

## BACKGROUND PAPER

## Digital Dividends

# Do Digital Technologies Facilitate Illicit Financial Flows?

**Tatiana Tropina**

*Max Planck Institute for Foreign and  
International Criminal Law*

This background paper was prepared for the *World Development Report 2016 Digital Dividends*. It is made available here to communicate the results of the Bank's work to the development community with the least possible delay. The manuscript of this paper therefore has not been prepared in accordance with the procedures appropriate to formally-edited texts. The findings, interpretations, and conclusions expressed in this paper do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

# Do Digital Technologies Facilitate Illicit Financial Flows?

Dr. Tatiana Tropina

---

## Summary

The emerging concept of illicit financial flows has become a crosscutting issue on the international agenda in recent years. This umbrella term refers to money illegally earned, transferred, or used. With the development of digital technologies, the use of information and communications networks as a tool for facilitating illicit financial flows is rising as one of the key challenges in tackling the problem of the movement of illegal funds.

Digital technologies facilitate illicit financial flows at each stage, be it earning money illegally, transferring illegal funds, or using them. There are several areas where clear links between technology and illicit financial flows can be established.

### ***Acquisition of money***

In addition to the creation of the underground illegal markets of cybercrime and cyber-related crime, digital technologies facilitate the migration of traditional organized crime online and provide a number of opportunities for fraud, corruption, tax evasion, and other criminal activities.

### ***Money transfers and use***

New digital tools for money transfers, such as online and mobile banking, electronic payments, cryptocurrencies, e-commerce providers, and online gambling services, especially if they are combined, provide a countless number of opportunities to distance money from illegal sources of profit or to illegally transfer money from legal sources. New forms of doing business online, and the digital economy as a whole, facilitate the transfer of illegal profits and the aggregation of illicit funds in offshore accounts, and their placement in fake e-commerce companies and offshore online businesses.

Digital technologies could also be considered as a tool to tackle the problem of the illicit financial flows. They can serve as a source of empowerment and transparency, and could be used in investigations, detection, and disruption of the illegal money transfers.

Technology as a tool for tackling the problem of illicit financial flows can complement, but will never substitute for, proper legal frameworks, international cooperation, and public-private collaboration. The problem of illicit financial flows requires implementation of a complex set of measures, which have to include technological, legal, and organizational components. Furthermore, the use of digital technologies in the investigation of illicit financial flows should always be balanced with human rights and safeguards and take into account privacy issues.

## Introduction

The emerging concept of illicit financial flows has become a crosscutting issue on the international agenda in recent years. Illicit funds from organized crime, corruption, and tax evasion, which are moving across borders, pose a big challenge to the security and stability of economies around the globe, with an especially devastating effect on developing countries. There are no reliable estimates of illicit financial flows. According to some assessments, nearly US\$1 trillion of illicit funds shifts out of emerging markets and developing countries annually (Global Financial Integrity 2014; ONE 2014). There is, however, no implicit proof of reliability of such estimates.

Corruption, tax evasion, organized crime, the drug trade, and human trafficking, and many other forms of crime as well illicit financial flows associated with these illegal activities pose significant

interconnected threats to poorer states. They considerably reduce already limited domestic resources available and decrease tax revenue that is needed to fund critical poverty-reducing programs and infrastructure (World Bank 2015). Indirectly, they also negatively impact investments, fuel excessive inflation that leads to higher interest rates, facilitate the creation of unstable economies, threaten security, promote inequality, and undermine the rule of law. These concerns increased the pressure from civil society and other actors to take action against illicit financial flows and brought this issue to the center of the development agenda.


The issue of illicit financial flows is not new; however, in the last few decades the increasing dependency of society on information and communications networks is changing the landscape of this problem. The growth of digital operations in legitimate markets is one of the critical drivers for economic development. However, as markets and trade have always attracted criminals seeking benefits from illegal activities, digital networks have become a key enabler for the new forms of earning and transferring illicit funds and a facilitator for many traditional ways of illicit financial flows. Criminal activity has been evolving in parallel with society's use of information networks, reacting to every technological development with new approaches to gain profits and hide them. The borderless nature and decentralized architecture of the internet, combined with a complex dynamic ecosystem of the digital economy, poses new challenges to governments, industry, and civil society in tackling the problem of illicit financial flows.

Due to the relative newness of the problem, there is still a lack of research on the issue of digital technologies as an enabler and facilitator of the illicit financial flows. This paper aims to provide insights into the nexus between information technologies and illicit financial flows and to show how technology is helping to earn, transfer, or use funds illegally. Since there have been relatively few studies in this field, by reviewing as many examples of the use of technology for facilitating illicit financial flows as possible, this analysis seeks to provide a context for further studies in this area.

The paper follows the outline presented in table 1, which summarizes both the structure of the paper and key results. The matrix refers to the findings of the study concerning the nexus of illicit financial flows and digital technologies with regard to three stages: earning, transfers, and use. The paper itself is structured as follows.

Part 1 defines illicit financial flows to establish the scope of the problem and provide the context for further analysis. Part 2 focuses on the issue of digital technologies in the process of earning money illegally and transferring illicit funds, and analyzes how technology can help in the process of acquisition, transfers, and integration of illicit finds. Part 3 discusses the role of technology in fighting illicit financial flows. Part 4 concludes with suggestions for further areas of research in this field and ways to tackle the problem more effectively.

**Table 1 Nexus of Digital Technologies and Illicit Financial Flows: The Structure of the Study**

	Earning	→	Transfers	→	Use
	<b>Sources:</b> <ul style="list-style-type: none"> <li>• Laundering proceeds of crime</li> <li>• Abuse of power</li> <li>• Market/regulatory abuse</li> <li>• Tax abuse</li> </ul>		<b>Stages:</b> <ul style="list-style-type: none"> <li>• Placement</li> <li>• Layering</li> </ul>		<b>Integration:</b> Integration of the laundered assets into the legal financial system
<b>How digital technologies facilitate illicit financial flows</b>	<ul style="list-style-type: none"> <li>• Digital underground economy: cybercrime and “crime as a service”</li> <li>• Migration of traditional organized crime online</li> <li>• Embezzlement and fraud in the telecom sector</li> </ul>		Combination of: <ul style="list-style-type: none"> <li>• Online and mobile banking: slicing and automation of transactions</li> <li>• Electronic payments via unregulated intermediaries</li> <li>• Digital/cryptocurrencies: ensuring anonymity</li> <li>• E-commerce: manipulation of supply of goods</li> <li>• Online gambling/online betting</li> </ul>		<ul style="list-style-type: none"> <li>• Offshore electronic bank and investment accounts</li> <li>• Fake e-commerce companies</li> <li>• Offshore online casinos</li> <li>• Terrorist financing</li> </ul>
<b>How digital technologies help address the problem of illicit financial flows</b>	<ul style="list-style-type: none"> <li>• Tackling crime activities: detection, prevention, digital investigations</li> <li>• Increase transparency and public scrutiny to reduce corruption</li> <li>• Speed up introduction of e-government systems in areas such as tax administration or customs</li> </ul>		<ul style="list-style-type: none"> <li>• Monitor suspicious transfers</li> <li>• Trace illegal transfers</li> <li>• Better information exchange (digital platforms, automatic exchange of information)</li> <li>• Facilitate due diligence</li> </ul>		<ul style="list-style-type: none"> <li>• Ex-post identification of illicit sources</li> <li>• Databases of beneficial ownership</li> <li>• Leaks of electronic data transfer trails and electronic documents to the attention of public and competent authorities</li> </ul>
	<div style="text-align: center;">  <p><b>Any technological means to fight illicit financial flows have to be combined with</b></p> <ul style="list-style-type: none"> <li>- Harmonization of legal frameworks</li> <li>- Mechanisms for international cooperation and mutual legal assistance <ul style="list-style-type: none"> <li>- Public-private collaboration</li> <li>- Awareness raising</li> </ul> </li> </ul> </div>				

## Part 1. Illicit Financial Flows: Definition

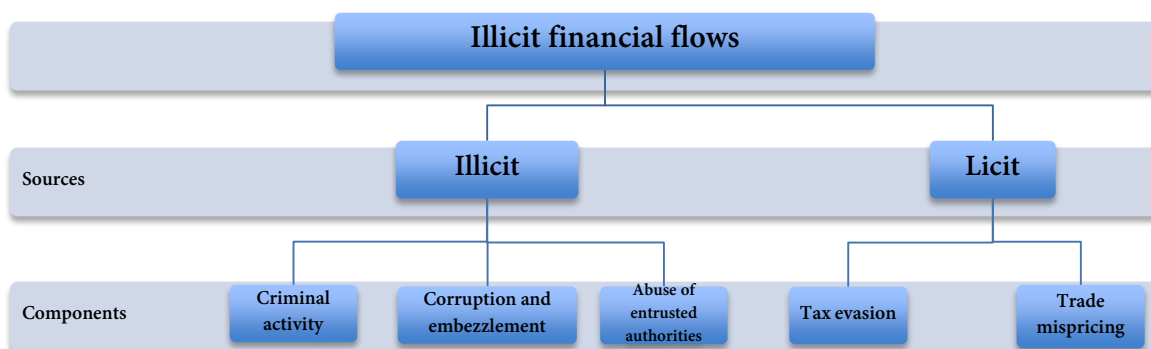
### *Illicit financial flows: Components*

The term “illicit financial flows” represents a relatively new concept (World Bank 2015). It emerged as an umbrella term to conflate previously disconnected issues related to tools, methods, and criminal activities aiming to move funds and assets across national borders in contravention of national or international laws (Goredema 2011; OECD 2013). There is still no consensus on the question of which practices actually constitute these tools and criminal activities; however, the common notion, which has been dominating in recent years, is that illicit financial flows can be defined as money “illegally earned, transferred or used” (UNECA 2015; World Bank 2015).

Despite the general agreement on the use of this relatively new term, a lack of consensus can be found in the studies debating the sources of the illicit financial flows. Most researchers agree that the term should cover money earned from criminal (illegal) activity, or money that was legally earned but became illegal because of the use, such as terrorist financing or illicit transfer (for example, violation of tax laws; see figure 1). Most of the literature refers to several sources of earning money from illegal activities: corruption, crime (including organized crime) and illegal commercial practices such as manipulation of custom duties, mispricing, and tax evasion (Global Financial Integrity 2014).

There are also other classifications; for example, Jansky (2013) splits illicit financial flows into three groups: illegal (criminal) flows, individual illicit flows, and corporate illicit (commercial) flows. Some studies approach the issue from a different angle and define illicit financial flows not through the activities, but through the negative impact. For example, Blankenburg and Kahn (2012) consider any financial transaction that is harming the economy to be a part of illicit financial flows, and thus create a somewhat vague and broad definition, which might cover many activities on the borderline between legal and illegal (Perez and Olivie 2014).

Figure 1 Illicit Financial Flows: Sources and Components



### *Differences in defining illicit financial flows*

There is a lack of agreement on where the line is between illicit and legal financial flows. There is an ongoing debate, for example, on whether such practices as tax avoidance should be included in the definition of illicit financial flows. On the one hand, recent studies, such as the “Report of the High Level Panel on Illicit Financial Flows from Africa” (UNECA 2015), highlight that the term “illicit” should be considered as a “fair description of activities that, while not strictly illegal in all cases, go

against established rules and norms, including avoiding legal obligations to pay tax” (UNECA 2015, 23). On the other hand, there are certain business practices that include legal tools to lower tax liabilities. There is an ongoing debate concerning the inclusion of reduction of tax liability in the definition of illicit financial flows. Such inclusion is advocated by civil society organizations and some states; however, major global financial centers favor a restrictive definition that covers crime and corruption and includes manipulation of tax payments only if they seriously and deliberately break the laws (World Bank 2015).

Because of the differences in taxation regulation among countries, it is hard to avoid the creation of grey areas, which will allow reduction of tax liability. Thus, the issue of tax reduction must always be addressed in the specific country context. These debates, however, are outside the scope of this study. The analysis in this paper will focus strictly on illegal activities.

Ultimately, due to the differences in national legal frameworks, a concept of what constitutes illicit financial flows will always depend on the legislation of the particular state. Furthermore, any international mechanisms implemented to tackle illicit financial flows can be undermined by the differences in national legislation and the fact that in some countries, laws can exist on the books but there is no capacity or no willingness to enforce the laws. These legal loopholes can be exploited by criminals and corrupt officials who seek safe havens—countries with weak laws and enforcement or states with preferable legal regimes for committing crimes—for tax avoidance or for carrying out operations for distancing illegal profit from its source. This situation requires not only identification of the loopholes in the national and international legal frameworks and harmonization of the legislation on the international level, but also proper implementation of these standards and capacity building for law enforcement agencies.

## **Part 2. Digital technologies and illicit financial flows: Earning and transferring money illegally**

The existence of the link between digital technologies and illicit financial flows, despite the lack of research in this field, has been widely recognized. However, the effect of information technology on the sources of the illicit profits is uneven. On the one hand, information and communications technologies (ICTs) have created new and facilitated traditional ways of earning and laundering money illegally. On the other hand, there is no direct link between ICTs and certain activities, such as bribery and corruption, which are considered a significant source of the illicit financial flows.

Of course, any illegal activity can be facilitated with the possibility of transferring funds anonymously or generating large amounts of money via aggregation of small sums. Yet, since there is almost no research or known—or even anecdotal—cases in this regard, it would be pure speculation to make a direct connection between digital technologies and some of the sources of the illicit financial flows, such as corruption or mispricing. This part of the study analyzes only those aspects of the nexus of illicit financial flows and digital technologies where a direct link can be established and confirmed by case studies. With reference to the definition of illicit financial flows, the chapter analyzes two aspects of the problem of information technologies and illicit financial flows: how digital technologies can facilitate the process of earning illicit profits and how technological developments influence illegal money transfers.

## 2.1. Money illegally earned: Digital technology as a way to get criminal profits

### Summary

There are several ways in which technology facilitates the process of earning illegal profits:

- Evolvement of the new types of crime (for example, cybercrime) and, as a result, the rise of a criminal underground economy. This underground digital market, where certain offenders specialize only in committing crimes involving digital technology, has already become an independent source of gaining illegal money.
- “Relocation” of traditional organized crime online: the use of digital technology for secure encrypted communications, for trade, information exchange, and for facilitating illegal activities in the offline world.
- Tax evasion practices facilitated by digital technologies.

### 2.1.1. Underground economy: Crime as service

#### *Digital technology and cybercrime: The rise of an underground economy*

In the early days of cybercrime, the scene was mainly dominated by individuals or loosely connected groups of hackers committing attacks just for fun or to demonstrate their technical skills (SecureWorks 2010). The development and growth of the digital economy dramatically changed both the criminal landscape and the motivation of offenders, transforming cyber-related crime into a complex and thriving criminal industry. As in the case of illicit financial flows in general, there are no reliable estimates on the criminal profits and the reputational losses and recovery costs that can go far beyond the direct harm. Most of the assessments come from the cybersecurity companies (see box 1) and, thus, are being questioned concerning the reliability of crime statistics and losses estimates (see, for example, Jardine [2015]). The uncertainty about crime profits and losses for businesses, however, does not mean that there is no general understanding that the aggregated criminal profits and direct and indirect losses for businesses are very high.

Though the primary targets of the cybercriminals are more wealthy developed countries, which heavily depend on information technologies, and there is a common notion that many crimes originate in countries in Asia, Africa, and Eastern Europe (Europol 2015), the underground economy itself exists independently of national borders. The development of the cybercrime industry is driven by the monetary value of data and services<sup>1</sup>, traded on the specific internet platforms and via communication channels, which are used as underground marketplaces (Europol 2014; Fallmann et al. 2010, 1).

This value represents an illicit commodity, intangible and easily transferrable across borders. Specific criminal activities have been developed and are being constantly improved in order to obtain data or

#### **Box 1 Impact of Cybercrime: Security Companies Assessments**

According to a McAfee assessment study, the underground industry of cybercrime costs global economies as much as US\$445 billion. This estimate includes both direct and indirect costs: profits of cybercriminals, and indirect costs such as reputational damage, defense, and recovery. McAfee makes a conservative estimate of US\$375 billion in losses, and the probable maximum as much as US\$575 billion (McAfee 2014). Even the smaller of these estimates of possible losses related to cybercrime exceed the GDP of most countries and the revenues of most private companies in the world.

<sup>1</sup> For example, according to KPMG research, in 2014 the prices for stolen credit card credentials ranged from US\$0.25 to US\$100 per item. Debit card information cost approximately US\$9.55 per item, stolen usernames and passwords US\$5.60 per item (Fowler 2014).



increase the value of services: phishing, farming, spoofing, sophisticated malware, and tools to obtain information from commercial databases. Online criminality includes a broad spectrum of fragmented and highly specialized economic activity, where both the skills and data are offered for sale: various criminal groups specialize in developing specific tools such as exploits, writing code for malicious software, or leasing the tools for automated attacks.

The underground economy is structuring its operations by copying business models from legitimate sectors. Technological developments, research, innovation, and the transformation of value chains into value networks have driven the globalization of the legal sectors and have affected business structures, making them more decentralized and collaborative with regard to external partners. In the same way, the development of digital technologies is fuelling the creation of new models of labor division, subcontracting, product placement, communications, and networking in the criminal ecosystem of the digital underground economy.

Schemes for doing illegal business resemble legitimate business-to-business (B2B) models. Highly sophisticated C2C (criminal-to-criminal) operations aim to make stolen data, crime tools, and professional skills for committing crimes available through digital networks (Ben-Itzhak 2008; Tropina 2013). The vulnerabilities of software and systems are exploited to create so-called “crimeware,” that is, “malware specially developed with the intention of making a profit and which can cause harm to the user’s financial well-being or valuable information” (ESET 2010, 4). Crimeware in the form of viruses, Trojans, key loggers, toolkits, and exploit kits offers cybercriminals the flexibility to steal and control data, to create and manage malicious programs, and to run networks of interconnected computers infected with malware (Kharouni 2012).

#### ***Automation: A core enabler of the illegal digital economy***

Automation plays a significant role in gaining illicit profits in underground markets. Technology is used to avoid the operation requirement for physical groupings and force of numbers (Europol 2011, 6). The core of automation is a system of botnets: networks of compromised computers that can be remotely controlled by the perpetrators and used as “zombies” for launching large-scale denial-of-service attacks on private and corporate systems, sending spam, disseminating malware, and scanning for system vulnerabilities. Without botnets, perpetrators would have to target victims and computer systems manually and individually, which would make attacks too costly and time-consuming (Europol 2011).

The system of delivering crimeware tools in the form of selling or hiring them drove the deployment of crime-as-service business models: trading botnets has become a high-revenue activity in the underground economy. Criminal organizations offer botnets at relatively low cost, profiting from the turnover based on the number of “customers.” At the beginning of 2015, according to Symantec, distributed denial-of-service (DDoS) attacks could be ordered from US\$10 to US\$1,000 per day (Wueest 2015). Moreover, as one of the logical steps in adopting business models from the legal economy, criminals are employing the policy of price differentiation, moving from static pricing lists to the flexible pricing schemes with discounts and bonuses (Danchev 2010).

In addition, they can offer different packages of the same products, depending on the service. For example, in 2012 the basic package of DDoS bot Darkness by SVAS/Noncenz could be bought for US\$450. The same botnet was also offered under “Bronze,” “Silver,” “Gold,” and other options that included, depending on the price, free updates, password grabbers, unlimited rebuilds, and discounts for other products (McAfee 2012). These costs are relatively low compared to the criminals’ financial gain: the estimated revenue of criminal groups using botnets ranges from tens of thousands to tens of millions of dollars.

Another “crime-as-a-service” model of operations that thrives alone with botnet trade is the pay-per-install (PPI) scheme, which was developed to meet one of the vital demands of the illegal market—infection of computer systems via digital networks. This service represents outsourcing of the dissemination of malware by determining the raw number of victims’ computers that should be

compromised within the scope of the “customer’s” budget (Caballero et al. 2011). A single PPI service can partner with thousands of affiliates, which get paid for the number of malware installs. This job does not require sophisticated computer skills, so malware distribution is nowadays open to anyone who wants to earn some money. A typical affiliate can supply more than 10,000 installs per month, which can generate millions of infected computers for illegal business, including thousands of affiliates (SecureWorks 2010). This business may be very profitable for affiliates; for example, Trend Micro once reported on an affiliate that generated US\$300,000 from rogue antivirus software installs in only one month (Trend Micro 2010).

### ***Tools-supplying business models: Another way to earn illegal money***

Tools-supplying business models are employed to create flexible “customer” systems for the commission of cybercrimes, where crime instruments and technics are available on demand. The owners of such servers with crimeware allow “users” to just log into the server and choose from the range of tools suitable for fraud, phishing, attacks, and data-stealing and then download them. Less-skilled criminals can buy tools to identify vulnerabilities, compromise systems, and steal data. More sophisticated offenders can purchase malware or develop custom tools and scripts on their own. When user data are stolen, criminals can use crimeware servers to commit organized attacks. Again, the prices are relatively low compared to the possible illicit profits.

In 2015, to rent a drive-by download web toolkit, which includes updates and 24/7 support, one needs as little as US\$100 to US\$700 per week. The online banking malware SpyEye is offered from US\$150 to US\$1,250 on a six-month lease (Wueest 2015). Even “teaching” skills are being converted into monetary value; nowadays, criminals can profit not only from committing crimes, but also from teaching others how to do it. For example, the training tutorials on Exploit Kits, DDoS attacks, Spam attacks, and phishing and other malicious activities can be purchased from as little as US\$1 (SecureWorks 2014). Furthermore, the next generation of business models has started offering licensed malware and technical support for illegal software and tools (SecureWorks 2010), and employing such schemes as “try it for free” or a “100% Satisfaction Guarantee on Stolen Credit Cards or They Will Be Replaced” (SecureWorks 2014).

### **2.1.2. Underground economy: “Traditional” organized crime and digital technologies**

#### ***Digital technologies: A new medium for traditional organized crime***

In addition to being a platform for the new type of criminal activity analyzed above, cyberspace and digital technologies also serve as a new medium for facilitating the criminal business of traditional mafia-style organized crime groups. This trend is not surprising. Under the general assumption, traditional organized crime always searches for “safe havens” offered by states with weak governments and unstable political regimes (Williams 2002, 2). Cyberspace, with its anonymity, absence of borders, and the opportunity to commit offenses without being physically present at the crime scene, constitutes a perfect environment, especially when criminals can operate from countries that do not have proper legal frameworks and technical capabilities for digital investigations (Goodman 2010). This poses a particular threat and calls for the adoption of proper legal frameworks and capacity building, especially in developing countries.

While traditional organized crime is still operating in a physical world—which is why it should not be confused with the new type of crime and underground industry of cybercrime—these groups can still benefit from the use of technology and underground marketplaces. Underground forums provide those involved in drug and arms trafficking, human trafficking, and trade in illegal goods with a perfect platform for trade of goods and services and a hub for networking, planning, and coordinating crimes. At the illegal online marketplaces (see box 2), the trade of crimeware tools for cybercrime coexists with the trade of illegal goods, fake identification documents, and different services associated with offline crimes.

#### **Box 2 Illegal Online Marketplaces: Silk Road and Agora**

One of the most infamous examples of hidden online marketplaces is Silk Road, which functioned similarly to legal auctions such as eBay, allowing “customers” to buy illicit drugs and other illegal commodities. It has been estimated that from 2011 to 2013, Silk Road facilitated over US\$1.2 billion worth of sales between 4,000 vendors and 150,000 customers (Houses of Parliament 2015). The marketplace was shut down by the FBI (U.S. Federal Bureau of Investigation) in October 2013, but reappeared shortly after as Silk Road 2.0 to continue criminal trade, until it was hit again in the operation Onymous, which represented cooperation between law enforcement in the European Union and the United States, in October 2014.

The closure of Silk Road, however, has not stopped the further evolution of illegal marketplaces. The online marketplace, Agora, launched in 2013, surpassed Silk Road in illegal drug trade and was named “the largest online narcotics emporium in the world” (Bertrand 2015) one year after it was established. It has been estimated that Agora, as a platform for trade of drugs, weapons, and illegal services, became the biggest black market operating online (Bertrand 2015; Greenberg 2014).

#### ***Digital technologies: Crime as service for traditional organized crime groups***

As reported by Europol (2014), traditional crime groups had already started using digital technologies as “crime as service,” hiring sophisticated cybercriminals to facilitate illegal operations. For example, in June 2013, law enforcement agencies in Belgium and the Netherlands took down a Netherlands-based drug smuggling ring, which employed hackers to penetrate the systems controlling the movement and location of shipping containers at the Belgian port of Antwerp. This infiltration involved interference with computer data to allow the criminals to remove shipping containers with drugs before the legitimate carrier could collect them (Europol 2014). There are still relatively few known cases of such sophisticated manipulations with digital technologies in facilitating traditional criminal operations. However, they illustrate very well the potential scale of this problem.

#### **2.1.3. Digital technologies and tax evasion**

##### ***Digital technologies and challenges of the digital economy***

It is unclear to what extent digital technologies can facilitate illegal attempts to evade tax payments. Though it is hard to assume that the development of global communication networks has no effect on tax evasion at all, it would be speculative to say there are many known distinct tools to illegally avoid taxes in the use of digital technologies. Of course, the global digital economy and the borderless internet create loopholes in the taxation frameworks, blur the line between illegal tax evasion and legal practices of tax avoidance, and pose particular challenges for tackling illegal activities.

This area of research has emerged recently on the agenda of international organizations, such as the Organisation for Economic Co-operation and Development (OECD 2014), which are currently undertaking studies and developing action plans concerning the problems of taxation in the era of digital technologies. Though the OECD admitted that severe erosion of tax bases could occur in the digital economy (OECD 2014), there is still no debate about the attribution of this problem to the use of particular technologies or to specific behavior.

There is little doubt that complex tax fraud and tax scam schemes can rely on the use of digital technologies. However, while technology can play a certain role as enabler of illegal activity, the main challenges are the globalization of the economy itself, the creation of digital multinational giants, and the possibility that digital technologies provide for the practice of “tax shopping,” making it easier for companies to provide services without a physical presence and to look for the best place for establishing their headquarters and moving their profits.

### ***Interconnection fraud and tax evasion in the telecommunications sector***

The only known practice of tax evasion that is statistically proven and distinctly linked to communication technologies is the so-called “SIM box fraud” or “interconnect fraud”—a type of manipulation that employs the internet to avoid call termination charges and, thus, revenue taxation. This scheme is a common practice in developing countries. It uses the voice-over-internet-protocol to channel international calls away from mobile network operators and deliver them as local calls. In this case, the international call appears to be local and cannot be subject to significant international terminating charges.

The same technique can be used to make local out-of-network calls appear to be handled within the network and, again, avoid termination charges (Ghosh 2012, 18). Furthermore, when the government levies taxes on the international calls, the operators themselves can use this scheme for diverting international calls, transforming them into local calls and making fake declarations of incoming international call minutes to reduce the tax payable to the government (UNECA 2015). This scheme especially affects developing countries, in particular, on the African continent (see box 3).

#### **Box 3 Interconnection Fraud: A Growing Problem for African Countries – Estimated Losses**

In March 2015, Uganda’s Financial Intelligence Authority started investigating suspected money laundering, revenue diversion, and tax evasion in the telecommunications sector, which could amount to US\$144 million in lost revenue. The Ugandan Financial Intelligence Authority claims that the government loses as much as 45 percent in tax revenue, while the telecommunication operators lose more than 80 per cent of their revenue (*The East African* 2015).

A report from the High Level Panel on Illicit Financial Flows from Africa states that the massive growth of the mobile industry brought significant losses in potential tax revenues because of the use of interconnection fraud. The report estimates losses in taxable revenue in Kenya as US\$440,000, and refers also to the estimates of the Governments of Ghana (US\$5.8 million in stolen taxes) and the Democratic Republic of Congo (US\$90 million in tax revenue losses a year) (UNECA 2015).

## **2.2. Illegal money transfers and use: Digital technologies and money laundering**

### **Summary**

- With speed of communication, automation, and anonymity, digital technologies offer a number of unique tools to facilitate illicit financial flows at all stages of money transfer and use: placement, layering, and integration.
- Digital technologies can be used to transfer money coming from any source of illegal income, including corruption, embezzlement, organized crime, tax evasion, and any other activities. Digital technology does not care about the source that money came from: electronic money transfers can be used to move and place any funds.
- Digital technologies, in many cases, allow offenders to avoid a placement stage because money illegally earned or stolen already exists in the online environment.
- A combination of the following tools allows criminals to distance their profits from illegal sources: online and mobile banking, electronic payments, digital currencies, online gambling, and betting services and e-commerce schemes.
- As a final stage of illegal transfers—comingling illegal funds with a legal sector—money can be safely placed via online banking in offshore jurisdictions. In addition, digital technologies allow using such tools as fake

e-commerce companies or faking online gambling services in offshore jurisdictions for the integration stage.

### ***Digital technologies: A sure enabler of illegal money transfers***

Transfers of illegal funds and money laundering have been dramatically influenced by the development of information and communications networks. Digital technologies offer countless opportunities to facilitate each traditional stage of illegal money transfer on their way to being distanced from illegal sources—placement, layering, and integration.<sup>2</sup> Initially, the problem of money laundering with the use of digital technologies was mostly associated with the underground economy of cybercrime. However, as the payment systems are becoming more complex, decentralized, and dependent on the information networks, criminals can enjoy the opportunities digital technologies offer to transfer any type of illicit funds (see box 4).

#### **Box 4 Digital Technologies and Embezzlement/Corruption Schemes in Developing Countries**

One of the biggest concerns with regard to illicit financial flows is the possibility of siphoning money, especially foreign aid funds, in developing countries, through embezzlement and money laundering. Millions of dollars are diverted from poverty-stricken nations through “phantom” firms and wire transfers to the bank accounts and companies in industrialized countries. For example, ONE, an international campaigning and advocacy organization, estimates that “at least \$1 trillion is being taken out of developing countries each year through a web of corrupt activity that involves shady deals for natural resources, the use of anonymous shell companies, money laundering and illegal tax evasion” (ONE 2014). Though this might be an overestimate, certainly the funds flying out of the developing countries constitute very large sums.

The question of how digital technology can facilitate this process is complex. In general, digital technology will enable any complicated money transfers, independently of the source—thus, it can be used to slice down the money and transfer it through a combination of bank and e-payment transactions to aggregate illegal funds in a safe jurisdiction or integrate the money into the legal sector. However, the nexus of digital technology and corruption/embezzlement is much more complex than can be narrowed down to electronic money transfers only. Digital technology is not the only factor that can possibly contribute to the complexity of transactions; it is the whole combination of such factors as cross-border trade, speed of communications, and the possibility of opening anonymous phantom companies without presenting identification documents or even without a physical presence. Establishing shell companies in some jurisdictions requires less information than obtaining a driver’s license or opening a bank account (ONE 2014).

These complex schemes might rely on information and communications technologies, but there is a lack of research and of evidence concerning the role that digital transactions can play in those intricate corruption and embezzlement models. There is little doubt that any tools for digital transfers analyzed in this chapter can be employed as a part of these schemes. However, further research and case studies are needed to investigate the nexus of digital technologies and complex schemes used to syphon money from developing states.

### ***Technology does not care about the source of illegal income***

While criminals can use different techniques and ways to gain ill-gotten profits, the tools that digital networks offer for distancing this capital from illegal activity are the same for any “dirty” money. The only difference between online and offline criminal activity is that money gained from cybercrime usually exists in cyberspace and has to be further transferred into cash and distanced from its source, so the placement stage of money laundering would be missing (Filipkowski 2008). However, this can also happen with the illegal trade of goods online in digital currencies; money in this case is “prelaundered” because it is placed in an unregulated financial institution (National Drug Intelligence Center 2008).

### ***Information and communication networks as a game changer for money laundering***

Digital technologies have a number of unique features that make them a game changer for money laundering:

- ***Automation, speed, and their cross-border nature***

The main advantages of global information networks—ease of use, speed of information transfers, automation, their cross-border nature, and the ability to operate in different jurisdictions without

---

<sup>2</sup> Placement is depositing money into the financial system, layering is distancing money from its source through a series of transactions, and integration is the commingling of money with funds in legal sectors.

being present onsite—enable fast transfers of illegal money and reduce the risk of being detected (Dumitrache and Modiga 2011, 50; Filipkowski 2008).

- ***Anonymity***

The absence of face-to-face transactions, which makes it difficult to implement know-your-customer techniques or monitor the behavioral patterns of the customers (FATF 2008, 21), is another key enabler of money-laundering schemes. Furthermore, many of the payment tools do not implement this technique at all and allow customers to enjoy full anonymity. Anonymity in general eroded the old models of traditional financial systems, which were usually based on long-term relationships with customers; unregulated online payment gateways nowadays provide the possibility for occasional transactions and transfers of micropayments (Council of Europe 2012, 30).

- ***Complexity of online transactions***

The complexity of the ecosystem of online transactions can be attributed to the rise of the new payment intermediaries. These intermediaries follow different rules and allow for various activities; many payment providers permit transfers from one intermediary to another, some online payment platforms authorize peer-to-peer transfers, and a number of payment systems are connected to the traditional banking system and allow credit accounts with bank cards. Implementation of the traditional techniques to monitor suspicious transactions by the payment providers can be undermined by the lack of the implementation of these tools by other intermediaries or by the insufficiency of the information about client behavior (Council of Europe 2012, 36).

- ***Less or no regulation***

Most of the intermediaries operating online are either less regulated than traditional financial institutions or not regulated at all (FATF 2008). Anti-money-laundering measures that were implemented to fight illicit transfers fail when it comes to most digital payment providers. Moreover, a payment intermediary can always benefit from the differences in regulation between various jurisdictions and choose a less regulated environment while being able to operate all over the world through global information networks.

The aforementioned characteristics of digital technologies and online payment systems combined with the development of the information and communications networks allow criminals to combine different means for distancing ill-gotten money from the source of illegal profits (see table 2). There are several tools that are mostly associated with money laundering in cyberspace: banking products and services, which to a large degree include regulated intermediaries; electronic payment systems via nonbank intermediaries; digital currencies, which are mostly unregulated and can also be decentralized; online services and trading platforms; online gambling; and e-commerce. These new tools can be combined with traditional methods of money laundering, thus creating a complex online and offline chain of multiple transactions, which are hard to trace and monitor, especially when they involve several jurisdictions. The following analysis provides insights into the way digital technology can facilitate transfers of illicit funds.

**Table 2 Digital Technologies and Illegal Money Transfers**



Placement	Layering	Integration
<ul style="list-style-type: none"> <li>- In many cases, no need for placement (money exists online)</li> <li>- Use of money mules (scarce resources)</li> </ul>	<ul style="list-style-type: none"> <li>- Online and mobile banking</li> <li>- Payments via unregulated online intermediaries</li> <li>- Digital currencies</li> <li>- Online gambling/betting services</li> <li>- E-commerce</li> <li>- Combination of all above</li> </ul>	<ul style="list-style-type: none"> <li>- Offshore electronic bank and investment accounts</li> <li>- Fake e-commerce companies</li> <li>- Offshore online casinos</li> </ul>

### ***Online banking***

Online banking is one of the most well-known nexuses of technology and money transfers, both legal and illegal. This link also represents the connection between technology and illegal ways to earn money; banks and their customers are still one of the major targets for profit-driven criminals. Thus, in many cases, in the beginning of the process of illegal transfers, offenders are still dependent on the online transfers from or via regulated financial intermediaries, though frequently it can be combined with other tools (Council of Europe 2012, 40–41).

Since regulated financial intermediaries carry out know-your-customer procedures and enter a business relationship with customers before online banking can be used, criminals need to employ more complex schemes than just transferring funds using online banking. This is why, for example, when money is stolen from bank accounts with the use of digital technologies, cybercriminals face a certain bottleneck; to distance this illegal profit, they need money mules for online transactions (iDefence 2006), and money mules are a scarce resource (Cisco 2011, 9). This is why criminals are searching for ways to avoid the use of mules and try, for example, to split money into small amounts below the reporting threshold (Thomason 2009, 18) and move them quickly from and to different bank accounts between different financial institutions (Weaver 2005, 456). This is where the benefits of digital technologies and automation are fully exploited.

Some studies reveal that money launderers can carry out “hundreds of meaningless transactions across various bank accounts, followed by a limited number of cash withdrawals” (Council of Europe 2012, 42). The possibility of performing many transactions through different institutions in various jurisdictions then makes it difficult, if not impossible, to detect illegal financial flows and trace them back (Malhotra 2010, 13).



### ***Mobile banking and mobile payments***

Mobile banking is a way of carrying payments via mobile phone with the use of different protocols such as text or internet. In the process of mobile banking communication, operators act as financial intermediaries for handling the payment between a client and business or financial institution (Filipkowski 2008, 23.). Mobile communications operators, though subject to telecom regulation, are usually not opposed to the obligation to perform anti-money-laundering checks (LIRNEasia and UP-NCPAG 2008). The main driver for the evolvement of mobile banking is the growing demand for micropayments, especially in developing countries (Forbes 2007, 28). The main vulnerability associated with the risk of the use of mobile banking for money laundering in many jurisdictions is the possibility of buying a pay-as-you-go SIM-card without registration and identity checks, and, thus, a great degree of anonymity, from which money launderers can benefit (Villasenor et al. 2011, 13).

However, the potential scope of using mobile banking for illegal transfers is debatable, because most of the transfers involve very small amounts of money. Although mobile payments are frequently named in different studies as one of the possible sources of digital money laundering, the latest reports produced rather controversial results and questioned the role of mobile banking in illicit financial flows. For example, a recent report from the Overseas Development Institute on capital flight in African countries concluded that although “in principle mobile banking is likely to facilitate capital flight, especially the movement of illegal funds abroad...data on mobile money in Africa, however, seem not to confirm this hypothesis since no clear correlation can be identified between capital flight and mobile banking” (Massa 2014, 11). The report, however, still highlighted the vulnerabilities of online banking concerning illegal funds transfer and its potential for being used for money laundering.

### ***Electronic payments via nonbank intermediaries***

Online nonbank payment services provide a cheap, quick, and anonymous way to make international money transfers or to pay for goods and services (see, for example, Dumitrache and Modiga 2011, 54). Unlike regulated financial institutions such as banks, these intermediaries are not subject to anti-money-laundering obligations and thus do not have to perform checks on their customers or detect suspicious money transfers. While the biggest online payment service providers, such as PayPal, developed anti-money-laundering policies and are trying to trace suspicious transactions, there are still many such intermediaries who allow criminals to enjoy freedom of money transfers with no checks.<sup>3</sup>

Furthermore, some of the services allow peer-to-peer money transfers, making monitoring of suspicious activities even harder and giving yet more possibilities to criminals for money laundering (FATF 2008, 39). In addition to the absence of anti-money-laundering obligations, criminals can benefit from the possibility of aggregating large sums by transferring very small amounts of money many times without attracting the application of techniques to monitor suspicious behavior, and then move this money inside the payment system or between different e-payment providers, or from e-payment systems to bank accounts and back (Piller and Zaccariotto 2009: 70–71; Richet 2013). Thus, e-payment services allow for illegal money transfers either in a way similar to online banking or in the form of transferring cash into online money and further purchase of goods, services, and digital currencies.

### ***Digital currencies***

Digital currencies embody a fast-growing area of internet commerce, driven by demand for low-friction e-commerce (Meiklejohn 2013) and micropayments (Tucker 2009, 601). Digital currencies represent

---

<sup>3</sup> It is difficult to estimate the number of online payment providers, and especially the number that do not conduct due diligence. For example, FATF (2010) reported that 15 of the jurisdictions responding to the FATF questionnaire indicated that Internet Payment Service providers were operating in their respective jurisdictions without giving the number of such providers; the estimated number of providers in different countries ranged from 1 to 23. With the growth of the digital economy in the last several years, this number could have increased significantly both on the national and international levels. Reliable statistics concerning the number of electronic payment intermediaries, which could show the whole picture on both the international and national levels, are not available.



value exchange systems that operate electronically and make transactions with the currencies that exist only online, are not issued by financial institutions, and thus are exempted from regulation. These currencies can be exchanged between account holders, or changed into traditional money (FATF 2010, 43). They are accessible from any part of the world, and allow making money transfers instantly, at low cost and with anonymity (Samani et al. 2013, 6–7), sometimes leaving virtually no trace. The anonymity of digital currencies and no regulation in this field make this type of payment an attractive option to criminals (Bryans 2014).

The role of digital currencies in illegal money transfers is prominent and constantly evolving. First, the use of digital currencies for illegal money has been confirmed by several criminal investigations against currency providers, such as E-gold or Liberty Reserve (Samani et al. 2013, 8; FATF 2014, 10). Second, it is a well-known fact that digital currencies, like Bitcoin, are used for payments at the online underground markets (Federal Bureau of Investigation 2012; FATF 2014). What makes the situation even more difficult is that many of those currencies are decentralized and thus hard to control; for example, shutting down Bitcoin literally requires shutting down the internet because there is no core node that can be taken down (Brito and Castillo 2013, 34).

Digital currencies, as a way to transfer money illegally, can be further converted into cash or other means of traditional payments. Illegal markets offer a number of possibilities for such transfers; there are websites, both in legal and illegal parts of the web, anonymous and non-anonymous, which offer not only to exchange Bitcoins for money via PayPal, Automated Clearing House (ACH), or Western Union, but also to turn Bitcoins into cash sent directly via mail (Ciancaglini et al. 2015, 21–22).

According to Europol's predictions, with further evolvement of cryptocurrencies, it is likely that we will witness development of more niche currencies, which would be specifically tailored to carry out illicit transfers and will provide greater levels of security and true anonymity (Europol 2014). The French anti-money-laundering body—TRACFIN—already mentioned at least two such anonymous and virtually untraceable digital currencies: Zerocoin, which represents an extension to Bitcoin's protocol for greater anonymity, and Darkcoin, which offers fully encrypted transactions and anonymous block transactions (TRACFIN 2014). Further developments in this field also include such applications as Dark Wallet, which makes Bitcoin transactions untraceable and allows for laundering someone's own Bitcoins, private cryptocurrencies created solely for the Russian underground market, and others (Europol 2014; TRACFIN 2014).

### ***Online casinos, e-gaming, and online betting websites***

For decades, casinos in the offline world have been considered a sure way to launder ill-gotten money (Filipkowski 2008, 22). It is natural, then, that online casinos attracted the attention of law enforcement and regulators as a possible way to use digital technologies for illicit funds transfers (Council of Europe 2013). However, despite this conventional wisdom, there have not been many known cases thus far of the use of online casinos for money laundering.

A few cases have been detected, however, in the use of e-betting systems. For example, in Australia, an Albanian organized crime syndicate employed an online betting system combined with internet payment services to launder illicit funds obtained from the sale of cannabis. The services were used to receive international transfers and to move money offshore. The online betting service was used in this illegal scheme to store the funds and make them accessible to other network members through sharing account passwords. The value of incoming and outgoing money was counted in the millions of Australian dollars (Australian Government 2012). Therefore, despite the lack of case studies and investigations, such examples prove that online gambling and betting services can be used for illegal transfers, especially when they are combined with online payment systems and digital currencies. As is argued by some researchers, online gambling can allow money to be distanced from the illicit source for the criminal enterprise of any size, both by gambling or by establishing an online casino in an offshore jurisdiction (Fiedler 2013).

## ***E-commerce***

Since the internet offers countless possibilities for trading goods, or exchanging money for goods and then selling them further, these activities can certainly be employed as a way for laundering illicit profits. Such schemes as the exchange of illegally obtained money for certain goods and trade of these goods in order to distance the profit from the source can be a part of the placement or layering stages of illegal money transfers (Villasenor et al. 2011, 10). Another possibility of using the internet for illicit transfers is the establishment of an e-commerce company, be it real or fake, and to offer services or trade goods that are never actually delivered (Filipkowski 2008, 20–21; Weaver 2005, 455).

### ***A complex landscape of illicit financial flows***

As can be seen from the analysis above, the landscape of the illicit financial flows on the internet is complex and can be attributed to various online activities and distinct areas of regulation. The convergence of different fields, such as online gambling and digital currencies, e-commerce and e-payments, and telecom services and banking, makes the ecosystem extremely complicated in terms of oversight and control. The internet itself is already a complex and decentralized cross-border network, where the possibility of tracing and prosecuting crimes requires effort and international cooperation. Tackling the problem of illicit financial flows in cyberspace represents a great challenge for regulators and law enforcement agencies because of the complexity and borderless nature of the online environment. The analysis below will focus on the question of how technology can help in tackling the problem of illicit financial flows—both on the internet and in the offline world.

## **Part 3. Digital technologies in fighting illicit financial flows**

One of the critical issues to consider in the discussion about the nexus of digital technologies and illicit financial flows is the question of whether and how technology can be used to address this problem. This question, in turn, should be discussed even in the broader context of the debate on the role of technology in fighting illicit financial flows in the digital era. This debate involves a set of complex issues, which go far beyond the discussion about the choice of particular technologies for investigation or the ways regulators and law enforcement agencies can use communication information and networks for disrupting illegal activity. The following analysis deals with two main aspects of this discussion: the use of information technologies for empowerment; and the role of digital tools for the prevention, detection, and investigation of criminal activity.

### **3.1. Digital technologies as a tool for empowerment**

---

#### **Summary**

- Digital technologies can be used as a tool to fight corruption and promote a culture of transparency.
- Different initiatives, from government efforts to establish e-government programs to grassroots anticorruption movements, can be seen as successful attempts to employ digital technologies in tackling illicit financial flows.
- To realize their full potential as a transparency and empowerment tool, however, digital technology tools should be combined with infrastructural, social, and economic changes.

There is a broad consensus that technology can help in the fight against corruption and facilitate efforts to fight illicit financial flows when it comes to good governance, transparency, awareness, empowerment, and crime reporting. Corruption, as one of the sources of illicit financial flows, has not been prominently linked to digital technologies for the facilitation of the commission of crimes. However, in this very area, governments and civil society can employ information and communications networks for strengthening efforts to tackle the problem. Digital technologies, and those related to e-government, in particular, are being praised as a cost-effective solution for promoting transparency and facilitating positive social changes (Bertot et al. 2010). Governments can employ the technologies for better communication, efficiency, and transparency, while citizens and civil society can use the technologies to report abuse, raise awareness, and monitor activities of the public sector (U4 2013).

Many initiatives, such as online reporting, online databases, and exit surveys, have also been developed by civil society organizations to collect data about corruption and make this data more accessible to public officials, investigative journalists, and nongovernmental organizations, and, ultimately, to citizens, who can play a monitoring role (The Engine Room 2012). These technologies can exist in the form of digital portals and platforms, websites, and mobile phone applications (see box 5).

Grassroots anticorruption movements and civil society initiatives are developing, along with the efforts of many governments, to create and promote a culture of transparency by launching e-government programs. Technology greatly contributes to these processes of empowerment. However, as some researchers have pointed out, despite the great promise the information and communications technologies might have in tackling the problem of corruption, they cannot be a silver bullet, and require a complex set of political, infrastructural, social, and economic factors to realize their full potential (U4 2013).

#### **Box 5 Digital Technology in the Fight against Corruption: Initiatives on the National Level**

##### **Reporting centers:**

The Janaagraha Centre for Citizenship's corruption reporting website in India is where citizens can report on the nature, number, pattern, types, location, frequency, and values of actual corrupt acts they have experienced; some of the reports on the website have already resulted in arrests and convictions. This initiative started in India, but was later duplicated in Greece, Kenya, Zimbabwe, and Pakistan with some other countries, which followed this experience and decided to launch such websites (U4 2013).

##### **Data aggregation platforms:**

The K-Monitor database in Hungary collects media reports about corruption and structures them in a way so that people can view data by category, such as institution, location, political party, and other (The Engine Room 2012).

##### **Capacity-building initiatives:**

The Nigerian anticorruption database, Acid, is a reporting platform combined with capacity-building initiatives. In addition to providing the digital tools to track corruption in the public sector, it offers downloadable training and advocacy materials. The website also hosts interactive tools, which allow citizens to text or tweet corruption reports to Google Maps in order to name corrupt officials and raise awareness (Roberts 2012).

### **3.2. Digital technologies in prevention, disruption, investigation, and detection of illicit financial flows**

#### **Summary**

- The use of digital technologies for investigation, prevention, and detection represents a big challenge because of the intrusiveness of these techniques and the necessity of finding a balance between crime prevention and crime control and human rights, safeguards, and privacy concerns.
- Digital technology, though one of the main enablers of the new types of crime and illegal money transfers, cannot be used alone as a response to illicit financial flows. Technological tools for law enforcement can be manipulated by criminals and can create even more vulnerabilities and risks. Thus, the use of intrusive technologies should be carefully considered with regard to the risks they might pose.
- Digital technology can be used to tackle money transfers at any stage of illicit financial flows. At the level of **gaining criminal profits**, it can help in crime investigation and disruption. At the transfer stage,

technology can be used to trace illegal transactions and information exchange. After the integration stage, digital technologies, such as the use of beneficiary databases or source leaks, can still help with identification of illegal money.

- Using digital technologies to fight illicit financial flows can complement, but will never substitute for, proper legal frameworks, international cooperation, and public-private collaboration. Addressing the problem of illicit financial flows requires complex multifaceted strategies that employ all the necessary components, including technological tools.

### ***Digital technologies in tracing and investigating illicit financial flows: Debates and challenges***

The second, much more complex and debatable aspect of the issue of the use of information technologies in tackling illicit financial flows is the use of digital tools in crime prevention and investigation. It has become conventional wisdom that law enforcement has been suffering because of the technological gap between sophisticated criminals and law enforcement officials who are much less equipped with technology. This common notion causes many debates in the field of fighting illegal activities in global information networks to revolve around the prohibition of certain technologies, or the need to regain control over technologies or—in general—the use of technology as a primary tool to prevent and investigate online criminality. As a result of these discussions, some initiatives, such as bulk data collection or permission to use such intrusive methods of investigation as remote forensic software, or the prohibition of certain types of encryption or demanding the backdoors for encryption are praised as the necessary solutions to empower law enforcement with the necessary capacity to trace and prevent illegal activities (Abelson et al. 2015; De Nardis 2015; Shields 2005).

Several factors are frequently overlooked in the technology-focused debates. First, technology is a facilitator of illegal activities online, but technology alone is not responsible for the problem. The problem is that technology, in many cases, overtook the law. Technology facilitates crime because there are different legal frameworks and borders, which technology can easily bypass, but which will not be bypassed by the capacity of national law enforcement agencies.

Second, the same technology can be used for both legal and illegal purposes. The new payment methods play one of the driving roles in the growth of the online economy and legal trade. Mobile banking is important in developing countries for the micropayments for people who have never had a bank account or landline phone. Even such services as Tor networks, which are free software for enabling anonymous communication and which are frequently-associated with cybercrime services, are used not only by criminals for gaining and moving illicit funds, but also by journalists, dissidents in authoritarian states, and even law enforcement for private and secure communications. Surveillance and bulk data collection, controls on certain technologies, or intrusion into communications in the absence of real suspicion will not necessarily lead to crime reduction and crime control, because when technology facilitates the crime, there are always people behind the criminal act. Moreover, the creation of backdoors to the secure communications and the use of intrusive technologies by law enforcement create the risk of exploitation of the same backdoors and technologies by criminals, thus, producing even more vulnerabilities and risks.

Third, sophisticated cybercriminals will always search for ways to cheat technology (Abelson et al. 2015). As Pena (2009) rightly points out, by trying to close the technological gap and imposing such measures as monitoring and surveillance, the states are “fighting fire with fire,” hoping “to find a cure for a problem in the very technology that seems to breed it.”

### ***Digital technologies as a tool for investigation, detection, and disruption***

Do all the challenges discussed above mean that technology cannot help in fighting illicit financial flows? The simple answer is no. Law enforcement, regulators, and businesses need to be technologically equipped to tackle the problem of illicit money. Even more, without technology it is impossible to detect, trace, investigate, and prosecute crime and illegal money transfers. Special equipment is needed for

crime investigation, collecting and handling electronic evidence, profiling with the purpose of prevention, and early disruption of crime online. Furthermore, technology can help in ex-post identification of illicit sources, when the money has already been integrated into the legal financial systems. Technology can help obtain data from databases of beneficial ownership or obtain electronic records about transaction trails.

The possible ways of using technologies are summarized in the table 3. This list is not exclusive, because anti-money-laundering software vendors and developers of investigation software offer many cutting-edge technical solutions that both industry and law enforcement agencies can use to trace and investigate illicit financial flows. There are already many technical tools employed by regulators and law enforcement for tackling crime in general, and the problems of illicit financial flows specifically. For example, the French anti-money-laundering body's secure networks, CEGmont Secure WebE, and CFIU.NETE, manage requests from abroad and allow fast and secure information exchange for the purpose of fighting illicit financial flows (TRACFIN 2013).

**Table 3 Digital Technologies in Prevention, Investigation, and Detection of Illicit Financial Flows**

Illegal Money Acquisition	Illegal Money Transfer	Illegal Money Integration
Digital tools to investigate crime (interception of content data and traffic data, remote forensic software, etc.)	Maintaining risk-based profiles based on transactional activities	Ex-post identification of illicit sources
Digital tools to trace and disrupt crimeware	Real-time payment screenings	Digital tools for searching for and obtaining beneficial ownership information in the databases
Databases for profiling	Creation of lists: fraud lists, blacklists, frozen lists, etc.	Leaks of electronic data transfer trails and electronic documents to the attention of public and competent authorities
Platforms for cross-border information exchange among law enforcement	Better information exchange (digital platforms, automatic exchange of information)	

Even challenging new technological developments offers law enforcement agencies certain opportunities. For example, criminals and law enforcement agencies alike can use the recent development—Big Data—for the application of qualitative analytical techniques for identifying likely targets; but, in the case of law enforcement, this technique of statistical predictions could be used either for investigations or for prevention (Eruopol 2014).

There are many examples of the use of specific technologies and tools that help to tackle the problem; however, there is a need for a clear understanding that for the purpose of detection, investigation, and prevention of crime and money laundering, technological means are a very important component, but they are still just one element among other critical tools. The complexity of the issue of using technology for disruption of the technological schemes employed in the illicit market can be briefly illustrated with the example of botnet—a network of “zombie” computers, which represents one of the backbones of the underground economy (box 6).

#### **Box 6 Use of Technology for Botnet Disruption: Complexity of the Issue**

To take down a botnet, it is not enough just to use technology to tackle the infrastructure of zombie networks. The network cannot be taken down by just shutting down the servers because the bot herder (the individual who controls and maintains a botnet), if he or she is not arrested, can set up new servers and reconnect with a network of compromised computers.

Arresting the bot herder without shutting off the infrastructure will not help either, because the network can be taken over by another person and the criminal activity will continue. To cope with this situation, law enforcement agencies have to disrupt communication between the bot herder and the network and then arrest the bot herder; however, even this is not the last step. When the bot herder is arrested and servers are taken down, the malware will remain in hundreds of compromised computers; only new infractions will be prevented.

Thus, the users of compromised machines always need to be contacted and helped to clean their computer systems (van der Wagen and Pieters 2015)—and this neither law enforcement nor other governmental bodies can do on their own; the help of the internet service providers is always needed. This is why in many countries there are special public-private collaboration programs on tracing malicious traffic from the IP (Internet Protocol) addresses and contacting users and helping them clean their machines.

#### ***Technology: A core component, but not a silver bullet***

In addition to the use of technologies, law enforcement agencies always have to tackle many components of the criminal value networks simultaneously and with the use of different tools. Even the best digital tools in crime investigation will not work when there are no harmonized legal frameworks, proper regulation, collaboration between industry and governments, or user awareness. The complexity of the problem of using digital technologies for illicit activities comes not only from technology itself, but also from the borderless and decentralized nature of the internet, uncooperative states, the complexity of digital ecosystems with a myriad of players in the landscape of the digital economy, and, as a result, a lack of coordinated efforts, legal uncertainty, and jurisdictional problems (Thomason 2009, 24). This is why the approach to fighting the process of earning and transferring illicit money should employ relevant technologies, but never rely solely on technologies.

Technology can equip the criminal justice system with the necessary tools, but will not fix the system itself and will not bridge all the capacity gaps, let alone the legal gaps. In order to use investigative technologies properly and to facilitate cross-border investigations and the exchange of electronic evidence, there is a need for common digital forensics standards and procedures, including standards on tools, data formats, and direct data transfers. Even when the most crosscutting technologies are employed by law enforcement, investigation will always rely primarily on legal frameworks; thus, all the technology-related tools have to be combined with the effective mutual legal assistance and electronic evidence rules. Since the use of investigative instruments, surveillance, and data collection can have more drastic privacy implications than those caused by crime, any invasive technological means for prevention and detection of illicit financial flows have to take into consideration privacy and human rights concerns and have to be carefully balanced.

Furthermore, the existence of the thousands of stakeholders in the field of digital economy requires public-private cooperation between industry and governmental bodies. Thus, there is a need for a



complex approach—from awareness and education of users to public-private cooperation, and from proper national legal frameworks to mutual legal assistance instruments that are able to cope with the speed of information transfers in the digital era.

Fighting illicit financial flows requires coordinated efforts on harmonization of legislation and approaches to mutual legal assistance on the global level with the involvement of all stakeholders, including governments, industry, and civil society. One of the key issues in this regard is the difference in capacity between developed and developing countries, and the special needs poorer countries have in order to be able to address the problem properly. This issue is twofold.

On the one hand, substantive and procedural legal frameworks should be harmonized in the same way to allow international cooperation; therefore, differences in the legal frameworks might create loopholes and grey areas for cybercriminals. Thus, there should be a clear understanding that legal instruments should be drafted in the same way in both developed and developing countries. On the other hand, though legal frameworks play a central role in tackling illegal activity in digital networks, the law will not work without proper technical instruments and the special knowledge of those who are applying it. This is why it is important to focus on capacity building and awareness raising in developing countries, which can have special needs depending on the state of technological development, the structure of penetration of different type of networks and services, and the current capacity of law enforcement agencies.

Even wealthy nations, which have been the target of cyber-related crime for decades and have already made significant efforts to build capacity to fight technology-related crime and promote a culture of cybersecurity, are struggling with many problems in this field. The problems include harmonization of procedural instruments, differences in legislation, slow mutual legal assistance processes, sophisticated encryption, and constantly evolving cyberthreats. For developing countries, the issue of cyber-related illegal activity might have a different dimension: many of them, while not being a primary target of digital crime, are struggling with “bread and butter” problems, like food and water supply, fighting corruption, and traditional organized crime and reduction of poverty, to name a few, in addition to technology-enabled illicit financial flows.

However, with the fast development of the new forms of crime, any developing country with cybersecurity flaws can become if not a target, at least a country of origin of digital crime. Thus, capacity building and the promotion of a cybersecurity culture should be one of the priorities in developing countries in order to avoid a potential “cybersecurity divide,” which can undermine efforts to facilitate economic and social development, and, as a result, open a new schism “between [the] haves and have nots” (Gercke et al. 2011, 189). It is necessary to adopt proper legal frameworks, and educate law enforcement agencies in developing countries and equip them with appropriate technological tools for investigations. Therefore, a special focus should be put on addressing the needs of the poorer states to tackle the global problem of transborder illegal activities with the use of digital technologies.

#### **Part 4. Conclusion: The way forward**

Fighting illicit financial flows in the interconnected society is like chasing a moving target. In the borderless decentralized communications networks, the problem of illegal money extends beyond national borders and spans different jurisdictions. The complexity of the digital economy and fast-evolving technologies, when money can be illegally earned and transferred across borders with a simple mouse click, requires a shift from the legal and technical paradigm to the principle “follow the money” in tackling the problem of illicit financial flows. While information technologies are evolving, the very existence of these technologies and their vulnerable and transborder nature are the primary factors for the evolvement of illegal activity carried out with the use of digital networks or facilitated by such use.

Since technology is evolving every day, there is no silver bullet—no perfect frameworks or technologies—that could be implemented to solve the problem from a long-term perspective. Any set of

solutions should be considered just as a way to address the current state of technology and as another step in the continuous process of tackling the problem. The situation requires complex strategies and forward-looking approaches, where efforts should be directed not only to solving the current problems, but identifying the new threats and predicting the risks posed by new technologies. These strategies should focus on a broad range of issues, such as:

- Identification of the gaps in international standards concerning illegal money transfers
- Harmonization of substantive and procedural criminal law (including electronic evidence frameworks) in the field of cybercrime and digital investigation on the international level
- Proper implementation of the international standards and legal frameworks on the national level
- Capacity building, especially in developing countries, in order to increase the effectiveness of legal and regulatory frameworks
- Efforts to raise awareness among governments, regulators, and private industry
- Use of modern technology in tackling illicit financial flows, but balancing the use of technological tools with privacy and human rights and implementing necessary safeguards
- Identification of technology-related risks in order to create a risk-based approach to prevention, detection, and monitoring of illicit financial flows
- Public-private collaboration in the field of tackling cybercrime
- Private sector engagement in monitoring illegal money transfers
- Technical capacity building among law enforcement and private industry.

Ultimately, any approach to tackling illicit financial flows should be based on a common understanding that detection, prevention, and tracing of illegal profits earned or transferred in the digital environment will be a continuous process of addressing new technological challenges. It is also necessary to take into account the complexity of the ecosystem of the digital economy and to bear in mind that heavy regulation can have a negative effect on the development of new technologies and services and, in the end, undermine the benefits that the internet and digital technologies can bring to society.



## References

- Abelson et al. 2015. "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications." [http://www.crypto.com/papers/Keys\\_Under\\_Doormats\\_FINAL.pdf](http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf).
- Australian Government. 2012. "AUSTRAC typologies and case studies report 2012." [http://www.austrac.gov.au/sites/default/files/documents/typ\\_rprt12\\_full.pdf](http://www.austrac.gov.au/sites/default/files/documents/typ_rprt12_full.pdf).
- Ben-Itzhak. 2008. "Organized cybercrime." *ISSA Journal* (October). <https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf>.
- Bertot et al. 2010. "Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies." *Government Information Quarterly* 27: 264–271.
- Bertrand. 2015. "Silk Road wasn't even close to the biggest drug market on the internet." <http://uk.businessinsider.com/silk-road-wasnt-even-close-to-the-biggest-drug-market-on-the-internet-2015-6?r=US&IR=T>.
- Blankenburg and Kahn. 2012. "Governance and Illicit Flows." In *Draining Development?: Controlling Flows of Illicit Funds from Developing Countries?*, edited by Peter Reuter. Washington, DC: World Bank. <https://openknowledge.worldbank.org/bitstream/handle/10986/2242/668150PUB0EPI0067848B09780821388693.pdf>.
- Brito and Castillo. 2013. "Bitcoin: A Primer for Policymakers." Mercatus Center, George Mason University, Fairfax, Virginia, United States. [mercatus.org/sites/default/files/Brito\\_BitcoinPrimer\\_embargoed.pdf](http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf).
- Bryans. 2014. "Bitcoin and Money Laundering: Mining for an Effective Solution (August 29, 2013)." *Indiana Law Journal* 89 (1). <http://ssrn.com/abstract=2317990>.
- Caballero et al. 2011. "Measuring pay-per-install: the commoditization of malware distribution," *Proceeds of the USENIX Security Symposium*, August. <http://www.icir.org/vern/papers/ppi-usesec11.pdf>.
- Ciancaglini et al. 2015. "Below the Surface: Exploring the Deep Web." TrendMicro, Forward-Looking Threat Research Team. <http://www.trendmicro.co.uk/media/wp/exploring-the-deep-web-whitepaper-en.pdf>.
- Cisco. 2011. "Cisco 2010 annual security report. Highlighting global security threats and trends." [http://www.cisco.com/en/US/prod/collateral/vpndevc/security\\_annual\\_report\\_2010.pdf](http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf).
- Council of Europe. 2012. "Moneywal report: Criminal money flows on the internet: methods, trends and multi-stakeholder counteraction."
- . 2013. "The use of online gambling for money laundering and the financing of terrorism purposes. Research report."
- Danchev. 2010. "Study finds the average price for renting a botnet." <http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>.
- DeNardis. 2015. "Internet Architecture as Proxy for State Power." In *IP Justice Journal: Internet Governance and Online Freedom Publication Series*. <http://www.ipjustice.org/digital-rights/internet-architecture-redesign-as-proxy-for-state-power-by-laura-denardis/>.
- Dumitrache and Modiga. 2011. "New Trends and Perspectives in the Money Laundering Process." *Challenges of the Knowledge Society Law* (1): 50–57.

- ESET. 2010. "Cybercrime Coming of Age." White paper, January. <http://go.eset.com/us/resources/white-papers/EsetWP-CybercrimeComesOfAge.pdf>.
- Europol. 2011. "Threat assessment (abridged). Internet facilitated organised crime." Internet Organised Crime Threat Assessment (iOCTA). File No.: 2530–264, The Hague, January 7. <https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf>.
- . 2014. "The Internet Organised Crime Threat Assessment (iOCTA)." September 29. <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>.
- . 2015. "The Internet Organised Crime Threat Assessment (iOCTA)." September 30. <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>.
- Fallmann et al. 2010. "Covertly probing underground economy marketplaces." Vienna University of Technology Secure Systems Lab. [http://www.iseclab.org/papers/dimva2010\\_underground.pdf](http://www.iseclab.org/papers/dimva2010_underground.pdf).
- FATF (Financial Action Task Force). 2008. "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems." <http://www.fatf-gafi.org/>.
- . 2010. "Money Laundering Using New Payment Methods." October. <http://www.fatf-gafi.org/>.
- . 2014. "FATF Report. Virtual Currencies. Key Definitions and Potential AML/CFT Risks." June. <http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.
- Federal Bureau of Investigation. 2012. "Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity." April 24. [www.wired.com/images\\_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf](http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf).
- Fiedler. 2013. "Online Gambling as a Game Changer to Money Laundering?" April 30. <http://ssrn.com/abstract=2261266>.
- Filipkowski. 2008. "Cyber Laundering: An Analysis of Typology and Techniques." *International Journal of Criminal Justice Sciences (IJCJS)* 3 (1): 15–27.
- Forbes. 2007. "Convergence of Telecom and Financial Services and Its Effects on AML/CFT Wire Remittance Operations." *United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI), Resource Material Series No. 71*: 24–31.
- Fowler. 2014. "Being cyber resilient. KPMG Insurance Issues Conference," December 1. <https://www.kpmg.com/Ca/en/IssuesAndInsights/ArticlesPublications/Evolving-Regulation-Series/Documents/Being-Cyber-Resilient.pdf>.
- Gercke, Tropina, Lozanova, and Sund. 2011. "The role of ICT regulation in addressing offences in cyberspace." In *Trends in Telecommunication Reform November 2010. Enabling Tomorrow's Digital World*. Geneva: International Telecommunication Union.
- Ghosh. 2012. "How to prevent fraud in the Indian telecom industry." *Journal of Advanced Analytics* 3Q 2012: 18. [https://www.sas.com/news/intelligence\\_quarterly/q312.pdf](https://www.sas.com/news/intelligence_quarterly/q312.pdf).
- Global Financial Integrity. 2014. "Illicit Financial Flows." <http://www.gfintegrity.org/wp-content/uploads/2014/09/GFI-Analytics.pdf>.
- Goodman. 2010. "International dimensions of cybercrime." In *Cybercrimes: A multidisciplinary analysis*, edited by S. Ghosh and E. Turrini. Berlin and Heidelberg: Springer-Verlag.
- Goredema. 2011. "Combating illicit financial flows and related corruption in Africa: Towards a more integrated and effective approach." <http://www.cmi.no/publications/file/4214-combating-illicit-financial-flows-and-related>.

- Greenberg. 2014. "Drug Market 'Agora' Replaces the Silk Road as King of the Dark Net." *Wired*. <http://www.wired.com/2014/09/agora-bigger-than-silk-road/>.
- Houses of Parliament. 2015. "The darknet and online anonymity." *Postnote* Number 488 March. [www.parliament.uk/briefing-papers/POST-PN-488.pdf](http://www.parliament.uk/briefing-papers/POST-PN-488.pdf).
- iDefence. 2006. "Money Mules: Sophisticated Global Cyber Criminal Operations." iDefense, A VeriSign Company. [http://complianceandprivacy.com/WhitePapers/iDefense\\_MoneyMules\\_20060329.pdf](http://complianceandprivacy.com/WhitePapers/iDefense_MoneyMules_20060329.pdf).
- Jansky. 2013. "Illicit Financial Flows and the 2013 Commitment to Development Index," CGD Policy Paper 034, Center for Global Development. <http://www.cgdev.org/publication/illicit-financial-flows-and-2013-commitment-development-index>.
- Jardine. 2015. "Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime." Chatham House, Global Commission on Internet Governance. Paper Series: NO. 16 — July 2015. [https://www.cigionline.org/sites/default/files/no16\\_web\\_1.pdf](https://www.cigionline.org/sites/default/files/no16_web_1.pdf).
- Kharouni, Loucif. 2012. "The Crimeware Evolution." Trend Micro Incorporated Research Paper 2012. <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-crimeware-evolution.pdf>.
- LIRNEasia and UP-NCPAG. 2008. "Mobile banking, mobile money and telecommunication regulations." [http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0\\_Final\\_Hor\\_EA.pdf](http://lirneasia.net/wp-content/uploads/2008/05/Mobile-2.0_Final_Hor_EA.pdf).
- Malhotra. 2010. "A New Dimension of Socio-Economic Offences: E-Money Laundering." July 7. <http://ssrn.com/abstract=1505795>.
- Massa, Isabella. 2014. "Capital flight and the financial system." ODI Working Paper, December 4. <http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9392.pdf>.
- McAfee. 2012. "McAfee Threats Report: First Quarter 2012." <http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q1-2012.pdf>.
- . 2014. "Net Losses: Estimating the Global Cost of Cybercrime." <http://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf>.
- Meiklejohn et al. 2013. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names." *Login* 38 (6): 10–14. <https://www.usenix.org/publications/login/december-2013-volume-38-number-6>.
- National Drug Intelligence Center. 2008. "Money Laundering in Digital Currencies." U.S. Department of Justice, Washington, DC. <http://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf>.
- OECD (Organisation for Economic Co-operation and Development). 2013. "Measuring OECD Responses to Illicit Financial Flows from Developing countries." Organisation for Economic Co-operation and Development, Paris. [http://www.oecd.org/corruption/Illicit\\_Financial\\_Flows\\_from\\_Developing\\_Countries.pdf](http://www.oecd.org/corruption/Illicit_Financial_Flows_from_Developing_Countries.pdf).
- . 2014. "Addressing the Tax Challenges of the Digital Economy." OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing, Paris. <http://www.oecd.org/ctp/tax-challenges-digital-economy-discussion-draft-march-2014.pdf>.
- ONE. 2014. "Trillion Dollar Scandal." [https://s3.amazonaws.com/one.org/pdfs/Trillion\\_Dollar\\_Scandal\\_report\\_EN.pdf](https://s3.amazonaws.com/one.org/pdfs/Trillion_Dollar_Scandal_report_EN.pdf).
- Pena. 2009. "Exporting Criminality: Money Laundering in a Domestic and International Context." [http://web.stanford.edu/group/journal/cgi-bin/wordpress/wp-content/uploads/2012/09/Pena\\_SocSci\\_2009.pdf](http://web.stanford.edu/group/journal/cgi-bin/wordpress/wp-content/uploads/2012/09/Pena_SocSci_2009.pdf).

- Perez and Olivie. 2014. "Europe Beyond Aid: Illicit Financial Flows Policy Responses in Europe." Center for Global Development. Consultation Draft. [http://www.cgdev.org/sites/default/files/Europe-Beyond-Aid-Illicit-Financial-Flows\\_0.pdf](http://www.cgdev.org/sites/default/files/Europe-Beyond-Aid-Illicit-Financial-Flows_0.pdf).
- Piller and Zaccariotto. 2009. "Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organizations." *Transition Studies Review* 16 (1): 62–76.
- Richet. 2013. "Laundering Money Online: A Review of Cybercriminals Methods. Tools and Resources for Anti-Corruption Knowledge." United Nations Office on Drugs and Crime (UNODC), New York, June 1. [arxiv.org/pdf/1310.2368](http://arxiv.org/pdf/1310.2368).
- Roberts, Tony. 2012. "Technology is helping the fight against corruption: All over the world citizens are using new technology to shine a light on fraud and bribery, and to blow the whistle on corrupt practices." <http://www.computerweekly.com/opinion/Technology-is-helping-the-fight-against-corruption>.
- Rush, H., C. Smith, E. Kraemer-Mbula, and P. Tang. 2009. "Crime online. Cybercrime and Illegal Innovation." NESTA Research Report, July. [http://www.eprints.brighton.ac.uk/5800/01/Crime\\_Online.pdf](http://www.eprints.brighton.ac.uk/5800/01/Crime_Online.pdf).
- Samani et al. 2013. "Digital Laundry. An analysis of online currencies, and their use in cybercrime." White Paper, McAfee Labs. <http://www.mcafee.com/de/resources/white-papers/wp-digital-laundry.pdf>.
- SecureWorks. 2014. "Underground Hacker Markets." December. <http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf>.
- . 2010. "The Next Generation of Cybercrime: How it's evolved, where it's going." Executive Brief, [secureworks.com](http://secureworks.com).
- Shields. 2005. "When the 'information revolution' and the US security state collide. Money laundering and the proliferation of surveillance." *New Media & Society* August 7 (4): 483–512.
- The EastAfrican. 2015. "Uganda financial body probes \$144m telecoms fraud," March. <http://www.theeastafrican.co.ke/news/Uganda-financial-body-probes--144m-telecoms-fraud-/-/2558/2661148/-/k0hyke/-/index.html>.
- The Engine Room. 2012. "New Technologies Against Petty Corruption. Tactics and Lessons from the 2012 International Anti-corruption Conference." <https://www.theengineroom.org/wp-content/uploads/New-Technologies-Against-Petty-Corruption.pdf>.
- Thomason. 2009. "How has the establishment of the internet changed the ways in which offenders launder their dirty money?" In *Internet Journal of Criminology* 2009. [http://www.internetjournalofcriminology.com/Thomason\\_Internet\\_Money\\_Laundering\\_July\\_09.pdf](http://www.internetjournalofcriminology.com/Thomason_Internet_Money_Laundering_July_09.pdf).
- TRACFIN (Treatment of intelligence and action against clandestine financial circuits). 2013. "Annual Analysis and Activity Report 2013." Unit for intelligence processing and action against illicit financial networks. [http://www.economie.gouv.fr/files/ra\\_tracfin\\_anglais\\_2013.pdf](http://www.economie.gouv.fr/files/ra_tracfin_anglais_2013.pdf).
- . 2014. "Regulating virtual currencies. Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering." <http://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf>.
- Trend Micro. 2010. "The business of cybercrime. A complex business model." Focus Report Series, January. [http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt\\_business-of-cybercrime.pdf](http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf).

- Tropina, Tatiana. 2013. "Organised Crime in Cyberspace." In *Transnational Organized Crime. Analyses of a Global Challenge to Democracy*. Bielefeld, Transcript Verlag, edited by Heinrich-Böll-Stiftung and Regine Schönenberg, pp. 47–60.
- Tucker. 2009. "The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy?" *Cardozo Journal of International and Comparative Law* 17 (3): 589.
- U4. 2013. "Technological innovations to identify and reduce corruption. U4 Expert Answer." <http://www.u4.no/publications/technological-innovations-to-identify-and-reduce-corruption/>.
- UNECA (United Nations Economic Commission for Africa). 2015. "Illicit Financial Flows. Report of the High Level Panel on Illicit Financial Flows from Africa." [http://www.uneca.org/sites/default/files/PublicationFiles/iff\\_main\\_report\\_26feb\\_en.pdf](http://www.uneca.org/sites/default/files/PublicationFiles/iff_main_report_26feb_en.pdf).
- van der Wagen and Pieters. 2015. "From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks." *British Journal of Criminology* 55 (3): 578–595.
- Villasenor, et al. 2011. "Shadowy Figures: Tracking Illicit Financial Transactions in the Murky World of Digital Currencies, Peer-to-Peer Networks, and Mobile Device Payments." The Brookings Institution and the James A. Baker III Institute for Public Policy. <http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf>.
- Weaver. 2005. "Modern Day Money Laundering: Does the Solution Exist in an Expansive System of Monitoring and Record Keeping Regulations?" *Annual Review of Banking & Financial Law* 24: 443–465.
- Williams. 2002. "Organized crime and cyber-crime: Implications for business." <http://www.cert.org/archive/pdf/cybercrime-business.pdf>.
- World Bank. 2015. "Illicit Financial Flows (IFFs)." <http://www.worldbank.org/en/topic/financialmarketintegrity/brief/illicit-financial-flows-iffs>.
- Wueest. 2015. "Underground black market: Thriving trade in stolen data, malware, and attack services." Symantec official blog. <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>.