Digital Shadow Economy: a Critical Review of the Literature

Prof. Dr. Ligita Gaspareniene

Mykolas Romeris University, Banking and Investment Department
ligitagaspareniene@mruni.eu

Assoc. Prof. Dr. Rita Remeikiene

Mykolas Romeris University, Banking and Investment Department
rita.remeikiene@mruni.eu

Doi:10.5901/mjss.2015.v6n6s5p402

Abstract

One of the biggest problems of the last decade is hardly defined economic activities, objects and subjects in cyber space. Through cyberspaces, such as social networking platforms, e-commerce, e-business systems or cyber computer games, real money circulates but in most cases these transactions are not accounted and do not generate the taxes to the state budget. For this reason, a deeper insight in the phenomenon of digital shadow economy is purposeful. The performed analysis of various scientific sources leads to the conclusion that the previous research on the topic of digital shadow economy is mostly limited with the studies in cybercriminal activities, e-fraud and the motives of the consumers to get involved in digital piracy. However, the complex scientific research in the field of digital shadow economy has not been performed, which determined the aim of this research – to systematize the scientific literature on digital shadow economy and perform the critical analysis of the researched phenomenon. The methods used in the research include systematic and comparative analysis of the scientific literature. The research has enabled to specify the concept of digital shadow economy, identify its forms and activity channels in digital black markets and define the differences between traditional and digital shadow economy.

Keywords: *digital shadow economy, critical review of digital shadow economy, shadow economy.*

1. Introduction

Although advances in information technologies and internet have expanded the ways of conducting business, they have also provided an environment for a wide range of illegal activities. With reference to Amasiatu and Shah (2014), "with online business transactions hugely reliant on trust and identity validation/authentication, there are so many avenues for dishonest financial gains" (p. 805), or for digital shadow economy. One of the biggest problems of the last decade is hardly defined scope of economic activities, objects and subjects in cyber space. Through cyberspaces, such as social networking platforms, e-commerce, e-business systems or cyber computer games, real money circulates but in most cases these transactions are not accounted and do not generate the taxes to the state budget. Although the value of the digital shadow economy as a whole is not yet known, one recent estimate of global corporate losses stands at around €750 billion per year (Europol, 2011). For this reason, many countries are rising a topical issue on how the volumes of digital shadow economies could be reduced without violating the privacy and mobility of both individuals and businesses, and at the same time the revenue earned by the subjects in digital space as well as the changes of their assets could be estimated in their real value.

The previous research on the topic of digital shadow economy is mostly limited with the studies in cybercriminal activities, such as breaking into online banking systems or decryption of PIN codes (Yip, et al., 2012; Holz, et al., 2012), forms of e-fraud (Thomas & Martin, 2006; Yip et al., 2012; Mello, 2013; Vlachos, Minou, Assimakopouos, & Toska, 2011; Amasiatu & Shah, 2014; Zorz, 2015 and others) and the motives of the consumers to get involved in digital piracy (Williams, Nicholas, & Rowlands, 2010; Sirkeci & Magnusdottir, 2011; Camarero, Anton, & Rodriguez, 2014; Amasiatu & Shah, 2014; Vida, Koklic, Kukar-Kinney, & Penz, 2012; Taylor, 2012; Arli, Tjiptono, & Porto, 2015; Yu, Young, & Ju, 2015 and others). However, the scientific literature still lacks of the complex studies in the field of digital shadow economy, which determined the aim of this research – to systematize the scientific literature on digital shadow economy and perform the critical analysis of the researched phenomenon. The defined aim has been detailed into the following objectives: 1) to review the concepts and interpretations of digital shadow economy; 2) to analyse the forms of digital

shadow economy in digital black markets; 3) to perform the comparative analysis of traditional and digital shadow economy. The methods used in the research include systematic and comparative analysis of the scientific literature.

2. The Concepts and Interpretations of Digital Shadow Economy

According to Holz et al. (2012), growing scopes of digital economy have stimulated criminal activities in digital business, which, in turn, have led to a digital shadow economy. Due to the volatility and fast advance of technologies, tracking and understanding of this kind of economy is extremely difficult. For this reason, different interpretations of digital shadow economy can be found in the scientific literature, depending on the aim, object and nature of the particular study.

Minding its offensive nature, the concept digital shadow economy is equalized with the concept of "digital underground economy", which is described as offences committed exploiting networked technology to carry out incredibly complex and far-reaching tasks that can be repeated countless times globally (Yip et al., 2012). With reference to Moore, Clayton and Anderson (2009), digital underground economy is the online trading, performed in the blatant manner with no need to hide. Herley and Florencio (2010) interpret digital underground economy as Internet-based crime, which is profit-driven, and the nature of this activity exceeds the capacity of a closed group.

Considering criminal activities as the main feature of digital underground economy, it can be proposed that the concept of digital underground economy is closely related to the concept of cybercrime. Cybercrime is interpreted as a robust underground economy that is industrialized by making and delivering the tools for criminal behaviour (Mello, 2013) or technological advanced criminal activities, including the utilization of botnets, targeted attacks or custom malware, that cause serious threats for consumers, organizations and enterprises as well as for the public sector (Vlachos et al., 2011). According to Smith (2015), "cybercrimes are Internet-based crimes conducted remotely to illegally take wealth or resources from others. Stolen resources can include Internet access, computer hard drive space, financial resources, intellectual capital and other data or bandwidth. Illegality is defined by the governmental jurisdiction in which the crime is conducted, not from where the attack was launched" (p. 104).

The above presented definitions of cybercrime are basically linked with the activities of illegal service providers or sellers, which is logical since namely these subjects generate the illegal money flows in digital shadow economy. However, the concept of digital shadow economy should not be restricted only with generation of illegal money flows. Customers' illegal activities in e-space (i.e. getting particular products or services online without paying for them or paying only a part of the decent amount) should also be treated as a part of digital shadow economy since they deprive a legal seller or service provider from the revenues that could have been legally earned, accounted and declared. In the scientific literature, customers' illegal activities in e-space are usually linked with the term of e-fraud. E-fraud is understood as consumption of illegal copies of digital products services (Ho & Weinberg, 2011; Taylor, 2012; Arli et al., 2015), the breach of the contract established online (Hjort & Lantz, 2012) or the breach of the trust between the contract parties (Amasiatu & Shah, 2014). With reference to Amasiatu and Shah (2014), the trust is breached when one party reneges on the contract agreement. In first party fraud, the customer is the party who has acted dishonestly by violating the contract terms, in order to profit from his dishonesty. These acts of dishonesty by the customer are called first party frauds (Amasiatu & Shah, 2014).

Summarising, it can be stated that the concept of digital shadow economy is linked with illegal activities in cyberspace that enable to generate illegal money flows for illegal service providers or sellers (supplier's view) and deprive legal service providers and sellers from the revenues which could have been legally earned, accounted and declared (customer's view). Treating digital shadow economy as a system, it is considered to be a merger of digital and classical crime (Holz et al., 2012).

3. The Forms of Digital Shadow Economy in Digital Black Markets

Thomas and Martin (2006) gave the insight into digital shadow economy, analysing such form of its evidence as trading stolen credit card credentials over open Internet Relay Chat (IRC) channels. This form of digital shadow economy was later acknowledged by other authors (Herley & Florencio, 2010; Yip et al., 2012).

In the last few years, the interest in the forms of digital shadow economy has even increased, and a wider variety of the forms of digital shadow economy has become an object of the scientific research. Mello (2013) introduces the five following forms of cybercrime:

- Data breaches – stolen identities that drive industrial fraud complex through social networks such as Twitter, LinkedIn and LivingSocial's and others.
- Malware – fraud apps, typically used to impersonate a victim or gain access to their credentials. In many

cases, malware is designed to avoid detection by both human users and the anti-virus scans that may be running on a device.

- Mobile threats – malware by mobile and smart phones.
- Industrialisation – since online and mobile interactions are 'machine-to-machine', i.e. user's device is interacting with a business's server, cyber interactions lend themselves to automation. Once a fraudster secures the credentials required to access a victim's accounts, a process, in which multiple accounts are accessed automatically, can be started.
- Distributed Denial of Service Attacks – disruptions of the operations of a website, usually leading to an increased call centre activity, which drives up an organization's costs and undermines customers' trust in it.

Analysing the landscape of cybercrime in Greece, Vlachos et al. (2011) introduced such cybercrime forms as financial frauds (frauds that have financial incentives, from simplistic phishing attacks to pump "n" dump and money mule schemes), children issues (any case of children abuse, including children pornography or paedophilia), spams (unsolicited bulk e-mail that affects the performance of internet users and is related to fraudulent merchandise), breaches of privacy and personal data (all the incidents that are related to privacy issues and personal data, which were intercepted or obtained by electronic devices), technological advanced activities (including utilization of botnets, targeted attacks or custom malware), online games (serving for the stealing of accounts, illegal transfers of virtual money and virtual goods) and technical issues (deliberately caused technical problems related directly to computer or system security).

Yip et al. (2012) analysed online social networks, better known as carding forums (Holt & Lampke, 2010; Poulsen, 2011). According to the authors (Yip et al., 2012), online social networks previously were used as online black markets for trading of stolen data. However, their present activities cover sharing techniques, values of crime, trading of goods and services, forming of collaborations (Thomas & Martin, 2006; Holt & Lampke, 2010; Yip et el., 2012) and carding (money mule, bank data stealing, ID thefts, virtual currency exchanges, encoding of systems, etc.) (Holt & Lampke, 2010).

Researching digital underground economy that trades stolen digital credentials, Holz et al. (2012) investigated keylogger-based stealing of credentials via dropzones (publicly writable directories on a server in the Internet) as well as anonymous collection points of illicitly collected data. With reference to the authors, keylogger-based stealing is a newly emerging form of digital underground economy. The results of their research revealed that this technique is basically applied targeting the main online banking websites as well as extracting the information from the protected storage.

The above described forms of digital shadow economy emerge as supplier-initiated since their main aim is generation of illegal money flows to the supplier. However, since the researched phenomenon is also linked with consumers' activities that deprive legal service providers and sellers from the revenue that could have been legally earned, accounted and declared, it is purposeful to review the consumer-initiated forms of digital shadow economy.

Digital piracy is one of the most common forms of e-fraud, researched in the scientific literature. With reference to Ho and Weinberg (2011), digital piracy is a type of product piracy, emerging as the acts of producing, acquiring and/or consuming illegal copies of any authentic product. In more detail, it is buying, copying, downloading, and/or sharing illegal CDs and software (Arli et al., 2015), perplexing the service marketers, who produce easily-replicable digital products such as music (International Federation of the Phonographic Industry, 2009), movies (Castro, Bennett, & Andes, 2009), software (Business Software Alliance, 2009), etc. Thus, in the general cases of digital piracy, there remains a central premise that individuals, engaged in product piracy, benefit at the expense of the rightful owners of the authentic products/brands (Ho & Weinberg, 2011).

Amasiatu and Shah (2014) in their study focused on the forms of fraudulent consumer behaviour in e-tailing. The results of their research have enabled to identify the following forms of consumer e-fraud:

1. Deshopping – purchasing of a product online and using it with the intention to return after use for reimbursement.
2. Chargeback – making a fraudulent or illegitimate claim for financial gain.
3. Bust out – acquisition of credit facilities with no intention of honouring the credit agreement.
4. Misrepresentation of details – applicants' misrepresentation of their details to get access to facilities that they would not otherwise be entitled to, e.g. credit facilities.

The analysis of the scientific literature has revealed that deshopping is the prevalent form of consumer e-fraud (Hjort & Lantz, 2012; Amasiatu & Shah, 2014) and is frequently considered as a consequence of liberal return policies offered by e-retailers. Hjort and Lantz (2012) also noted that deshopping is reinforced by the offer of free returns; it is also initiated due to mitigation of consumer's total expenditure and delivery costs.

The common methods of chargeback, pointed in the scientific literature, include alleging that a customer has not

received the ordered commodities, although he in fact has, or claiming that not all ordered commodities were received, although they in fact were (Greek, 2010; Amasiatu & Shah, 2014). With reference to the report of Cybersource Corporation (2012), chargeback fraud can arise when a customer makes a purchase with his/her card and subsequently denies making this purchase. According to Amasiatu and Shah (2014), "chargeback frauds are opportunistic in nature and originated because of certain legal obligations (such as long distance regulation) designed to protect legitimate customers when they shop online; such as offering customers protection from payment card fraud and placing responsibility of any loss that occurs prior to delivery to the customer on the online merchant" (p. 811).

With reference to Fair Isaak Corporation (2008), bust out frauds commonly take place in financial institutions because of the availability of credit facilities. Amasiatu and Shah (2014) also note that extreme cases of bust out include the customers masking their intentions or hidden agenda by "lying low" for some period, which might later result in getting access to increased credit facilities that are rapidly utilized before evading the payment and disappearing.

With reference to CIFAS (2012), misrepresentation of details is prevalent in the mail order industry, where individuals hide their addresses with adverse credit information. They also emerge in insurance industry where customers inflate insurance claims as well as in the welfare/benefit system where benefit claimants misreport their earnings to benefit from the system (Amasiatu & Shah, 2014).

The performed analysis of the scientific literature has enabled to systematize the forms of digital shadow economy. The data presented in Figure 1 shows that digital shadow economy might emerge as supplier-initiated or customer-initiated. The most common supplier-initiated forms of digital shadow economy include financial frauds, children issues, spams, data and privacy breaches, online games, technological advanced activities, technical issues and carding. These forms are usually engaged for stealing of credentials, money mule, virtual currency exchanges, illegal transfers of virtual money, encoding of systems, malware and fraudulent merchandise. Consumer-initiated forms of digital shadow economy include digital piracy, deshopping, chargeback, bust out and misinterpretation of details. They are engaged for mitigation of consumer's total expenditure and delivery costs, getting access to increased credit facilities, inflation of insurance claims and claiming for welfare benefits.

With reference to Zorz (2015), different forms of digital underground economy emerge in different types of digital black markets, depending on the type of targeted products or services. Considering the object of activities (i.e. whether it is a non-digital product or service or a digital one), the author distinguishes two basic types of digital black markets: physical black market (online trading of illegal physical products such as guns, drugs or other non-digital services) and fraudulent data market (digital activities such as encoding, data breaches and similar system interferences). According to the author, the first market functions via Internet platforms (for example, TOR network), which allow anonymous clients and hosters to hide their locations, ensuring that their activities and identities cannot be tracked. The second market functions via traditional HTTP-based sites, accessible from any computer with a common web browser, and these sites are designed for dealing with stolen target data (for instance, credit card information, usernames and passwords, credential data are considered to be the most prevalent types of digital data offered for sale). Digital shadow activities are basically performed via such channels as IRC, carding forums, social networks and dropzones.

4. Comparative Analysis of Traditional and Digital Shadow Economy

Although considering its complex structure, digital shadow economy can be viewed as a merger of digital and classical crime (Holz et al., 2012), particular differences between the aims, communications, features of the people involved, sources of the people's knowledge, psychology and the ways of operation in traditional and digital shadow economy can be observed. Systematization of the scientific literature has enabled to perform a comparative analysis of traditional and digital shadow economy. The results of the comparative analysis have been reflected in Table 1. By reviewing the table, it can be seen that the nature of both traditional and shadow economy is the same – illegal and criminal, but the aims of the latter are wider – they include not only pure profit, but also access to particular resources (e.g. particular databases, accounts, systems, etc.). The participants in both cases are driven by such similar determinants such as unfavourable labour market conditions, high taxation or complicated overall regulation. However, social security burdens are more typical of traditional shadow economy whereas digital shadow economy is to the great extent determined by specific cyberspace determinants such as contrast between personal and corporate, anonymity, lack of ethics in software and IT business, inclusion that online act is victimless, doubtful copyrights, low level of perceived risk, etc. The basic method of finance in traditional shadow economy is cash whereas digital shadow economy is funded engaging Web money, electronic money, online payment systems and well-hidden financial transactions, which are often processed by legitimate merchant accounts or payments from credit card companies. Traditional shadow economy functions leaning on such marketing methods as words of mouth and underground distribution channels whereas in the case of digital

shadow economy products and services are positioned online, in particular cases even engaging customer support centres. With reference to "Trend Micro" report (2010), there is evidence that some pay-per-install businesses have established customer support centres to help their customers, who call to these centres for help thinking they have paid for a legitimate software. Interestingly, the security level of digital shadow economy is much higher than that of traditional one. It is linked with high technical skills of the people, who are commonly involved in digital shadow economy, although these participants are usually self-taught. According to Smith (2015), cybercriminals are able not only to use attack programs that are freely available on the Internet, but also they may develop new attack software by writing malware programs themselves. To make their targeted attacks over the Internet, they need to have an understanding of computer operating systems and the software packages being used on those systems. In addition, they must know how to gain unauthorized access by exploiting computer networks, which requires high technical skills. Digital shadow economy not only covers much wider (international) geographic area in comparison to traditional local shadow economy, but also is based on social psychology alongside with individual one. With reference to Li (2011), participants interact with each other in an online community. Hence, their behaviour is influenced not only by their personal motivations (e.g. aim for benefit, cost mitigation), but also by the influence of the other members of the community (e.g. their advice, responses, pressure, etc.). Finally, comparing the way of operation in both economies, it has been established that the participants of digital shadow economy are more inclined to collaboration and networking than the ones acting in traditional shadow economy. With reference to Yip et al. (2012), it is usual for cybercriminals to begin collaborating with one another while trading goods and services that contribute to the crime; some of the cybercriminals even venture as far as recruiting talents from universities.

Summarising, the results of the comparative analysis propose that digital shadow economy is of the same illegal nature and involves the same participants as traditional shadow economy. However, other significant characteristics are rather different. Contrary to the traditional shadow economy, digital shadow economy it is aimed not only at profits, but also at the access to valuable digital, financial resources and/or databases. It is highly determined by specific cyberspace determinants such as contrast between personal and corporate, anonymity, lack of ethics in software and IT business, inclusion that online act is victimless, doubtful copyrights, low level of perceived risk, etc. Funded with Web money, electronic money, online payment systems and well-hidden financial transactions, digital shadow economy leans on positioning of products and services online (in particular cases – with established customer support centres), online communication between the parties of transactions, social psychology and networking, which enables to cover international operation areas. High technical skills of the people involved allow to achieve a comparatively high operation security level in comparison to traditional shadow economy.

5. Conclusions and Discussion

With reference to the research results, the following conclusions can be made:

1. The analysis of the concepts and interpretations of digital shadow economy has revealed that the term of digital shadow economy is linked with illegal activities in cyberspace that enable to generate illegal money flows for illegal service providers or sellers (supplier's view) and deprive legal service providers and sellers from the revenues which could have been legally earned, accounted and declared (customer's view).
2. Depending on the initiating subject, digital shadow economy might emerge as supplier-initiated or customer-initiated. The most common supplier-initiated forms of the analysed phenomenon include financial frauds, children issues, spams, data and privacy breaches, online games, technological advanced activities, technical issues and carding, which are commonly engaged for stealing of credentials, money mule, virtual currency exchanges, illegal transfers of virtual money, encoding of systems, malware and fraudulent merchandise. Consumer-initiated forms of digital shadow economy include digital piracy, deshopping, chargeback, bust out and misinterpretation of details, which are engaged for mitigation of consumer's total expenditure and delivery costs, getting access to increased credit facilities, inflation of insurance claims and claiming for welfare benefits. Depending on the object of activities/trade, two basic types of digital black market – physical black market and fraudulent data market – can be distinguished; shadow activities in these markets are basically performed via such channels as IRC, carding forums, social networks and dropzones.
3. The results of the comparative analysis of traditional and digital shadow economy have shown that digital shadow economy is of the same illegal nature and involves the same participants as traditional shadow economy. Digital shadow economy is the part of shadow economy. However, contrary to the traditional shadow economy, digital shadow economy it is aimed not only at profits, but also at the access to valuable digital, financial resources and/or databases. It is highly determined by specific cyberspace determinants such

as contrast between personal and corporate, anonymity, lack of ethics in software and IT business, inclusion that online act is victimless, doubtful copyrights, low level of perceived risk, etc. Funded with Web money and electronic money, digital shadow economy leans on positioning of products and services online, online communication between the parties of transactions as well as social psychology and networking, which enables to cover international operation areas. High technical skills of the people involved in digital shadow operations allow to achieve a comparatively high operation security level in comparison to traditional shadow economy. Undoubtedly, it is a wrong way of thinking that in traditional shadow economy payments are made only in cash since in recent decade the substantial number of operations have been transferred to electronic space. What is more, shadow economy should be distinguished from criminal activities.

The analysis of the variety of information sources on the researched object proposes that the scientific literature still lacks of comprehensive and complex studies on digital shadow economy. The spread of the access to IT and e-services all over the world determines the favourable conditions for the diffusion of digital shadow economy. Thus, the future research on digital shadow economy could be aimed at identification of the features, determinants and operation models of this phenomenon as well as possible prevention strategies and measures.

References

Amasiatu, C. V., Shah, M. H. (2014). First party fraud: A review of the forms and motives of fraudulent consumer behaviours in e-tailing. International *Journal of Retail & Distribution Management, 42*(9), 805-817.

Arli, D., Tjiptono, F., & Porto, R. (2015). The impact of moral equity, relativism and attitude on individuals' digital piracy behaviour in a developing country. *Marketing Intelligence & Planning, 33*(3), 348-365.

Business Software Alliance. (2009). *Software piracy on the internet: A threat to your security* (A report). Retrieved from http:// global.bsa.org/internetreport2009/2009internetpiracyreport. pdf

Calluzzo, V., & Cante, C. (2004). Ethics in information technology and software use. *Journal of Business Ethics, 51*(3), 301-312.

Camarero, C., Anton, C., & Rodriguez, J. (2014). Technological and ethical antecedents of e-book piracy and price acceptance: Evidence from the Spanish case. *The Electronic Library, 32*(4), 542-566.

Castro, D., Bennett, R. & Andes, S. (2009). Steal these policies: Strategies for reducing digital piracy. *The Information Technology & Innovation Foundation, 12*. Retrieved from www.itif.org/files/2009-12-15.DigitalPiracy. pdf

CIFAS. (2012). *Fraudscape: depicting the UK's fraud landscape* (Research and Reports). Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Reports/External-Fraudscape_2013_Cifas.pdf

Cybersource Corporation. (2012). *13th annual online fraud report.* Retrieved from www. jpmorgan.com/cm/BlobServer /13th_Annual_2012_Online_Fraud_Report.pdf?blobkey¼id&blobwhere¼1320571432216&blobheader¼application/pdf&blobheadern ame1¼Cache-Control&blobheadervalue1¼private&blobcol¼urldata&blobtable¼MungoBlobs

Europol. (2011). *Cybercrime as a business: The digital underground economy* (Press Releases). Retrieved from https://www.europol.europa.eu/content/press/cybercrime-business-digital-underground-economy-517

Fair Isaak Corporation. (2008). *Reducing bad debt levels by addressing first party fraud and credit abuse* (white paper). Retrieved from http://brblog.typepad.com/files/first_party_fraud_2486wp_en.pdf

Greek, D. (2010). *Who is responsible when goods go missing in transit?* Retrieved from www.computeractive.co.uk/ca/consumer-rights/1931458/missing-transit

Herley, C., & Florencio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. *Economics of Information Security and Privacy, 10.* Retrieved from http://link.springer.com/chapter/10.1007%2F978-1-4419-6967-5_3#page-1

Hjort, K., & Lantz, B. (2012). (R)e-tail borrowing of party dresses: An experimental study. *International Journal of Retail & Distribution Management, 40*(12), 997-1012.

Ho, J., & Weinberg, C. B. (2011). Segmenting consumers of pirated movies. *Journal of Consumer Marketing, 28*(4), 252-260.

Holt, T.J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Holz, T., Engelberth, M., & Freiling, F. (2012). Learning more about the underground economy: A case-study of keyloggers and dropzones. *ESORICS Proceedings, 9,* 1-18.

International Federation of the Phonographic Industry. (2009). *New business models for a changing environment* (Digital music report). Retrieved from www.ifpi.org/content/ section_ resources/dmr2009.html

Li, D. C. (2011). Online social network acceptance: a social perspective. *Internet Research, 21*(5), 562-580.

Lisi, G. & Pugno, M. (2010). Entrepreneurship and the hidden economy: An extended matching model. *International Economic Journal*, 24(4), 587-605.

Lysonski, S., & Durvasula, S. (2008). Digital piracy of MP3s: Consumer and ethical predispositions. *Journal of Consumer Marketing, 25*(3), 167-178.

Mello, J. P. (2013). *Cybercrime fueled by mature digital underground* (Identity & Access). Retrieved from http://www.csoonline.com/article/2133649/identity-access/cybercrime-fueled-by-mature-digital-underground.html

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives, 23*(3), 3-20.

Ojo, S., Nwankwo, S. & Gbadamosi, A. (2013). Ethnic entrepreneurship: The myths of informal and illegal enterprises in the UK. *Entrepreneurship & Regional Development: An International Journal*, 25(7-8), 587-611.

Poulsen, K. (2011). *Kingpin: How one hacker took over the billion-dollar cybercrime underground*. New York: Crown Publishing.

Schneider, F., Buehn, A., & Montenegro, C. E. (2010). Shadow economies all over the world: New estimates for 162 countries from 1999 to 2007. *Policy Research Working Paper, 5356*. Retrieved from http://www-wds.worldbank.org/external/default /WDSContentServer/IW3P/IB/2010/10/14/000158349_20101014160704/Rendered/PDF/WPS5356.pdf

Shang, R., Chen, Y., & Chen, P. (2008). Ethical decisions about sharing music files in the P2P environment. *Journal of Business Ethics, 80*(2), 349-365.

Sirkeci, I., & Magnusdottir, L. B. (2011). Understanding illegal music downloading in the UK: A multi-attribute model. *Journal of Research in Interactive Marketing, 5*(1), 90-110.

Smith, G. S. (2015). Management models for international cybercrime. *Journal of Financial Crime, 22*(1), 104-125.

Taylor, S. A. (2012). Evaluating digital piracy intentions on behaviors. *Journal of Services Marketing, 26*(7), 472-483.

Thomas, R., & Martin, J. (2006). The underground economy: Priceless. *The USENIX Magazine*, *31*(6), 7–16.

Trend Micro. (2010). *The business of cybercrime: A complex business model* (Focus Report). Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf

Vida, I., Koklic, M. K., Kukar-Kinney, M., & Penz, E. (2012). Predicting consumer digital piracy behavior: The role of rationalization and perceived consequences. *Journal of Research in Interactive* Marketing, 6(4), 298-313.

Vlachos, V., Minou, M., Assimakopouos, V., & Toska, A. (2011). The landscape of cybercrime in Greece. *Information Management & Computer Security,19*(2), 113-123.

Wall, D.S. (2005). The internet as a conduit for criminal activity. In A. Pattavina (Eds.), *Information Technology and the Criminal Justice System* (78-94). California: Thousand Oaks.

Williams, C. C., & Nadin, S. (2012). Joining up the fight against undeclared work in Europe. *Management Decision,* 50(10), 1758-1771.

Williams, P., Nicholas, D., & Rowlands, I. (2010). The attitudes and behaviours of illegal downloaders. *Aslib Proceedings, 62*(3), 283-301.

Yip, M., Shadbolt, N., Tiropanis, N., & Webber, C. (2012). The digital underground economy: A social network approach to understanding cybercrime. In *Digital Futures 2012: The Third Annual Digital Economy All Hands Conference.* Retrieved from http://eprints.soton.ac.uk/343351/1/yip_de2012_submission.pdf

Yu, C. P., Young, M. L., & Ju, B. C. (2015). Consumer software piracy in virtual communities: An integrative model of heroism and social exchange. *Internet Research, 25*(2), 317-334.

Zorz, M. (2015). *Global black markets and the underground economy* (Featured News). Retrieved from http://www.net-security.org/article.php?id=2288

Table 1: Comparative analysis of traditional and digital shadow economy

Characteristic	Traditional shadow economy	Digital shadow economy
Nature	Illegal, criminal	Illegal, criminal
Aim	Profit	Profit and resources
Determinants	Labour market conditions (high unemployment rate, not promoted self-employment), taxation and social security burdens (high taxes, low after-tax earnings), overall regulation (administrative system, regulation complexity, difficult business registration procedures, etc.)	Taxation (high taxes, low after-tax earnings), overall regulation (administrative system, regulation complexity, difficult business registration procedures, etc.), cyberspace-related determinants (contrast between personal and corporate, anonymity, lack of ethics in software and IT business, inclusion that online act is victimless, doubtful copyrights, low level of perceived risk, etc.)
Participants	Service providers, product suppliers, customers	Service providers, product suppliers, customers
Finance	Cash, web money, electronic money, online payment systems	Web money, electronic money, online payment systems, well-hidden financial transactions are processed by legitimate merchant accounts
Marketing	Word of mouth, underground distribution channels, services online	Positioning of products and services online
Customer service	No customer service, usually relationship between a buyer and a seller break after the transaction, but not in all cases	In particular cases – established customer support centers
Communication	Face-to-face, Online	Online
Security	Comparatively high	Comparatively high
Geographical area	Local and international	International
Features of the people involved	Skills in an operation area, the level of technical skills is significant	Wide range of skills, high technical skills
Source of knowledge	Apprenticed, but also could be self-taught	Self-taught and apprenticed
Psychology	Individual and social (tax moral)	Individual and social
Way of operation	Single activity, collaboration, networking	Collaboration, networking

Source: compiled by the authors with reference to Trend Micro, 2010; Yip et al., 2012; Ojo, Nwankwo, & Gbadamosi, 2013; Smith, 2015; Williams & Nadin, 2012; Schneider, Buehn, & Montenegro, 2010; Lisi & Pugno, 2010; Williams et al., 2010; Calluzzo & Cante, 2004; Wall, 2005; Shang, Chen, & Chen, 2008; Lysonski & Durvasula, 2008.

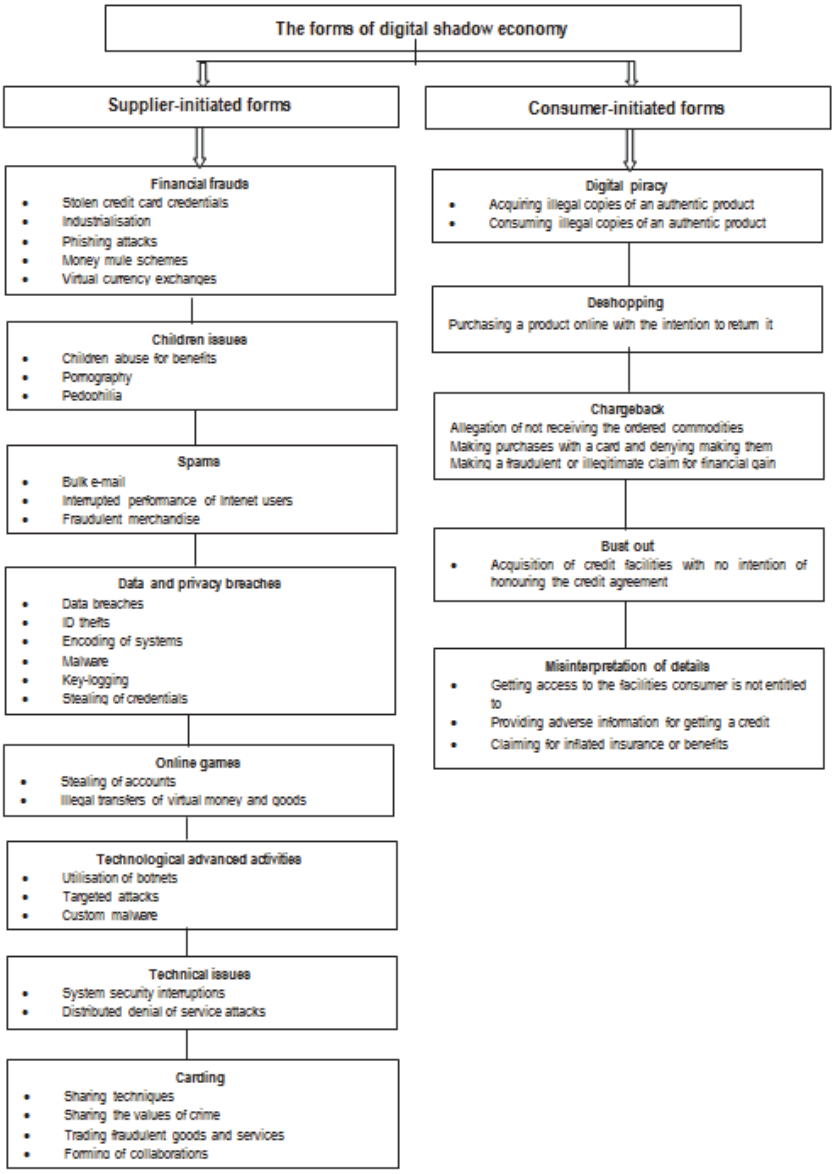

Fig. 1. Classification of the forms of digital shadow economy (compiled by the authors).