# Cybercrime Firms' Internationalization Strategy and Tactics: An Exploratory Framework

***Completed Research Full Paper***

**Nir Kshetri**
University of North Carolina—Greensboro
**nbkshetr@uncg.edu**

## Abstract

Cybercrime firms (CCFs) have significant global outreach. Combining insights from theories on white-collar crime (WCC), international relations (IR)/international political economy (IPE) perspectives, export market selection process, and market failures, we analyze CCFs' operations and internationalization. We present research findings from multiple case studies of CCFs to interrogate the above theories and to refine, extend and further develop their arguments. Extending WCC theory, resource constraints in countries with weak rule of laws result law enforcement apparatus' inability to cope. The IR/IPE provides additional insights by explicating mechanisms by which an economy's international integration can drive investments law enforcement resources. It explains the stages associated with CCFs' export market selection processes. Finally, we view that CCFs make excess/supranormal profits, for which market failure is necessary.

Keywords: cybercrime firms; cybersecurity; internationalization; jurisdictional arbitrage; supranormal profits; white-collar crime

## 1. Introduction

Some cybercrime firms (CCFs) have significant global outreach. For instance, the Conficker botnet reportedly controlled 7 million computer systems at 230 regional and country top-level domains (Mullins, 2010). As of February 2016, a criminal gangs involved in the so called CEO frauds had victimized companies in 108 countries (Scannell, 2016). Another similar example is Tartu, Estonia-based Rove Digital (RD). An international gang associated with RD used malicious software to hijack more than 4 million computers in over 100 countries (Bray, 2011). Some CCFs such as closely imitate business models of reputable legitimate corporations (Goodman, 2011; Kshetri, 2010).

Two intriguing observations can be made regarding CCFs' operations. First, many CCFs' activities have been extremely profitable. For instance, RD made US$14 million in profits in less than five years of its operations (Kshetri, 2013). According to the Internet Crime Complaint Center (I3C), the criminal gang involved in CEO frauds made US$2 billion in a few years (Scannell, 2016).

Second, there is generally an extremely low arrest and prosecution rates for cybercrimes. The U.S. Federal Bureau of Investigation (FBI) estimated that the probability of a cybercriminal's being caught was less than 1 in 20,000 and the overall conviction rate for a person accused of engaging in cybercrimes was 1 in 22,000 (Gabrys, 2002).

International business (IB) researchers typically study multinational enterprises (MNEs) engaged in formal, legal and legitimate economic activities crossing national borders. And for many reasons these issues are considered to be important. In some recent studies IB researchers have acknowledged the existence and importance of informal cross-border network organizations. By promoting the flow of economic and non-economic remittances in the forms of money and ideas, informal cross-border organizations such as diaspora networks have facilitated the formation and growth of new ventures (Oviatt & McDougall, 1994). Examples of such activities include micro-enterprises in developing countries funded by migrant remittances from abroad (Vaaler, 2011).

It is likely that some cross-border flows of money and ideas may shift from legally-questionable but legitimate business use (e.g., an unlicensed barbershop) to illegitimate business use (e.g., drug dealing). The focus of this paper is on the latter issue. CCF activities are cross-border in nature, organized with formally-defined or informally-understood responsibilities, not legally-sanctioned, and largely deemed as undesirable and thus illegitimate by community members, including those forced to "do business" with the CCFs.

The idea in this paper is to analyze CCFs' activities in ways that are analogous to other more conventional MNEs. Such an analysis helps researchers understand CCFs better. By developing a clearer understanding of how CCFs operate, organizations and individuals should be better able to defend against them and contribute to their control and eradication.

There are two fundamental considerations. First, whereas legitimate firms voluntarily exchange goods and services, CCFs are engaged in illegal activities. This means that the key actors in CCF networks prefer to be in places which are beyond the reach of the law-enforcement efforts. Second, based on the examples presented above, it can be argued that some CCFs are making supranormal profits. Two natural questions arise: RQ1) what strategies are used by CCFs to maximize security? RQ2) what are the basic mechanisms associated with CCFs' supranormal profits?

At the outset it must be clearly stated that there obviously are methodological, conceptual, logical, and statistical challenges in researching CCFs' internationalization. Nonetheless, instead of burying our heads under the sand, it would be better to address this issue with whatever clarity, rigor, and systematization that can be achieved.

The theory that emerges is that in order to maximize security, CCFs locate their strategic resources in jurisdictions with weak rules of law and/or low degree of law enforcement cooperation with victims' jurisdictions. In order to increase profitability, CCFs prefer pursuing targets that are characterized by weak cybersecurity (CS) mechanisms, high digitization of economic activities and low propensity to report to law enforcement agencies. Their modus operandi include relying on alliances that are physically located in the victims' jurisdiction and taking measures to make their virtual and physical activities undetectable and untraceable.

## 2. Literature Review

In order to analyze the jurisdictions in which CCFs tend to locate key resources, we apply two different theoretical frameworks. The literatures on white-collar crime (WCC) could be particularly helpful for identifying important causes and dynamics associated with individuals' engagement in cybercrime activities and the emergence of CCFs. Just like the WCCs (Tillman et al., 1996), cybercrime cases are complex and thus require substantial resources to investigate and prosecute. The international relations (IR)/international political economy (IPE) perspectives provides additional insights by explicating the mechanism by which an economy's international integration can drive the investment in such resources. With the decline of violent geopolitical conflicts, traditional issues such as nuclear war are losing salience and the focus and organizing principle in international relations have been on nontraditional security issues (Andreas & Price, 2001). Cyber-threat is increasingly recognized as a legitimate security issue (Kshetri, 2013a).

Next, most CCFs' internationalization is more akin to export than foreign direct investment (FDI). The export market selection process is thus more relevant to the context of this paper than foreign market selection or international market selection (Papadopoulos & Denis, 1988). Note that the latter pertain to the evaluation of markets for possible entry by means of modes other than export such as FDI.

Finally, one way to view CCFs' operations is to say that they are making excess profits from their operations. Economic theory emphasizes the effectiveness of markets in limiting profits to an average level. Market failures are necessary for supranormal profits, which needs the presence of "impediments to economic activity" (Yao, 1988, p. 59).

# 3. Method

The approach of this study can be described as theory building from multiple case studies, which is becoming increasingly popular in social science (Eisenhardt & Graebner, 2007). Connection with related literatures, establishment of theoretical gaps in the literature, and explicit statement of research questions to address the gaps are the key features of strong empirical research (Eisenhardt & Graebner, 2007). In qualitative research, it is also important to make a strong case for the importance of the research questions that have been raised (Bansal and Corley, 2012). We have established theoretical and practical importance of research on CCFs' internationalization.

*Selection of cases*
A potentially valuable research design to test the conceptual framework via multiple case studies would be to sample CCFs that engaged in cybercrime activities for financial gains. It is important to include CCFs with different strategies and levels of success to keep them beyond the reach of law enforcement efforts (security) as well as those that pursue different markets and strategies for maximizing profitability. Multiple cases are chosen for theoretical reasons which include (contrary) replication, a theory's extension and elimination of alternative explanations (Yin, 1994). In order to meet the above-mentioned criteria, a total of fifteen cases of CCFs have been selected.

# 4. CCFs' Internationalization Strategy and Processes

Eisenhardt and Graebner (2007) suggested providing a visual theory summary in the form of "boxes and arrows" diagram. To this end, Figure 1 presents a preliminary conceptual framework. In well-done case study research, theory and data are likely to be "patternmatched" and the propositions are consistent with most or all the cases (Eisenhardt & Graebner, 2007). In this regard, Table 1 provides a visual theory summary, matching with the cases.

*Maximizing security*
Location of strategic resources in jurisdiction with weak rules of law

The criminal gangs operating Rustock (case 5), RBN (case 9), and Rock Fish malware (case 11) operated from Russia. In the widely publicized coreflood case, the FBI and the DOJ filed a civil complaint against 13 "John Doe defendants", who were believed to be in Russia (case 1). Likewise, in the RD case, while the Estonian fraudsters were extradited to the U.S., one Russian involved in the case is on the loose (case 6). Another interesting observation is that Rustock had data centers in seven U.S. cities, where 96 servers had acted as the C&C system. The C&C servers were located in middle-America where it would face less regulatory scrutiny compared to major metropolitan areas (bbc.co.uk, 2011) (case 5).

Limited organizational resources and high caseload pressures lead to some governments' ability to investigate and prosecute (Pontell et al., 1994). Just like WCCs (Tillman et al., 1996), resource limitations are of particular concern for cybercrimes due to their complexity.

Locating in countries with low degree of law enforcement cooperation with victims' jurisdictions
The RBN (Case 9) reportedly sold website hosting services to cybercriminals. Cybercrimes targeting foreign victims are committed from Russia almost with impunity (Krebs, 2007). Regarding the operation of criminal gangs such as Rustock (case 5), RBN (case 9), and Rock Fish malware (case 11), Russia's difference with the West in legal and law enforcement matters is important (e.g., Hathaway et al., 2012).

One observation is that the founders of RD (case 6) could not protect themselves from law enforcement in Estonia. International pressures have led to the modernization of Soviet–era legislative framework and institutional structures of Estonia. Due to Estonia's high degree of integration with the west, cybercriminals are jurisdictionally "less shielded" compared to those in Russia. A similar conclusion can be deduced from a comparison of Russia and Ukraine. While Russia has established distance with the West, Ukraine has shown more willingness to cooperate and integrate. In 2010, the SBU arrested five alleged kingpins behind Zeus (case 3) (Onyshkiv & Bondarev, 2012).

*Maximizing profitability*
Pursuing targets with high digitization

Online casinos, banks, and e-commerce hubs are an industry sweet spot (cases 3, 10, 13). Most CCFs have found the U.S. market as a lucrative target. Regarding CCFs' market selection process (Kumar et al., 1994; Williamson et al., 2006), using variables specific to the cybercrime industry, while a short list may contain a number of countries, many CCFs chose the U.S. for the final selection. Operations in the U.S. can lead to a higher profitability due to a large number of computers and high digitization. The banker malware (case 7) is detected only in Brazil (Kazymirsky et al., 2016). Brazilian CCFs have not realized the need for internationalizing due to well-developed domestic financial sector.

### Pursuing newer domains

CCFs are finding it more attractive to monetize mobile malware. One example is Zitmo banking Trojan (or Zeus-in-the-Mobile) allegedly developed by the creators of Zeus (case 3). Likewise, RBN (case 9) stopped operations in November 2007. Some analysts suspected that "whatever protection RBN enjoyed was withdrawn because the group had overreached itself" (Espiner, 2007). Analysts also suggested that the group operating RBN may have shifted its operations to China and other Asian countries (Blakely et al., 2007). In the same vein, following the seizure of Coreflood's C&C servers by the DoJ and the FBI in 2011, the malware evolved with more than 100 updates (case 1). Regarding the success of RD (case 6), it is worth noting that most traditional malware is designed to steal valuable personal information. RD's scheme was on a newer domain and thus was not easily detected. Experts considered this as a very clever tactic as it manipulated the infrastructure of the Web involved in doing one of the most popular activities: display advertising.

The above strategies can be considered to be an attempt to shift the underlying demand by filling the niches between existing products (Yao, 1988). The gang involved in the CEO fraud used the lure of promotion in order to defraud employees (case 14). This strategy can be considered as finding a new dimension of product space (Yao, 1988).

### Low propensity to report

Internet gambling sites based in the Caribbean and Central America, most notably in Costa Rica, Aruba and Antigua, have been an easy target for online extortionists (case 10) (Kshetri, 2005). Such sites are illegal in the U.S. Police in these countries are poorly equipped to fight sophisticated cybercrimes (Baker, 2004). Some casino operators face indictments in the U.S. on illegal gambling charges. Law enforcement agencies such as the FBI do little to defend these sites. Grey-area businesses thus provide particularly appropriate examples.

Regarding transactions costs, excluding nonbuyers from the use of a product or service (Yao 1988; Arrow 1970) are key components. CCFs exclude law enforcement agencies from the access to information.

#### *Weak defense mechanism*

CCFs prefer to pursue targets with weak mechanisms. For instance, Zeus creator (case 3) reportedly found banks in Mexico and Chile as attractive targets as these banks employed weak single-factor authentication to secure their customers' accounts (Mathew, 2011). Likewise, out of 100,000 bots of Pushdo/Cutwail, 40% were in India (case 8).

Using the export market selection process, in the identification stage, variables specific to the product-based industry are used to generate a short list of countries that warrant further investigation in the selection stage (Kumar et al., 1994). For CCFs, markets with a lack of CS orientation of individuals and organizations provide an attractive target. Such markets are more likely to be shortlisted by CCFs and subsequently pursued.

#### *Pursuing victims in physically accessible jurisdictions*

Many Nigerian cybercriminals face barriers to travel to the U.S. due to strict immigration controls. They focus on developing economies such as India (case 4). Note that in the final stage of the export market selection process, firm specific criteria are used (Kumar et al., 1994; Williamson et al., 2006). Some CCFs exclude countries that cannot be accessed physically. In such cases, they focus on physically accessible jurisdictions, that is, those in which it is possible to make a physical presence.

Prior research indicates that political factors act as barriers to MNEs' activities in foreign locations (Dunning, 1988). Sinuraja (1995) observed that freer movement of people from the FSU economies to the West and vice versa stimulated the growth of organized economic crimes in FSU economies. For instance,

members of Russian organized crime groups intensified their efforts in gathering necessary information and formed networks (Williams, 1995).

*Establishment of predatory groups in foreign markets*
The Zeus creators (case 3) deployed predatory money mule gangs in the U.S. and the U.K. The stolen funds were transferred using money transfer agencies such as Western Union. The New York-based gang was operated by a Russian who supplied the mules with fake identity documents, and managed their activities. The gang stole over US$3 million from victims (Krebs, 2010). In 2010, the U.S. attorney's office in New York charged 37 defendants. It was noted that four of the defendants were "managers", "a few others" were recruiters, and the rest were mules.

Having predatory gangs in victims' jurisdiction can help address the problems of incomplete markets and transactions costs. This is because various market participants have different goals and may act opportunistically in pursuit of those goals (Williamson, 1975). The significant presence of transactions costs can make it more attractive to replace market arrangements with nonmarket arrangements such as vertical integration (Yao, 1988).

*Creation of reputation*
If users of machines infected by the banker malware (case 7) attempt to connect to their banks' websites, they are referred to fake login webpages (Kazymirsky et al., 2016). Similarly, in Dyre (case 13), when the infected victim tries to log in to bank websites, a new screen asks the victim to call a number to get help logging in. The criminals complete the wire transfer as soon as the victim hangs up the phone (Kuhn, 2015).In the CEO fraud (case 14), the phony accounts created to mimic the KPMG lawyer used the suffix @kpmg-office.com to trick individuals (Scannell, 2016).

Online extortionists rely on a different way to create and use reputation. After cracking into victims' computer systems, extortionists normally send e-mails demanding that ransoms as high as US$100,000 be sent via money transfer agencies (case 10). Gambling sites alone pay out millions of dollars in extortion money each year (Kshetri, 2005).

The prevalence of imperfect information (Yao, 1988) is probably the most important source of vulnerability that CCFs can exploit. Uninformed Internet users are more likely to fall victim to CCFs' tactics. In the above cases, CCFs attempted to create a false reputation, which has been possible due to anonymity of the Internet.

*Undetectability/untraceability of virtual and physical actions*
Nigerian scammers (case 4), who targeted vulnerable Indian job-seekers by promising fake jobs, had opened accounts in India's ICICI bank using fake documents (Ali, 2010). They bought data cards using someone else's identity. A version of Android malware found in China (case 12) automatically deletes messages sent from infected numbers to premium services (Nichols, 2011). The banker malware (case 7) and other Brazilian CCFs employ techniques to maintain stealthiness. In order to remain undetected, the banker malware changes basic security configurations. It turns off antivirus and firewall notifications, and disables browser certificate verification (Kazymirsky et al., 2016).

Regarding transactions costs as impediments to economic activity (Yao 1988), Arrow (1970), the costs associated with excluding nonbuyers from the use of a product or service and the costs of communication and information are key components. Related to the first category of costs, a main goal for most CCFs is to prevent non-victims from becoming aware of their tactics. In addition to non-victims, CCFs also want to make sure that law enforcement agencies and CS organization are not aware of the tactics.

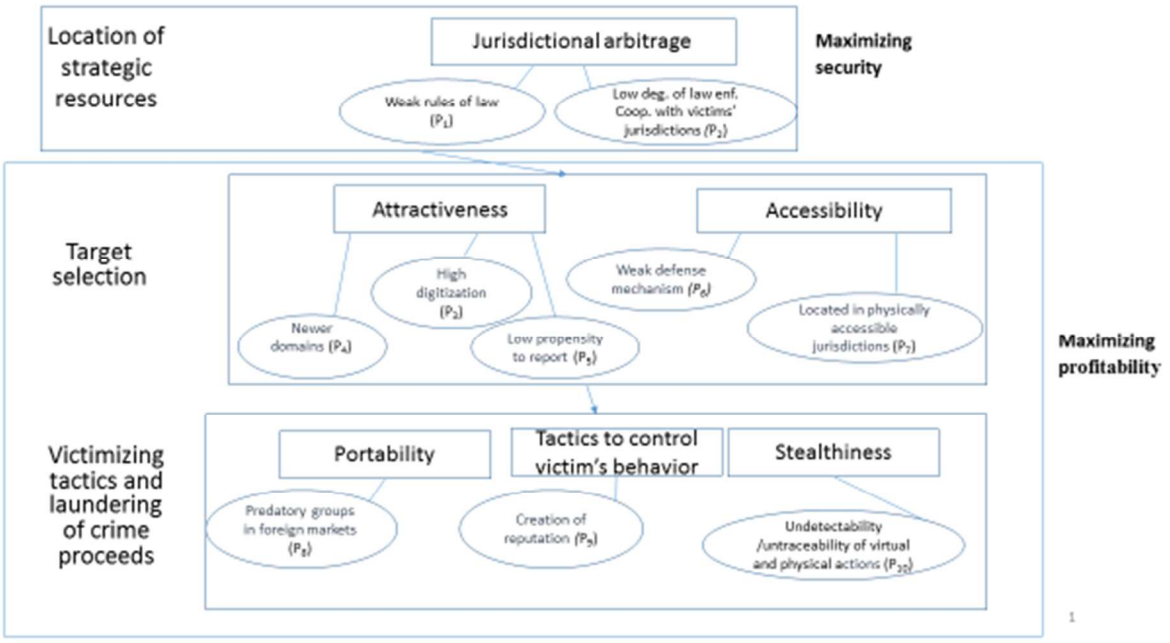
# 5. Discussion and Implications

Prior researchers have noted that there is a relative dearth of research related to the entrepreneurial process and related economic activities in the informal economy (Webb et al., 2009). This article addresses the dearth of literature by providing an analysis of special type of informal economy: cybercrime. It sheds some light on the CCFs' entrepreneurial activities by explicating the mechanisms by which they balance security and profitability expectations. Profitability is a function of targets selected and tactics used to victimize the targets and launder crime proceeds.

Figure 1 helps us see how various issues related to CCFs are different in an international context than in a purely domestic context. For instance, in some cases, jurisdictional arbitrage can only be accomplished by pursuing foreign victims. Also one way to benefit from such arbitrage is to victimize businesses and consumers in a country in which the home country government has a low degree of law enforcement cooperation. Second, foreign countries may be characterized by a higher density of profitable victims that are attractive and accessible. For instance, cybercrime strategies involving newer technological domains may be more suited to pursue foreign victims. Likewise, foreign locations can have potential victims that are highly digitized, exhibit low propensity to report and have weaker CS mechanisms. Finally some of the elements of the model (e.g., portability) are only relevant for foreign operations.

The various elements related to target selection in Figure 1 indicate that CCFs and legitimate firms are likely to differ in the criteria used in the export market selection. Countries with high density of grey area digital businesses (e.g., online betting websites) which have low propensity to report crimes to law enforcement agencies are likely to be shortlisted and finally selected by CCFs. These features may not be of interest to most legitimate firms. The above discussion also suggests that firm-specific strategic and business focus considerations determine CCFs' target selection, victimizing tactics and laundering of crime proceeds in order to maximize profitability. For instance, less-capable CCFs may focus efforts in pursuing victims with weak defense mechanism but that are less digitized and hence less attractive. More capable CCFs, on the other hand, may choose to target highly digitized victims or may focus efforts on newer domains.

**Figure 1: Cybercrime firms' internationalization strategy and processes**



| Dimension | Explanation | • Examples [Case No.] |
|---|---|---|
| Location of strategic resources | Weak rules of law | • Coreflood's "John Doe defendants" believed to be in Russia [1].<br>• IMU established in Ukraine by Westerners [2]<br>• Nigerian CCFs see India as a low risk country to operate [4]<br>• RD: Estonian alleged fraudsters were extradited to the U.S., one Russian involved in the case is on the loose [6] |
| | Low deg. of law cooperation with victims' jurisdictions | • Rock Fish malware operated from Russia [11]<br>• RBN sold website hosting services to cybercriminal [9]. |
| Target selection | High digitization | • Online casinos, banks, e-commerce hubs are attractive [3, 10, 13]<br>• The banker malware detected only in Brazil [7] |
| | Newer domains | • Zitmo banking Trojan [3]<br>• Ppromotion as an incentive to motivation and commitment [14]<br>• RD manipulated the infrastructure of the Web [6]. |
| | Low propensity to report | • Grey-area businesses such as gambling sites based in the Caribbean and Central America are easy target for online extortionists [10]<br>• Some casino operators face indictments in the U.S. |
| | Weak defense mechanism | • Zeus found banks in Mexico and Chile as attractive targets [3]<br>• Most bots of Pushdo/Cutwail were in India [8] |
| | Physically accessible jurisdictions | • Nigerian gangs focus on developing economies such as India [4].<br>• Zeus in the U.S. [3] |
| Victimizing tactics and laundering of crime proceeds | Predatory groups in foreign markets | • The Zeus creators deployed predatory money mule gangs in the U.S. and the U.K. [3] |
| | Creation of reputation | • Banker [3] and Dyre [13] malware: fake login webpage.<br>• CEO fraud, the phony accounts to mimic the KPMG lawyer [14] |
| | Undetectability /untraceability of virtual and physical actions | • The banker malware changes basic security configurations [7]<br>• Nigerian scammers opened accounts in India's ICICI bank using fake documents [4].<br>• Android malware found in China automatically deletes messages sent from numbers associated with premium services [12] |

**Table 1: Understanding CCFs' internationalization activities.**

## References


Andreas P. and Price R. 2001. " From war fighting to crime fighting: transforming the American National Security State". International Studies Review 3(3), pp. 31–52.

Dunning, JH. 1993. Multinational Enterprises and the Global Economy. Wokingham: Addison Wesley.

Eisenhardt KM. and Graebner ME. 2007. "Theory building from cases: opportunities and challenges". Academy of Management Journal 50(1), pp. 25-32.

Goodman M. 2011. "What Business can learn from organized crime. Harvard Business Review, 89(11) pp. 27-30

Greene D. and David JL. 1984. "A research design for generalizing from multiple case studies". Evaluation and program planning, 7, pp. 73–85

Guillén MF. and García-Canal E. 2009. "The American Model of the Multinational Firm and the "New" Multinationals from Emerging Economies". Academy of Management Perspectives 23(2), pp. 23-35

Guthrie, D., 1999. Dragon in a Three-piece Suit: The Emergence of Capitalism in China. Princeton University Press, Princeton, NJ and Oxford.

Hagan, J . and Parker, P. (1985). "White-collar crime and punishment: class structure and legal sanctioning of securities violations". American Sociological Review, 50, pp. 302–316.

Hathaway, O.A., Crootof, R., Perdue, W and Levitz, P. 2012. "The Law of Cyber-attack", *California Law Review* 100:817–885.

Hattari R. and Rajan RS. 2010. "India as a Source of Outward Foreign Direct Investment". Oxford Development Studies 38 (4), pp. 497-518

Kumar V, Stam A. and Erich AJ. 1994. "An Interactive Multicriteria Approach to Identifying Potential Foreign Markets". Journal of International Marketing 2 (1), pp. 29–52.

Mullins, R. 2010. " The biggest cloud on the planet is owned by … the crooks: Security expert says the biggest cloud providers are botnets". http://www.networkworld.com/community/node/58829?t51hb (Accessed July 24, 2010).

North, D.C. "Dealing with a Nonergodic World: Institutional Economics, Property Rights, and the Global Environment". Duke Environment, Law, and Policy Forum, 1999: 10(1), pp. 1–12.

Onyshkiv, Y. and Bondarev, A. (2012). "Ukraine thrives as cybercrime haven", March 8, http://www.kyivpost.com/news/nation/detail/123965/.

Oviatt B. and McDougall P. 1994. "Toward a theory of international new ventures". Journal of International Business Studies 25(1), pp. 45-64.

Papadopoulos N. and Jean-Emile D. 1988. "Inventory, Taxonomy and Assessment of Methods for International Market Selection". International Marketing Review, 5 (3), pp. 38–51.

Pigato M. 2000. Information and Communication Technology, Poverty and Development in sub-Saharan Africa and South Asia, World Bank, Washington, DC.

Pontell H, Calavita K. and Tillman R. 1994. "Corporate crime and criminal justice system capacity: government response to financial institution fraud". Justice Quarterly 11: 385–410.

Rui H. and Yip GS. 2008. "Foreign acquisitions by Chinese firms: A strategic intent perspective". Journal of World Business, 43, pp. 213–226

Shapiro, S. (1990). "Collaring the crime, not the criminal: reconsidering the concept of white-collar crime. American Sociological Review", 55, pp. 346–365.

Sinuraja T. 1995. "Internationalization of organized economic crime, The Russian Federation case". European Journal on Criminal Policy and Research 3(4), pp. 34-53

Tillman, R., Calavita, K. and Pontell, H. 1996. "Criminalizing white-collar misconduct: determinantsof prosecution in savings and loan fraud cases". Crime Law and Social Change, 26(1), pp. 53–76.

Vaaler P. 2011. "Immigrant remittances and the venture investment environment of developing countries". Journal of International Business Studies 42 (9), pp. 1121–1149.

Webb, J.W., Tihanyi, L., Ireland, R.D. and Sirmon, D.G. 2009. "You say illegal, I say legitimate: entrepreneurship in the informal economy", *Academy* of *Management Review*, 34(3), pp. 492–510.

Wijnberg, N. M. 1995. "Selection processes and appropriability in art, science and technology Journal of Cultural Economics", 19 (3), pp. 221-235

Williams P. 1995. "Transnational criminal organizations: strategic alliances. The Washington Quarterly, pp. 59-67

Williamson NC, Kshetri N, Heijwegen T. and Schiopu A. 2006. "An Exploratory Study of the Functional Forms of Export Market Identification Variables". Journal of International Marketing 14(1), pp. 71-97.

Woodruff, C. and Zenteno, R. 2007. "Migration networks and microenterprises in Mexico". Journal of Development Economics, 82, pp. 509–28.
Yao, D.A. 1988. "Beyond the reach of the invisible hand: Impediments to economic activity, market failures, and profitability". Strategic Management Journal, 9(S1), pp. 59–70.
Yin R. 1994. Case Study Research: Design And Methods (2nd ed.). Newbury Park, CA: Sage.