site AlphaBay, according to his indictment had "over $5 million in Bitcoin, $1.8 million in Ethereum, and $760,000 in Zcash, in addition to conventional bank accounts, valuable cars and expensive real estate properties."[164]

Revealing the scale of the money laundering through cryptocurrency was the 2017 arrest of Alexander Vinnik, a thirty-seven-year-old Russian, in Greece on an American arrest warrant for having laundered $4 billion through his Bitcoin exchange.[165]

Conclusion

Illicit business organizations often flourish in countries where the rule of law is weak and corruption is high. Yet countries with greater adherence to the rule of law and effective law enforcement are not exempt from the challenges posed by illicit businesses. Many associate "offers you can't refuse" only with the drug trade or with developing countries, but illicit traders and entrepreneurs also operate successfully in the G-7, the most affluent countries of the world. In developed countries, however, illicit commerce is less central to the national economy and represents less of the country's GDP than in the developing world.

The licit and the illicit are not distinct, and they intersect more often than many realize. This is true in both the real world and the virtual world. Legal and illegal products traverse the same supply routes and are often sold in the same marketplaces in the real world and in the cyberworld. In the cyberworld, more than six hundred cloud repositories, including those of Amazon, Google, and Groupon, have hosted malware and other malicious computer products. As many as 10 percent of these repositories have been tainted by malicious and illicit products.[166]

The rapid escalation of illicit trade and money laundering in the virtual world is assured, made all the more so by the rise of cryptocurrencies, many of them created with the deliberate intention of supporting criminal activity.[167] There is little to stem the growth of illicit cyber marketplaces at present. Many legitimate sales platforms facilitate the sale of illicit goods and people, and the private sector, which controls this technology, all too often prioritizes profits over human life and the sustainability of the planet.

Traders move rapidly in the cyberworld, whereas efforts to disrupt their activities move more slowly, often hindered by state-based laws crafted for an era of tangible commodities. Therefore, in the coming years we will face an even more asymmetric threat as harmful cyber-trade escalates and state and transnational capacity to counter it remains far behind.

The historical transformation of illicit trade, however, also provides new opportunities, because dark commerce operates through

private companies and leaves its traces in the data of financial institutions. Large-scale data analytics, when done well, reveal patterns of criminal activity in cyberspace and expose illicit networks, making it possible for law enforcement to pursue cases without invading privacy or violating individual rights. As long as the malicious use of the Dark Web and cryptocurrencies does not prevail, new ways may be found to contain illicit commerce in the future.