Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future

By: Nir Kshetri

Kshetri, Nir (2016). “Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future” *Crime, Law and Social Change*, 66 (3), 313–338.

The final publication is available at Springer via https://doi.org/10.1007/s10611-016-9629-3

*****Note: References indicated with brackets. Footnotes can be found at the end of the article.**

Abstract:

Cybercrime is rising rapidly in India. Developing economies such as India face unique cybercrime risks. This paper examines cybercrime and cybersecurity in India. The literature on which this paper draws is diverse, encompassing the work of economists, criminologists, institutionalists and international relations theorists. We develop a framework that delineates the relationships of formal and informal institutions, various causes of prosperity and poverty and international relations related aspects with cybercrime and cybersecurity and apply it to analyze the cybercrime and cybersecurity situations in India. The findings suggest that developmental, institutional and international relations issues are significant to cybercrime and cybersecurity in developing countries.

Keywords: cybercrime | cybersecurity | India | white-collar crime

Article:

Introduction

Cybercrimes originating from and affecting India are escalating rapidly. Among the Indian organizations, which responded to KPMG’s [1] Cybercrime survey report 2014, 89 % considered cybercrime as a “major threat” (p, 3). According to the Norton Cybercrime Report 2011, 30 million Indians had become cybercrime victims, which cost the Indian economy $7.6 billion a year. Another estimate suggested that 42 million Indians were victimized online in 2011 [2]. India has also been a target of high profile international cyberattacks. For instance, while the Stuxnet virus was programmed to damage Iran’s centrifuges at Natanz nuclear site, it also infected computers in India [3].

India also generates significant amount of cybercrimes that affect Internet users worldwide. For instance, India was the top origin country for spam in 2011 and 2012 [4, 5]. Likewise, a phishing survey released by the Anti-Phishing Working Group (APWG) in April 2012 found that India had the highest phishing TLDs by domain score (calculated as phish per 10,000 domains) in the second half (H2) of 2011 [6]. India is also among the top click fraud originating countries outside North America [7]. Finally, according to the U.S.-based Internet Crime Control Centre, India ranked fifth in the number of complaints received by the agency [8].

Since the degree of digitization of economic activities is tightly linked to the probability of experiencing cyberattacks [9], India's massive digitization efforts deserve mention. Among the most ambitious is the Unique Identification Authority of India (UIDAI) project. The new government of India (GoI) led by the Bharatiya Janata Party (BJP) has indicated that it would provide a strong support for the UIDAI project, which would require residents to have biometric IDs in order to collect government benefits. The project has set a target of 1 billion enrolments by 2015 [10]. The biometric ID assigns a person a 12-digit number, which is called the Aadhaar number. It requires the collection of 10 fingerprints, iris scans and other information such as the name, date of birth and address and will be hosted in the eGovernance cloud platform.

As a consequence of the above mentioned observations, there is an increasing cybersecurity concern among organizations, individuals and government agencies. Due to the country's lack of indigenous technology and patents related to cybersecurity, the GoI has announced that it would provide financial incentives to Indian firms to acquire foreign firms with high-end cybersecurity technology [11]. The Ministry of External Affairs would explore possible targets worldwide through Indian embassies and missions. The fact that Indian government agencies have been under cyber-attacks, suspected from foreign governments, has provided a major motivation for such an approach. An Indian company which owns the technology gained through the acquisitions is required to give the government agencies an access to the IPR.

A number of issues motivate this paper. First, criminologists have emphasized the need to understand the causes and motivations of frauds against consumers against the backdrop of rapid growth in such frauds and other types of crimes transcending international boundaries [12, 13, 14, 15]. Prior researchers have also suggested that an understanding of the structure of opportunity associated with white-collar crimes would help take countermeasures to prevent such crimes [16]. This argument is equally valid for cybercrimes.

Second, it is estimated that only about 10 % of cybercrimes are reported,[1] in India; and of those reported about 2 % are actually registered. The conviction rate was estimated at as low as 2 % [19]. As of August 2009, only four people in the country were convicted for cybercrimes [20]. Until 2010, there was not a single cybercrime related conviction in Bengaluru, the biggest offshoring hub. The total number of convicted cases by 2010 was estimated at less than 10 [21]. Past studies have suggested three explanations that may account for the low rates of prosecutions and convictions and differential treatment of white-collar offenders: organizational advantage argument, alternative sanctions argument and system capacity argument [22, 23, 24, 25]. This article attempts to examine these explanations and associated mechanisms in more detail in the context of cybercrime by drawing upon institutional theory and international relations (IR)/international political economy (IPE) perspectives.

Third, previous research has indicated that cybercrime and cybersecurity in developing economies have unique structural characteristics [26, 27]. Yet the literature does not discuss how key economic and social characteristics of developing countries such as low levels of human development and education and weak democratic institutions [28] are connected to cybercrime and cybersecurity. A related point is that while the roles of dual economy have been examined in the context of the growth of the informal sector [29], it is not clear how dualism would affect the key ingredients of cybercrimes.

Fourth, prior research has provided some evidence regarding the roles of public-private partnership (PPP) in fighting cybercrime and enhancing national cybersecurity (e.g., [26, 30]). In a study of the PPP in the fight against terrorism, Bures [31], however, reported that private businesses' roles were not appreciated and many private sector representatives considered the public-private partnerships more like" public-private dictatorships". More conclusive evidence is clearly needed to assess the contexts, mechanisms and processes associated with the effectiveness of public-private partnership.

Finally, policy makers need to re-examine various local and international tools and procedures to combat crimes with cross-border dimension. In this regard, while some attention has been paid to corruption and economic crime [32], relatively little systematic attention has been paid to international cybercrimes.

In an attempt to fill the above research gaps, the article draws together a wide variety of research from a number of fields such as criminology, international political economy (IPE), international relations (IR), institutional theory and developmental economics to examine cybercrime and cybersecurity in India. We first discuss relevant theories and concepts in order to develop a framework to cybercrime and cybersecurity in developing economies. Next, we apply the framework in the contexts of cybercrime and cybersecurity in India. Then, we provide discussion and implications of our study. The final section provides concluding comments.

Relevant theories and concepts

Institutional and economic factors

In order to provide insights into the low rates of prosecution and conviction for cyber-offenders in India, it is necessary to look at formal and informal institutions. Past researchers have recognized that economic activities and actors are embedded in formal and informal institutions [33, 34]. A related point is that the nature of activities of cybercriminals fits squarely with what Baumol [35] calls destructive entrepreneurship. Baumol hypothesized that the distribution of productive, unproductive, and destructive entrepreneurs is a function of the payoffs offered to these activities by the society's rules of the game. These rules are referred as institutions [36].

Economic and social characteristics of a developing economy

Some of the key economic and social characteristics of a developing country include a dual economy, low levels of income and education, which lead to low levels of human development;

high unemployment rates, high degrees of income inequality, and weak democratic institutions [28, 37]. We would argue that these characteristics are tightly connected to cybercrime and cybersecurity.

For instance, low levels of income and education lead to relative laggardness in developing world-based businesses' and consumers' adoption of new technologies. Many Internet users in the developing world are inexperienced and not technically savvy as a high proportion of them got their computers and connected to the Internet not long ago. A majority of them also lack English language skills. This later point is crucial due to the fact that most of the information, instructions, and other contents for security products are available in English language only. Many Internet users in economies in the developing world are unable to use IT security products developed in English language [26, 27].

In its basic form, a dual economy is characterized as one that has a relatively developed urban industrialized sector and a rural sector [37]. The dual nature of the economy also means that in addition to variation between sectors of the economy, developing economies are characterized by an uneven development within a given sector [38]. Cybercrimes targeting developing economies tend to be concentrated in well-developed industry sectors such as businesses in the online gaming industry in China, banking and financial sectors in Brazil and the offshoring sector in India [26, 27].

Causes of prosperity and poverty

Based on a review of the literature, Acemoglu [39] and Acemoglu et al. [40] have identified fundamental and proximate causes of prosperity and poverty. These are presented in Table 1 and the last column shows how some of them are linked to cybercrime and cybersecurity in India.

Table 1
Causes of prosperity and poverty and their relations to cybersecurity orientation

	Explanation	**Relevance to cybersecurity in developing economies**	**Example from India**
Fundamental causes of prosperity and poverty			
Political and economic institutions	• Institutions such as corruption, lack of accountability and weak law enforcement create bottlenecks for development [41] • National governments poorly equipped to deal with crimes.	• Many governments lack technological sophistication and are poorly equipped to fight the non-state criminal actors.	• Congestion in law enforcement systems: severe lack of law enforcement manpower reported in Delhi, Mumbai and other cities. • Lack of criminal database

Culture or informal institutions	• Sets of beliefs generated by some cultures may have anti-developmental consequences [42].	• Cybercrime are associated with a lower degree of stigmatization than in industrialized countries	• Lack of guilt, remorse and an ethical sense among cybercriminals • Call center employees consider it “undignified” to undergo security checks • password sharing is common: cases of crimes associated with such practice
Proximate causes of prosperity and poverty			
Human capital	• Most developing economies fail to invest enough in education and skills.	• Lack of cybersecurity related manpower • Lack of cybersecurity orientation of Internet users	• Significantly less number of cyber specialists than the demand • Sense of over-reliance on basic security solution such as antivirus
Technology	• Developing economies tend to have low investment in R & D and low rate of adoption of technology • They also have a tendency to use low-cost technologies	• Low rate of adoption of cybersecurity-related technology • Underdeveloped cybersecurity industry • Low-cost technologies are more prone to cyber-threats	• Lack of indigenous technology and patents related to cybersecurity • A higher proportion of computers using crime prone technologies such as IE6 • Researchers in R&D per million people lower than in other BRIC economies

Institutions, culture and geography are arguably fundamental causes of prosperity [39, 40]. Economically successful societies are characterized by good economic and political institutions [43]. Likewise, culture is related to different sets of beliefs regarding how people behave, which has strong implications for development [42]. Institutional theorists consider culture as an informal institution [36]. Since geography has a limited role in cybersecurity, we focus on the roles of formal and informal institutions.

First, we illustrate a direct connection between institutions and cybercrime/cybersecurity. As to many developing economies’ capability to build cybersecurity-related institutions, while the states “hold some trump cards” “at the most basic level”, for instance, with their power to define the activities that are illicit ([44], p. 409), many governments lack technological sophistication and are poorly equipped to fight the non-state criminal actors. Regarding the informal institutions, while most traditional illicit activities are viewed as deviant and carry a social stigma [44], this is not necessarily the case for cybercrime-related activities. For instance, many criminal hackers based in the developing world see their cybercrime activities victimizing developed world-based consumers and businesses as morally acceptable [45].

Among the proximate causes are physical capital differences, technology differences, human capital differences and functioning of markets [39]. In this paper, we focus on technology differences and human capital differences.

Institutional bottlenecks in developing economies

Building on the work of Roland [46], de Laiglesia [41] classifies institutions according to the rate of change: "Slow-moving" institutions include legal infrastructure, culture and social norms, while laws, rules and regulations, contract enforcement, political process and governance are examples of "fast moving" institutions. Some elements of fast-moving institutions such as corruption, lack of accountability and weak law enforcement may create bottlenecks for development.

The impacts of slow-moving and fast moving institutions on cybersecurity can be better explained with the concept of institutional bottlenecks. In a framework proposed by de Laiglesia [41] for an analysis of institutional bottlenecks in developing economies, technology-related issues and factors are present at three levels: technological progress and dissemination (institutional outcomes), technology opportunity set (interaction and decision area), technology use, adoption and development (intermediate outcomes) ([41], p. 14). In this section, we analyze these elements from the perspective of cybersecurity.

One way to understand the low level of technological progress is the lack of absorptive capacity, which means that many developing economies lack capabilities to assimilate technologies and associated organizational practices [47, 48]. This is mainly due to their institutional and social arrangements [49]. In expanding their attack sources such as botnets, hackers tend to focus on economies with less developed IT infrastructures [50]. In this regard, as to the technological progress and dissemination, most developing countries are characterized by poor performance in cybersecurity infrastructures. They often lack domestic anti-virus companies. Businesses and consumers in some developing countries also prefer to buy domestically manufactured software.

Developing economies also tend to use low cost and insecure technologies. While some argue that networks in developing have built-in security mechanisms as they have "wired security into their IT network infrastructure" compared to the Western approach of "bolting it on afterward to legacy systems" ([51], para. 11), contrary observations have been reported.

Some developing country-based manufacturers also reportedly use cybercrime-prone products in order to reduce the cost of PCs and other devices. The documents of a cyber-fraud lawsuit filed by Microsoft against a Chinese-owned domain provide a glimpse into this phenomenon. Microsoft's digital crimes unit investigating counterfeit software and malware in China had bought 20 new computers from Chinese retailers. The unit found counterfeit versions of Windows installed on all the machines and malware pre-installed on four of them [52]. It was reported that when a brand new and direct from the factory condition laptops bought in Shenzhen was booted up for the first time, the Nitol virus was hidden in the laptop's hard drive. The virus started searching for another computer on the Internet. The laptop was made by a Guangzhou, China-based computer manufacturer, Hedy [52].

Differential treatment to white-collar offenders

Based upon the related literature of white-collar offenders [22, 23, 24, 25], three explanations can be offered regarding the differential treatment of cyber-offenders. According to an organizational advantage argument, offenders that are in "organizationally shielded" positions receive more lenient treatment. Hagan and Parker's [22] analysis of securities fraud in Canada indicated that employers were less likely to be prosecuted under criminal statutes than were offenders in lower-class positions. The authors concluded that organizational structure of corporations embedded class advantage in such a way that employers were often shielded from prosecution.

According to an alternative sanctions argument, civil sanctions may replace criminal sanctions in the response to white-collar crimes. Shapiro's [24] study of violators of securities law in the U.S. indicated a higher tendency to prosecute lower-status offenders than higher-status ones. Her analysis, however, indicated that the variation in prosecutions and sanctions across different levels of status was due to the availability of alternative sanctions in cases involving higher-status offenders and was not because of a class bias.

Finally the system capacity argument maintains that the legal response to suspected crime is a function of organizational resources and caseload pressures [23]. Resource limitations are of particular concern for white-collar crimes due to their complexity, which require substantial amounts of investigative and prosecutorial efforts [25].

It is recognized, however, that the three explanations above provide complementary rather than mutually exclusive interpretation regarding the differential treatment of white-collar offenders. For instance, prior research indicates that the limited capacity of criminal justice agencies due to the complexity and hidden nature of white-collar crime and the system overload caused by such crimes reduces state capacity to respond to such crimes [53]. Likewise, due to the difficulty involved in obtaining direct evidence against high level criminals that are "organizationally shielded", system capacity limitations may lead to prosecution of lower-level employees, for whom it is easier to locate the evidence ([25], p. 53).

International relations (IR)/International political economy (IPE) perspectives

In light of the cross-border nature of most serious cybercrime activities, In order to provide further insights into cybercrime and cybersecurity in India, it is also important to understand the importance of cyber-security issue from the IR/IPE perspective. A large body of literature indicates that 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 [54, 55, 56]. Cyber-threat is increasingly recognized as a legitimate security issue because cyber-attacks present threats to national security for the simple fact that most of the critical infrastructures are connected to the Internet [57, 58]. This issue is also tightly linked to economic security of countries.

The state's regulatory/participatory roles and public-private partnership

An analysis of the regulatory and participatory roles of the state would provide a helpful perspective in identifying the potential roles of the public and the private sector in strengthening data privacy and security protections (Table 2). By regulatory state, we mean a set of factors that influence the enforcement of contracts, sound political institutions and the rule of law, corruption of public officials, bureaucratic quality, a strong and effective court system and citizens' willingness to accept the established institutions [60, 61]. There are a number of barriers and challenges in India to perform the functions of the regulatory state. The states have faced budget problems and have failed to comply with federal directives to hire more judges and upgrade legal infrastructures and court facilities [62].

Table 2

	Direct effects	**Effects associated with indirect causal chains and externality**
Maintaining established orders	• Enforcing industry codes related to cybersecurity • The requirement of external audit of cybersecurity practices	• Providing law enforcement agencies with cybersecurity-related expertise
Facilitating institutional changes	• Developing new industry codes and norms related to cybersecurity to account for shifts in technology, market and other external factors.	• Mimetic effects associated with high performing members • Help develop national cybersecurity regulative framework

Adapted from Kshetri & Dholakia [59]

The participatory state captures the extent to which policies and institutions represent the wishes of the members of society [61]. In such a state, businesses may participate in the national policy making arena through "dialogue, litigation, and mimesis" ([63], p. 502). Prior research indicates that business groups can work closely with state agencies to protect their independence and autonomy [64].

Applying the framework in the Indian context

Political and economic institutions

Various sources of institutional bottlenecks noted above [41, 46] are a major concern in India, and are even greater and more evident in cybercrime and cybersecurity. For one thing, the gap between the law in the book and the law in the action has been substantial. India has clearly experienced rapid growth in cybercrime and congestion in cybercrime related law enforcement systems. For instance, consider India's only Cyber Appellate Tribunal (CAT), which started functioning since 2006 [65]. It was reported in June 2014 that the tribunal had not adjudicated a single case during the previous 3 years due to the non-availability of the chairperson and judicial members [66].

To take another example, in 2004, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division [67]. As of 2011, the Delhi police cybercrime cell had only two inspectors [68]. In 2012, the Delhi High Court criticized the lack of functionality of the

Delhi Police website, which according to the court was “completely useless … obsolete and does not serve any purpose” ([69], p. A1).

The observations in the prior literature regarding the complexities of white-collar crimes, difficulty involved in obtaining direct evidence against criminals involved and the system overload caused by such crimes, leading to a limited capacity of criminal justice agencies and the state to respond to such crimes [25, 53] have special significance to cybercrimes in India. For instance, the Information Technology Act 2000 (Amended in 2008) did not cover issues such as data protection and privacy, which hindered the development of call-center and BPO industries. A survey reported that while most BPOs in Gurgaon had been cybercrime victims, about 70 % of the respondents did not report to the police [70]. Most organizations expressed concerns about competence, professionalism and integrity of the police in handling cybercrimes. About 50 % of the respondents not reporting thought that the cases are not dealt with professionally and 30 % noted that they had no faith in the police [70].

India’s social scientists have speculated and law enforcement officers have admitted that the actual numbers of crimes in the country are significantly greater than what are reported in the official crime statistics by National Crime Records Bureau and other agencies [12]. To put things in context, according to the National Crime Records Bureau (NCRB) (http://ncrb.gov.in/), in 2013, the states of Mizoram, Nagaland and Sikkim did not register any cybercrime related cases. The reason probably could be attributed to the lack of reporting of cybercrimes in these states rather than the non-occurrence of cybercrimes in these states.

One reason behind the low rate of registration of cybercrime cases concerns the barriers, hurdles and hassles that confront the victims. In some cases the police show unwillingness to take the extra works needed for the investigations [21]. There are reports that the police allegedly were unsupportive to victims, who wanted to file a cybercrime case. Cybercrime victims have also complained that the police follow a long and inefficient process to build a case [68].

A related point is that a major factor behind the low conviction rate concerns the technological illiteracy and low level of cybercrime awareness in the law-enforcement community. For instance, it was reported that when a police officer was asked to seize the hacker’s computer in an investigation, he brought the hacker’s monitor. In another case, the police seized the CD-ROM drive from a hacker’s computer instead of the hard disk [20].

In one way, there is the development of a vicious circle: a) law enforcement agencies’ unwillingness to put efforts for investigating cybercrimes and their technological illiteracy indicate that they lack the skills, orientation and capability to address cybercrime related offenses; b) the survey conducted among Gurgaon-based BPOs indicates that there are low cybercrime reporting rates because of the victims’ lack of confidence in law enforcement agencies: and c) cybercriminals may become more confident, resourceful and powerful because their offenses are not reported.

A final point that must be considered concerns the international political economy of immigration. Whereas immigration policies in most industrialized economies provide a legal tool to restrict entry and settlement, such policies are weak in India, which partly explains the

Nigerian cyber-fraudsters' presence in India. For a Nigerian cybercriminal, for instance, fewer efforts are required in establishing a predatory group in India compared to that more advanced economies such the U.S.

Over the past few years, the popular press in India has routinely published story about Nigerian cybercriminals' engagement in cybercrimes, principally based on social engineering techniques. Indians are reported to be victims of various versions of "Nigerian 419" frauds, which account for a significant proportion of cyber-frauds in the country. Below we discuss some representative examples among the numerous ones reported in the media. In 2012, Indian Police arrested six Nigerians for allegedly defrauding hundreds of Indians. They seized 14 laptops, seven memory sticks, 23 mobile phones, fake documents and cash [4]. A Defense Research & Development Organization (DRDO) scientist reportedly paid Rs. 5.5 million (about US$110,000) to a Nigerian scammer [71]. In another case, in 2009, two Nigerians were arrested in Kolkata, who duped a housewife paying Rs. 122,000 (US$2,400) for a lottery scam [72]. The police suspected that they were members of a cybercrime ring, ran a fake lottery scam and made more than Rs. 10 million (US$200,000) in 3 months before their arrests.

It is important to understand the modus operandi used by the Nigerian cybercrime rings. A Nigerian national involved in fake job racket, which allegedly victimized at least 40 people, had recruited several women in his gang as money mules. Note that money mules in cybercrimes are often duped and recruited on-line to transfer stolen money illegally. The mules falsely think that they are employed in a legitimate business. The victims were asked to deposit Rs. 6,000–60,000 (US$ 110–1,100) as travel and related expenses for interviews. The women's bank accounts were used to receive the crime proceeds and their ATM cards were used to withdraw cash. The victims were promised that the money would be refunded after the interview [73]. In light of prior findings, which indicate a high degree of vulnerability of Indian women in the cyberspace [74], this is yet another mode of victimization of women.

Recent regulatory developments

In an attempt to address some of the above issues, India is seeking to improve cybersecurity performance through regulatory developments and institutional reforms. As a response to domestic and international pressures to enhance cybersecurity measures, in July 2013, the GoI released National Cyber Security Policy (NCSP) 2013, which set forth 14 objectives that included enhancing the protection of critical infrastructure, and developing 500,000 skilled cybersecurity professionals by 2018 [75]. The development of PPP efforts towards enhancing the cybersecurity landscape is a also key component of the NCSP. The GoI has made efforts to create a favorable climate for a higher participatory involvement in cybersecurity. For instance, a Joint Working Group (JWG) on cybersecurity was established with representatives from government agencies and the private sector, which was mandated to come up with recommendations for consideration by the GoI on PPP in capacity building and policy making. The JWG released its report "Engagement with Private Sector on Cyber Security" in October 2012. As a further sign for an improving climate for participatory involvement of the private sector, in October 2012, India's National Security Advisor announced a plan to establish a permanent working group on cybersecurity with representatives from the government and the private sector. The working group would implement the country's cyber-defense framework. The

NSA advisor noted that this would mark the first time that the GoI allowed the participation of the private sector in national security matters [30].

Among other positive changes in the Indian cybersecurity landscape, in July 2014, the IT minister informed the lower house, Lok Sabha that all central and state/Union Territory government agencies had been asked to conduct security auditing of their IT infrastructures, websites and applications. State governments were also asked to build adequate technical capacity including infrastructure, cyber police stations and sufficient manpower [76]. Likewise, in 2011, the central bank, Reserve Bank of India (RBI) introduced a set of recommendations, which include the formation of separate information security groups within banks and maintenance of adequate cybersecurity resources based on their size and scope of operation.

Culture or informal institutions

The Asians often emphasize on social harmony and human relationships whereas the Westerners' place relatively higher emphasis on efficiency and control of time [77]. This aspect of the Asian culture has a clear cybersecurity implication. For instance, call center employees in India consider it "undignified" to undergo security checks [78]. A related point is that due to the social circumstances, password sharing is more common in India than in the West. There have been reported cases of crimes associated with this practice. In 2010, an employee of the Indian IT company, Wipro used his colleague's password to steal about US$4 million from the company's bank account [79].

The lack of previously developed mechanisms and established codes, policies, and procedures and non-existence of identifiable victims in many cases [80] are likely to lead to much less in cybercrimes guilt compared to conventional crimes. These conditions are more likely to be prevalent in the developing world, where cybercrimes is more likely to be justifiable. An official of India's Cyber Crime Investigation Cell (CCIC) noted that many young people in the country have committed cybercrimes for fun "without actually realising the gravity of their actions" ([81], para 11).

A related point is that in many cases, people engaged in cyber-offenses are not aware of the potential damage that their activities can cause to others. For instance, studies found that click fraud is pervasive in India but most people involved in such frauds click on ads just to make money and may not know that some businesses are victimized by their activities.

Human capital and technology

Studies and reports issued over the past few years have pointed out that a severe shortage of qualified cybersecurity professionals currently exists in India. One estimate suggested that India needs 250,000 cyber specialists to deal with cybercrime [82]. According to the market research firm, International Data Corporation (IDC), only 22,000 security professionals were available in India in 2012 whereas the country needed 188,000 [83].

There is also a severe lack of cybersecurity orientation among consumers, businesses and policy makers. According to a Norton survey, 60 % of Indian Internet users believed that a basic security solution such as antivirus would be sufficient for cybersecurity [84]. Cybersecurity orientation has also been low among high-level politicians. In 2012, three Indian lawmakers resigned after they were filmed allegedly watching pornography on a cell-phone during debate at a state assembly in Bangalore [85].

According to the World Bank, India had 100 researchers in R&D per million people in 2000 (the numbers for other BRIC economies were: Brazil: 424, China: 548 and Russia: 3,451) [86]. Looking at more recent data, according to a report presented by the then Science and Technology Minister Kapil Sibal to the Rajya Sabha, the upper House of the Indian Parliament, India had 156 researchers in R&D per million people in 2008. As a point of comparison, according to the World Bank, the corresponding numbers for other so called BRIC economies for 2008 were: Brazil: 696, China: 1,199 and Russia: 3,152. Sibal suggested that universities in India were characterized by inferior R&D quality and capabilities [87]. A related point is that much of the R&D in India is geared toward smaller projects that complement other innovation centers in Silicon Valley and elsewhere [88].

India’s status as a low human development country also means that most cybercrimes associated with the Indian offshoring industry are related to inside abuse rather than high-tech crimes requiring super-hacker skills. Here, for illustration, we offer some representative examples. In 2005, workers at Pune, India, subsidiary of Mphasis, a provider of outsourcing services, transferred about US$500,000 from four Citibank customers’ accounts to their personal accounts. This was among the first major BPO scams in India [89]. In another case, the British Tabloid, Sun, reported that an employee of the Gurgaon-based BPO firm Infinity E-Search sold confidential information of 1,000 bank accounts for US$5.50 each to its reporter working as an undercover [58]. In still another case, in 2006, two employees of Mumbai-based BPO, Intelenet Global allegedly manipulated credit records of 400 U.S. customers [89]. In a more recent case reported in March 2012, two ‘consultants’, who claimed to be workers in Indian offshoring firms met undercover reporters of The Sunday Times. They came with a laptop full of data and bragged that they had 45 different sets of personal information on about 500,000 U.K. consumers. The information included credit card holders’ names, addresses, phone numbers, start and expiry dates and security verification codes. Data for sale also included information about mortgages, loans, insurance, phone contracts and Television subscriptions [90]. In another interesting example, the U.S. Federal Trade Commission (FTC) sued the California-based American Credit Crunchers in 2012, According to the FTC, a company based in India associated with American Credit Crunchers made threatening calls to U.S. consumers with histories of applying for payday loans, which are short term, high interest loans that are typically applied online. Agents in India with massive amount of personal data allegedly called potential victims and threatened the victims if they did not pay the fictitious loans of up to US$2,000. U.S. consumers had lost over US$ 5 million to the scam by 2012, which had been in operation since 2010 [89].

India’s low R&D profile has an important implication for cybersecurity. Due to poor R&D and innovation performance, some liken economic activities in the Indian IT and offshoring industry to a “hollow ring”. An Economist article notes: “India makes drugs, but copies almost all of the compounds; it writes software, but rarely owns the result. … [it has] flourished, but mostly on the back of other countries’ technology” ([91], para 1). Regarding the location of R&D activities in Russia, Moscow-based Kaspersky Lab's CEO and Chairman Eugene Kaspersky noted: "[Engineers in] China or India …are good if you just want something programmed, but if it's about research, then it has to be Russia" [92].

Notably absent from India are complex and sophisticated malware and spyware. Note that the creation of sophisticated malware is a R&D intensive task. One explanation of the lack of sophisticated malware originated from India could be the country's low R&D profile. To further understand the absence of major malware originated from India, it is also worth noting that unlike some developing countries, India lacks major anti-virus companies. For instance, in 2010, Moscow-based Kaspersky Lab was the world's fourth biggest IT security company. Some other former second world economies also have top IT security companies such as Czech Republic's AVG Technologies, Romania's BitDefender, and Slovak Republic's ESET [93]. Likewise, the Belarusian firm VirusBlokAda was the first company to identify the Stuxnet code in June 2010 [94]. This issue is important as malware firms and anti-virus companies tap into the same skill base.

India's cyber-victimization can also be partly attributed to the country's crime-prone technologies. According to Microsoft's IE6Countdown website, as of January 2012, 6th version of IE6 accounted for 6 % of browsers in India [95].

The dual economy's implications

As to the dual economy's implications, India's well-developed legitimate IT industry is associated with a low cybercrime rates, especially involving sophisticated and complex malware. Nandkumar Saravade, ex-director of cybersecurity for the National Association of Software and Services Companies (NASSCOM) noted: ".. .. any person in India with marketable computer skills has a few job offers in hand" ([96], para 9).

The duality of the Indian economy also means that there is a high degree of intersectoral differences in cybercrime target attractiveness. More specifically, as indicated by some of the most high-profile and widely publicized cybercrimes, the Indian offshoring industry has become a lucrative target for data thieves. Data frauds have been reported in call centers in major cities such as Pune, Hyderabad, Bangalore, and Gurgaon. A survey indicated that most BPOs in Gurgaon had been cybercrime victims [70]. In first- and second-tier cities, data brokers reportedly obtain data from offshoring companies' employees and sell to cybercriminals [20].

A further implication of the duality is that some illegal and extra-legal global enterprises have opened call centers in India. In the early 2008, a criminal group involved in botnet attacks set up offices in India to process applications that cannot be completed automatically [97]. Information technology (IT) workers in India offered help to facilitate signing up of free e-mail accounts. Likewise, the Ukrainian scareware producer, Innovative Marketing Ukraine had established call centers in India [98].

These realities of the cyberspace have put tremendous pressures on Indian companies in the offshoring sector to strengthen cybersecurity. In an attempt to address their clients' cybersecurity-related fear, Indian outsourcing firms have taken strict measures. They have established biometric authentication controls for workers and banned cell phones, pens, paper, and Internet access [99]. Computer terminals lack hard drives, e-mail, CD-ROM drives, or other ways to store, copy, or forward data [100]. Indian outsourcing firms also extensively monitor and analyze employee logs [99].

The roles of industry bodies and trade associations

An extensive literature is devoted to explore firms' participation in cooperative ventures and alliances such as trade associations [101]. Some researchers argue that network-based organizations such as trade and professional associations represent an alternative to the coercive state [102, 103]. Note that one of the roles of trade and professional associations is to monitor their members' compliance with normative and coercive expectations [104]. In this way, they can play an important role in defining key issues within an industry or a business sector and facilitating the diffusion of the concepts and practices associated with those issues [105].

When the state's regulatory roles are weak, trade associations and industry bodies may fill the regulatory vacuum. Previous research has suggested that interfirm linkages such as trade associations in emerging economies can play an important role in establishing moral legitimacy of the industry in Western economies [106]. To put things in context, developed world-based offshoring clients may rely more on trade associations such as the NASSCOM than on the weak, ineffective state.

Trade associations such as the NASSCOM influence industry behaviors in a number of ways. First, these associations' norms and codes can influence firms to behave in a certain way by penalizing noncompliance with various mechanisms [36]. Second, prior research indicates that such associations can work closely with state agencies to protect their self-regulating independence and autonomy [64]. Just as important is the fact that in some situations, the state finds it beneficial to collaborate with them to rationalize an arena of activity [107]. Professional and trade associations thus play an important role in strengthening the regulative institutions by providing the state with their expertise in developing new regulatory framework and strengthening the enforcement mechanisms [59].

Influencing and monitoring industry behaviors

In light of the state's inability to enforce regulations due to various bottlenecks [41, 46], the NASSCOM monitors member companies to ensure they adhere to the standards. For instance, the NASSCOM requires its members self-police and provide additional layers of security. Non-compliant companies would lose memberships [108]. The Data Security Council of India (DSCI) is a self-regulatory member organization set up by the NASSCOM to create trustworthiness of Indian companies as global outsourcing service providers. Companies that fail to secure can be fined up to US$1 million [19].

Trade associations such as the NASSCOM influence industry behaviors directly as well as through indirect causal chains (Table 2). Indirect effects related to externalities also arise via mimetic isomorphism, which entails mimicking behaviors of other actors that are perceived to be exemplar and have a higher degree of effectiveness [109, 110]. Most obviously exemplar firms serve as models for smaller firms to imitate. In such a case, knowledge flow takes place by externalities [111, 112, 113]. It is important to emphasize that while mimetic isomorphism may take place in the absence of an association, the association is likely to accelerate the process by stimulating interaction among member companies.

A trade association's enforcement strategy becomes efficient and powerful if a large number of firms in the industry join the association [102]. NASSCOM members and professionals have supported the DSCI enthusiastically. As of August 2014, the DSCI had about 700 organizations as Corporate Members, and more than 1350 security and privacy professionals and practitioners as its Chapter Members [30].

The NASSCOM's measures have paid off brilliantly. Commenting on data security measures in the Indian offshoring sector, a report of the UK's Banking Code Standards Board (BCSB) noted: "Customer data is subject to the same level of security as in the UK. High risk and more complex processes are subject to higher levels of scrutiny than similar activities onshore" ([114], para. 12). Citing the findings of the BCSB and Forrester Research, the NASSCOM's then president, Karnik, asserted that security standards in Indian call centers were among the best in the world and there were more security breaches in the U.K. and the U.S. in 2005 than in India (AFX [115]).

Contribution to the formulation of cybersecurity-related legislation and policy framework

The NASSCOM partnered with the Ministry of Information Technology to draft data protection and data privacy laws to respond to privacy concerns of offshore clients [116]. A main goal was to bring Indian data protection laws to the same level as the European and the U.S. standards. In 2011, the DSCI announced a plan to set up a cloud security advisory group that would develop a policy framework. The group would also advise the GoI on security and privacy issues in a cloud environment [117].

Many of the NASSCOM's responses are the results of a hollow state and the thin institutions that hamper legislative and law enforcement efforts. For instance, India lacks standard identifiers like the U.S. Social security number making it difficult to check potential employees' backgrounds. It was reported that a thorough background check cost up to $1,000 per employee to [118]. In response to the lack of such databases, in 2005, NASSCOM announced a plan to launch a pilot employee-screening program called "Fortress India", which would allow employers to screen out potential workers who have criminal records. Subsequently it was developed into the National Skill Registry (NSR), which allows employers to perform background checks on existing or prospective employees. It is a voluntary registry for call center employees (Table 2).

Facilitating the enforcement of legislation

Various ongoing efforts and activities initiated by the NASSCOM and the DSCI in facilitating the enforcement of cybersecurity regulations in the country deserve mention. They prepared a detailed project report to set up cybercrime police stations and Cyber Labs across the country. NASSCOM helped police departments of Mumbai and Thane in establishing cybercrime units and in training officers [119]. In 2005, NASSCOM announced a training initiative for Pune's cybercrime unit [120]. A cybercrime unit established in Bangalore in 2007 has resources to train more than 1,000 police officers and other law-enforcement personnel annually [121]. As of April 2014, there were eight Cyber Labs in various Indian cities, which provided training to over 28,000 police officers [122].

The NASSCOM and the DSCI also meet with bar councils in different cities to educate legal communities. In addition, NASSCOM offered to work with authorities in the U.K. and India to investigate cases involving identity theft [123]. This issue is especially important because identity theft-related crimes are rapidly growing worldwide [124].

The West's response to India's weak cybersecurity performance

The observations regarding the decreasing salience and level of nontraditional security issues and the evolution of cyber-threat as a more legitimate security issue [54, 55, 56, 57, 58] are consistent with the emergence of IR issues involving India. India's weak cybersecurity infrastructures and capabilities have been a matter of concern to Western countries. India undoubtedly occupies an important geopolitical position, which has made it an attractive target for high profile politically motivated cyberattacks. At the same time, such a position would qualify for a strategic partnership with major global players. Cybersecurity experts, for instance, have preached that in order to win the competition with China, the U.S. government needs to work with like-minded countries such as India to define international norms about cyberspace [125]. There have already been some progresses on this front. In July 2011, the U.S. and India signed a Memorandum of Understanding (MOU) to promote cybersecurity related cooperation and exchange information [126]. In April 2012, bilateral talks were held between India and the U.S. While the talks also included a number of other issues, the main emphasis was on India's cybersecurity capacity. As India has emerged as a major offshoring destination for back offices as well as other high value business functions, cybersecurity orientation of Indian businesses has been an issue of pressing concern to U.S. businesses. The U.S. officials involved in the talks were especially interested in India's capability to detect and investigate cybercrime. India has also signed MoU on cyber security cooperation with Japan and South Korea [127].

Discussion and implications

The escalation of cybercrime activities originated in and affecting India can be attributed to formal and informal institutions that are conducive to such activities as well as poor cybersecurity orientation of consumers, businesses and government agencies. India's approach to cybersecurity and capabilities are economic developmental as well as international relations issues facing the country.

As to the escalation of cybercrime activities originated in India, cybercriminals consider Indian computers as low hanging fruit due to weak cybersecurity. The weak cybersecurity condition can be attributed to the low level of human development [28, 37], unaffordability of and inability to use IT security products [26, 27], resource limitations to respond to cybercrimes due to their complexity [25] and resulting institutional bottlenecks noted above [41, 46]. Indian computer networks have provided the means to commit cybercrime acts for foreign criminals. A case in point is the European hacker nicknamed Poxxie, who broke into the computer network of a U.S.

company in 2011 and sold the credit card information to underworld buyers. Poxxie's site was run from an Indian server CVV2s.in [128].

Second, industrialized economies clearly perform better in terms of the economic and institutional conditions discussed above and thus provide unfavorable environment for cybercriminal. An upshot is that developing economies such as India become top cybercrime hotspots as cybercriminals are forced out of industrialized economies with strong controls, regulations and cybersecurity measures. For instance, security specialists believe that the arrests of several spambot operators in the U.S. forced others to operate from India and other developing countries [129]. Note that the U.S., which was No. 1 spam generator for many years, was not on the top 10 spam-sending countries list in 2011.

Third, a low level of income as discussed earlier is a key characteristic of a developing economy [28, 37]. India's low wages have been an attractive factor for performing some cybercrime activities from the country. One example concerns generating clicks on ads, and collecting commission from pay-per-click (PPC) programs. In this regard, most search terms cost just US$ 0.10–0.15 per click. Let's assume that it takes 8 s for an individual to click on an ad and view a page and the advertiser has to pay US$ 0.10 to a PPC provider for the click. At this rate, the clicker's activities generate US$ 45 per hour. Even if we assume that PPC providers and other intermediaries involved in click fraud activities take 90 % of this amount, the clicker can still make US$ 4.50 per hour. This amount is much higher than many people make in developing countries. Declining connectivity and computer costs have made this a reality.

To better illustrate how weak formal and informal institutions have facilitated cybercrimes, consider click fraud activities. There were reports that housewives, college graduates, and working professionals in India make US$ 100–200 per month by clicking on Internet ads [130]. It was reported that fraudsters openly advertised in national newspapers in India looking for people, who would use home computers to click on Internet ads [131]. Many click fraudsters engage in such activities just to make money and they do not know that their actions would be victimizing businesses.

Uneven and unequal development associated with the duality of the Indian economy [28, 37] has translated into differential risks as well as differential cybersecurity performance and capability. This can be illustrated best by comparing India's outsourcing sector with other economic sectors. The outsourcing sector has become the target of many high-profile cybercrime incidents. Consequently the industry was forced to take measures to strengthen the cybersecurity orientation.

The PPP constitutes an important force that has substantially contributed to strengthening cybersecurity in India. Contrary to the findings reported by Bures [31], the outcome of the NASSCOM-government partnership in India has been a fruitful one, which is based on mutual understanding and trust. As to the NASSCOM‘s measures to enhance cybersecurity, it is worth noting that the Indian economy is less centralized with more room for associations to flourish and to have a strong voice [132]. A strong mutual interdependence between the state and the private economic actors, particularly organized business groups, has developed very quickly after the economic liberalization of the 1990s.

It is also interesting to contrast and compare this situation with China, where non-government entities, special interest groups and the civil society are organized loosely. There is little room for these groups to influence national policymaking. Some nascent special-interest groups such as environmental and animal-rights organizations and sports clubs have placed new demands on the state and created competition for resources, attention, status and legitimacy. While such groups provide tremendous societal benefits, their potential for mobilizing people on a regional or even nationwide scale has increased the government's nervousness. Although China's industrial leaders and state science and technology officials have repeatedly appealed to the government to take measures necessary to increase the participation of the trade, industry and professional associations, unsurprisingly, the regime has responded with reluctance and resistance to accept an increased role of the independent civil society.

Regarding the low cybercrime reporting rates, it is worth noting that reporting rates are also low for some forms of conventional crimes. Chockalingam's [12] findings indicated that many crimes occurring in India are not reported, the police recorded version of facts about crimes may provide only a limited perspective on the realities of victimization and police figures "are only the tip of the iceberg". In order to provide further insights and a deeper understanding of this issue, it is important to consider primary and secondary victimization. Note that primary victimization occurs when a person becomes a victim of the crime itself. Some mechanisms involved in primary victimization include physical/psychological suffering or financial losses. Secondary victimization, on the other hand, takes place due to the actions of the victim's social environment. Key mechanisms involved in secondary victimization include stigmatization, social isolation, or intrusive and humiliating questioning [133]. Secondary victimization also occurs due to journalists' faulty and insensitive practices in gathering or reporting news or inappropriate actions of the criminal justice system [133]. As noted earlier, law enforcement agencies' unsupportive attitudes and unwillingness to help victims have contributed to a low reporting rate of cybercrime cases [68].

Prior researchers have noted that despite the existence of laws against cyber-harassment in India, the criminal justice system in the country has failed to perform its roles. Worse still, cybercrime victims may face further victimization [134]. For instance, in some cases of online victimization (e.g., bullying, stalking, defamation), as a response to the offender's actions, the victims themselves are likely to engage in activities that can be considered to be a crime. In such cases, police, lawyers and the courts may blame the victim of an online assault [135].

The issue of stigmatization deserves further elaboration and discussion. Wiesenfeld et al. [136] argue that arbiters' "constituent-minded sensemaking" influences stigmatization process. They have identified three categories of "arbiters"— social, legal, and economic [136]. Social arbiters include members of the press, governance watchdog groups, academics, and activists. Tandon [133] reported that Indian media have a tendency to invade the privacy of victims, offenders and celebrities. In this regard, some criminal activities are more likely to be of interest to the media than others. These may include crimes involving children, sexual offenses [133] and new criminal activities such as cybercrimes [7]. Concerns related to secondary victimization by the media are likely to result in low reporting rates. For instance, a study of four South Indian cities indicated that only 4 % of the victims of sexual offences had reported the crimes to the police [12].

Chockalingam [12] also found that, in cases involving consumer frauds and corruptions the reporting rate was less than 1 %. In such cases, consumers and citizens often fear that they would be penalized in future dealings with law enforcement agencies, government agencies and commercial organizations if they report such crimes [12]. In this example, law enforcement agencies, government agencies can be considered to be legal arbiters, who enforce rules and regulations. Commercial organizations on the other hand can be viewed as economic arbiters, who make decisions about engaging in economic exchange with individuals [136].

As noted earlier, among cybercrimes that are reported, prosecution rates are low. A main reason why cyber-offenders are often not criminally prosecuted may not be not because alternative sanctions are applied as predicted by the alternative sanctions argument [24], but no sanctions may be actually imposed. This is similar to what prior research has noted in the context of the economies in the Former Soviet Union and Central and Eastern Europe (FSU&CEE) [58]. On the other hand, while most international cybercriminals were found to "jurisdictionally shield" themselves in some FSU&CEE economies due to their low degree of cooperation and integration with the West, this is not the case for India-based cyber-offenders. As noted by prior white-collar crime researchers [25], resource limitations are of particular concern for addressing cybercrime issues in India due to their complexity, which require substantial amounts of investigative and prosecutorial efforts. The findings of prior research on cybercrime in FSU&CEE economies regarding the outdated regulative institutions and unwillingness of law enforcement agencies to pursue cyber-fraud cases as the criminals mainly victimize foreigners [58] are less relevant in India.

Regarding the regulative institutions, as mentioned earlier, while legal infrastructures are slow-moving institutions, laws, rules and regulations are considered to be fast moving institutions. India has been relatively quick in following the global trend in enacting cybersecurity related laws and regulations. For instance, the Information Technology Act was passed in 2000, which was amended in 2008 to address a number of issues (e.g., adoption of electronic signatures and a more detailed and careful approach to child pornography). For instance, the Information Technology Amendment Act of 2008 has made it an offence to facilitate the abuse of children online.

Nonetheless, the development of legal infrastructures such as building a well-functioning cybersecurity-related court system, employing judges well versed in cybersecurity and enforcement mechanisms has been a challenging problem for the GoI. Likewise, a large number of IT security auditors are needed to evaluate the adequacy of controls in the management of project and business processes and validate whether the controls are effective [137]. An estimate suggested that in 2013, India had only 60 auditors [76]. Regarding the requirement of government agencies to conduct security auditing of IT infrastructures, websites and applications, it is important to note that most Indian government agencies' websites are hosted by the National Informatics Centre (NIC), which was established by the GoI to promote IT culture among government organizations. It is argued that NIC-hosted websites are vulnerable to cyberattacks due to a shortage of manpower, especially IT security auditors. NIC outsources security audit works due to the lack of manpower. The country is also finding it difficult to enforce the RBI guidelines due to the lack of IT security auditors to validate banks' cybersecurity practices [138].

Concluding comments

India has begun developing ambitious digital projects such as the UIDAI. It is pursuing equally ambitious plans in the area of the development of cybersecurity professionals. Recent measures such as the National Cyber Security Policy (NCSP) can help put the Indian cybersecurity landscape on the path toward a brighter future. For instance, the lack of human resources is a key problem facing the GoI. If India is successful to accomplish even a part of the goal of developing 500,000 skilled cybersecurity professionals by 2018, it would be a considerable achievement.

While factors such as corruption, lack of accountability and weak law enforcement have created bottlenecks for development in India, such bottlenecks seem to have more negative effects on cybersecurity. In addition, cybercrime activities in India are also associated with a lower degree of stigmatization than in the West. Due to these factors, India's overall cybersecurity orientation is weak. Cybersecurity currently is also relatively a low priority for the GoI due to tremendous resource pressure to address problems related to poverty and underdevelopment. Overcoming these policy and institutional bottlenecks that constrain the country's ability to fight cybercrimes is central to improving the cybersecurity profile. This is important because this problem is increasingly recognized in broader economic sectors and thus no more limited to the offshoring industry.

The unique features of the Indian dual economy are connected in many ways with cybercrime and cybersecurity. In part, relatively lower rate of cybercrimes in India compared to that in some former Soviet economies may be due to the development of the legitimate IT industry. A related point is that India's low R&D profile is associated with the lack of the origin of sophisticated malware products.

It is reasonable to expect that cybersecurity awareness levels of consumers, businesses and policy makers will improve in the future. While culture is considered to be a slow-moving institution, even some aspects of culture that are linked to cybersecurity (e.g., a high propensity to share password) is likely to change over time. In order to further strengthen Internet users' cybersecurity orientation, contents related to cybersecurity need to be appropriately integrated in the high school and university curricula.

Major roles have been played by trade associations such as the NASSCOM to strengthen India's cybersecurity landscape. Such roles are especially valuable in the context of the state's weak regulatory roles in India. However, compliance is voluntary. Moreover, best practice security standards, procedures, guidelines developed by the NASSCOM have relatively little influence in strengthening cybersecurity outside the offshoring industry. While the DSCI's codes of behavior are irrelevant outside the offshoring sector, training and education to law enforcement personnel are one of the key mechanisms to strengthen the national cybersecurity profile. In this regard, one reason behind the extremely low conviction rate could be that the training programs provided by the DSCI often are insufficient to develop measurable competence in cybercrime investigation among law enforcement officers. A majority of the initiatives are special lectures or programs that do not last longer than 3–5 days. More comprehensive training programs will allow them to master the cybercrime investigation techniques, and feel confident about their ability to deal with cybercrimes. While most of the current programs mainly focus on police officers, the DSCI and the GoI need to place more emphasis on educating prosecutors, judges and lawyers using practical and layman's language.

Footnotes

[1] It is important to recognize that, as is the case of any underground economy [17], estimating the size of a country's cybercrime industry and its ingredients such as reporting rate is a challenging task. Cybercrime-related studies and surveys are replete with methodological shortcomings, conceptual confusions, logical challenges and statistical problems [18].

References

1. KPMG (2014).*Cybercrime survey report 2014*. Retrieve from www.kpmg.com/in.

2. indolink.com (2012). India battles against cyber crime. Retrieved from http://www.indolink.com/displayArticleS.php?id=102112083833.

3. Rid, T. (2012). Think again: cyberwar. *Foreign Policy*, *192*, 1–11.

4. bbc.co.uk (2012). *'Spam capital' India arrests six in phishing probe.* Retrieved from http://www.bbc.co.uk/news/technology-16392960.

5. King, R. (2011). *Cloud, mobile hacking more popular: Cisco.* Retrieved from http://www.zdnet.com/cloud-mobile-hacking-more-popular-cisco-1339328060/.

6. Aaron, G., & Rasmussen, R. (2012). *Global phishing survey: Trends and domain name use in 2H2011, APWG*, Retrieved from http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf.

7. Kshetri, N. (2010). The economics of click fraud. *IEEE Security and Privacy, 8*(3), 45–53.

8. Internet Crime Complaint Center (2011). *2010 internet crime report.* Retrieved from http://www.ic3.gov/media/annualreport/2010_ic3report.pdf.

9. Kshetri, N. (2009). Positive externality, increasing returns and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141–144.

10. cio.de (2014). India's biometric ID project is back on track. Retrieve from http://www.cio.de/index.cfm?pid=156&pk=2970283&p=1.

11. Thomas, T.K. (2012). *Govt will help fund buys of foreign firms with high-end cyber security tech*. Retrieved from http://www.thehindubusinessline.com/industry-and-economy/info-tech/article3273658.ece?homepage=true&ref=wl_home.

12. Chockalingam, K. (2003). Criminal victimization in four major cities in southern India. *Forum on Crime and Society, 3*(1/2), 117–126.

13. Holtfreter, K., VanSlyke, S., & Blomberg, T. G. (2005). Sociolegal change in consumer fraud: from victim-offender interactions to global networks. *Crime Law and Social Change, 44*, 251–275.

14. Kumar, J. (2006). Determining jurisdiction in cyberspace. The *Social Science Research Network* (*SSRN*). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=919261.

15. Sharma, V. D. (2002). International crimes and universal jurisdiction. *Indian Journal of International Law, 42*(2), l39–l55.

16. Benson, M. L., Tamara D. M & John E. E. (2009). White-collar crime from an opportunity perspective. In S. S. Simpson & D. Weisburd (Eds.) *The criminology of white-collar crime*(pp 175–193). Heidelburg: Springer International Publishing.

17. Naylor, R. T. (2005). The rise and fall of the underground economy. *Brown Journal of World Affairs, 11*(2), 131–143.

18. Kshetri, N. (2013). Reliability, validity, comparability and practical utility of cybercrime-related data, metrics, and information. *Information, 4*(1), 117–123.

19. Hindustan Times (2006). Securing the web.

20. Aggarwal, V. (2009). Cyber crime’s rampant. *Express Computer*. Retrieved 27 October, 2009,from http://www.expresscomputeronline.com/20090803/market01.shtml.

21. Narayan, V. (2010). *Cyber criminals hit Esc key for 10 yrs*.. Retrieved from http://timesofindia.indiatimes.com/city/mumbai/Cyber-criminals-hit-Esc-key-for-10-yrs/articleshow/6587847.cms.

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

23. Pontell, H. N., Calavita, K., & Tillman, R. (1994). Corporate crime and criminal justice system capacity. *Justice Quarterly, 11*, 383–410.

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

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

26. Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives*. New York, Berlin and Heidelberg: Springer.

27. Kshetri, N. (2010). Diffusion and effects of cybercrime in developing economies. *Third World Quarterly, 31*(7), 1057–1079.

28. UNDP (2006). *Country evaluation: Assessment of development results Honduras, New York: United Nations Development Programme Evaluation Office.* Retrieved from http://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf.

29. Tanaka, V. (2010). The 'informal sector' and the political economy of development. *Public Choice, 145*(1/20), 295–317. **23**.

30. Kshetri, N. (2015). India's cybersecurity landscape: the roles of the private sector and public-private partnership. *IEEE Security and Privacy, 13*(3), 16–23.

31. Bures, O. (2013). Public-private partnerships in the fight against terrorism? *Crime Law and Social Change, 60*(4), 429–455.

32. Salifu, A. (2008). Can corruption and economic crime be controlled in developing economies - and if so, is the cost worth it? *Journal of Money Laundering Control, 11*(3), 273–283.

33. Granovetter, M. (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology, 91*(3), 481–510.

34. Parto, S. (2005). Economic activity and institutions: *Taking Stock*, *Journal of Economic Issues*, *39*(1), 21–52.

35. Baumol, W. J. (1990). Entrepreneurship: Productive, unproductive, and destructive. *Journal of Political Economy 98*(5), 893–921.

36. North, D. C. (1990). *Institutions, institutional change and economic performance*. Cambridge: Harvard University Press.

37. Lewis, A. (1954). Economic development with unlimited supplies of labour. *Manchester School of Economic and Social Studies,* XXII (May *1954*), 139–91.

38. Chenery, H. B. (1975). The structuralist approach to development policy. *The American Economic Review*, *65*(2), Papers and Proceedings of the Eighty-seventh Annual Meeting of the American Economic Association, 310–316.

39. Acemoglu, D. (2005). Political economy of development and underdevelopment, *Gaston Eyskens Lectures*, Leuven, Department of Economics, Massachusetts Institute of Technology, Retrieved from http://economics.mit.edu/files/1064.

40. Acemoglu, D., Johnson,S., & Robinson.A.J. (2005). Institutions as a fundamental cause of long-run Growth, *Handbook of Economic Growth, IA. Edited by Philippe Aghion and Steven N. Durlauf Elsevier B.V.*, Retrieved from http://baselinescenario.files.wordpress.com/2010/01/institutions-as-a-fundamental-cause.pdf.

41. de Laiglesia, J. R. (2006). Institutional bottlenecks for agricultural development a stock-taking exercise based on evidence from Sub-Saharan Africa. *OECD Development Centre Working Paper No. 248*, Research programme on: Policy Analyses on the Institutional Requirements for Advancing Peace and Development in Sub-Saharan Africa, Retrieved from http://www.oecd.org/dev/36309029.pdf.

42. Greif, A. (1994). Cultural beliefs and the organization of society: a historical and theoretical reflection on collectivist and individualist societies. *Journal of Political Economy, 102*, 912–950.

43. Jones, E. L. (1981). *The European miracle: Environments, economies, and geopolitics in the history of Europe and Asia*. New York: Cambridge University Press.

44. Andreas, P. (2011). Illicit globalization: myths, misconceptions, and historical lessons. *Political Science Quarterly, 126*(3), 403–425.

45. Kshetri, N. (2005). Pattern of global cyber war and crime: a conceptual framework. *Journal of International Management, 11*(4), 541–562.

46. Roland, G. (2004). Understanding institutional change: fast-moving and slow-moving institutions. *Studies in Comparative International Development, 28*(4), 109–131.

47. Cohen, W., & Levinthal, D. (1990). Absorptive capacity: a new perspective on learning and innovation. *Administrative Science Quarterly, 35*, 128–152.

48. Dahlman, L., & Nelson, R. (1995). Social absorption capability, national innovation systems and economic development. In B. H. Koo & D. H. Perkins (Eds.), *Social capability and long-term growth* (pp. 82–122). Basingstoke: Macmillan Press.

49. Niosi, J. (2008). Technology, development and innovation systems: an introduction. *Journal of Development Studies, 44*(5), 613–621.

50. Kim, S. H., Wang, Q., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66–73.

51. Hawser, A. (2011). Hidden threat. *Global Finance, 25*(2), 44.

52. Kirk, J. (2012). *Microsoft finds new PCs in China preinstalled with malware*. Retrieve from http://www.pcworld.com/article/262308/microsoft_finds_new_computers_in_china_preinstalled_with_malware.html.

53. Benson, M., Cullen, F., & Maakestad, W. (1990). Local prosecutors and corporate crime. *Crime and Delinquency, 36*, 356–372.

54. Andreas, P., & Price, R. (2001). From war fighting to crime fighting: transforming the American National Security State. *International Studies Review, 3*(3), 31–52.
55. Collins, A. (2003). *Security and Southeast Asia: domestic, regional, and global issues.*Lynne Rienner Pub

56. Wenping, H. (2007). The balancing act of China's Africa policy. *China Security*, 3 (3), summer, 32–40.

57. Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Houndmills, Basingstoke: Palgrave Macmillan.

58. Kshetri, N. (2013). Cybercrimes in the former Soviet Union and Central and Eastern Europe: current status and key drivers. *Crime Law and Social Change, 60*(1), 39–65.

59. Kshetri, N., & Dholakia, N. (2009). Professional and trade associations in a nascent and formative sector of a developing economy: a case study of the NASSCOM effect on the Indian offshoring industry. *Journal of International Management, 15*(2), 225–239.

60. Oxley, J. E., & Yeung, B. (2001). E-commerce readiness: institutional environment and international competitiveness. *Journal of International Business Studies, 32*(4), 705–723.

61. Sobel, A. C. (1999). *State institutions, private incentives, global capital*. Ann Arbor: University of Michigan Press.

62. Lancaster, J. (2003). In India's creaky court system, some wait decades for justice; 82- year-old man still fighting charges dating to 1963. *The Washington Post* 27.

63. Edelman, L. B., & Suchman, M. C. (1997). The legal environments of organizations. *Annual Review of Sociology, 23*, 479–515.

64. Greenwood, R., & Hinings, C. R. (1996). Understanding radical organizational change: bringing together the old and the new institutionalism. *Academy of Management Review, 21*(4), 1022–1054.

65. catindia.gov.in (2014). History, Retrieve September 22, 2014, Retrieve from http://catindia.gov.in/History.aspx. Cyber Appellate Tribunal, Government of India.

66. Singh, S.R. (2014). *India's only cyber appellate tribunal defunct since 2011*. Retrieve from http://www.hindustantimes.com/india-news/india-s-only-cyber-appellate-tribunal-defunct-since-2011/article1-1235073.aspx.

67. Duggal, P. (2004). *What's wrong with our cyber laws?* Retrieved from http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml.

68. Anand, J. (2011). *Cybercrime up by 700% in Capital*. Retrieved from http://www.hindustantimes.com/India-news/NewDelhi/Cyber-crime-up-by-700-in-Capital/Article1-766172.aspx.

69. Nolen, S. (2012). India’s IT revolution doesn’t touch a government that runs on paper. *The Globe and Mail (Canada)*, A1.

70. indiatimes.com (2011b). Most Gurgaon IT, BPO companies victims of cybercrime: survey. Retrieved from http://timesofindia.indiatimes.com/city/gurgaon/Most-Gurgaon-IT-BPO-companies-victims-of-cybercrime-Survey/articleshow/10626059.cms.

71. Rahman, F. (2012). *Views: Tinker, tailor, soldier, cyber crook*. Retrieved from http://www.livemint.com/2012/04/06111007/Views--Tinker-tailor-soldie.html?h=A1.

72. timesofindia.com (2009). *Nigerians held for internet fraud, May 28*. Retrieved March 1, 2011 from http://articles.timesofindia.indiatimes.com/2009-05-28/kolkata/28212706_1_kolkata-police-prize-moneyracket/2.

73. indiatimes.com (2011a). *Two including Nigerian held for job fraud.* Retrieved from http://articles.timesofindia.indiatimes.com/2011-02-16/gurgaon/28551786_1_nigerian-gang-job-racket-bank-account.

74. Saha, T., & Srivastava, A. (2014). Indian women at risk in the cyber space: a conceptual model of reasons of victimization. *International Journal of Cyber Criminology, 8*(1), 57–67.

75. timesofindia.indiatimes.com (2013). *Government releases national cyber security policy 2013*. Retrieve from http://timesofindia.indiatimes.com/tech/it-services/Government-releases-National-Cyber-Security-Policy-2013/articleshow/20874965.cms.

76. Doval, P. (2013). Govt orders security audit of IT infrastructure. Retrieve from http://timesofindia.indiatimes.com/tech/tech-news/Govt-orders-security-audit-of-IT-infrastructure/articleshow/38398644.cms.

77. De Mooij, M. K. (1998). *Global marketing and advertising: Understanding cultural paradoxes*. CA: Sage.

78. The Economist. (2005). Business: busy signals; Indian call centres. *The Economist, 376*(8443), 66.

79. Mishra, B.R. (2010). *Wipro unlikely to take fraud accused to court, business-standard.com.* Retrieved March 1, 2011, from http://www.business-standard.com/india/news/wipro-unlikely-to-take-fraud-accused-to-court/386181/.

80. Phukan, S. (2002). IT ethics in the Internet age: New dimensions. *InSITE*. Retrieved October 27,2005,
from http://proceedings.informingscience.org/IS2002Proceedings/papers/phuka037iteth.pdf.

81. Sawant, N. (2009).Virtually speaking, crime in the city on an upward spiral, *Times of India.* Retrieved from http://timesofindia.indiatimes.com/news/city/mumbai/Virtually-speaking-crime-in-the-city-on-an-upward-spiral/articleshow/5087668.cms, accessed 27 October 2009.

82. PRLog (2011). *India Plans to set-up state-of-the-art information technology institute to combat cybercrime: India requires 2.5 lakh cyber specialists to deal with the menace of cybercrime*. Retrieved from http://www.prlog.org/11302019-india-plans-to-set-up-state-of-the-art-information-technology-institute-to-combat-cybercrime.html.

83. Saraswathy, M. (2012). *Wanted: ethical hackers.* Retrieved
from http://www.wsiltv.com/news/three-states/Protect-Yourself-from-Cyber-Crime-139126239.html.

84. ciol.com (2012). *Most Indians unaware of security solns: study*. Retrieved
from http://www.ciol.com/Infrastructure-Security/News-Reports/Most-Indians-unaware-of-security-solns-study/161905/0/.

85. foxnews.com (2012). *Indian lawmakers filmed 'watching porn on phone during assembly' resign*. Retrieved from http://www.foxnews.com/world/2012/02/08/indian-lawmakers-filmed-watching-porn-on-phone-during-assembly-resign/.

86. The World Bank Group (2014). *Researchers in R&D (per million people).* Retrieve
from http://data.worldbank.org/indicator/SP.POP.SCIE.RD.P6?page=2.

87. rediff.com (2008). *Researchers? Only 156 per million in India.* Retrieved
from http://www.rediff.com/money/2008/mar/12rnd.htm.

88. Economictimes (2005). *R&D in India: The curtain rises, the play has begun, August 24*. Retrived August 11, 2011 from: http://economictimes.indiatimes.com/rd-in-india-the-curtain-rises-the-play-hasbegun/articleshow/1207024.cms.

89. Shaftel, D., & Narayan, K. (2012). Call centre fraud opens new frontier in cybercrime. Retrieved September 1, 2016, from http://www.livemint.com/2012/02/26225530/Call-centre-fraud-opens-new-fr.html.

90. Gardner, T. (2012). *Indian call centres selling your credit card details and medical records for just 2p*. Retrieved from http://www.dailymail.co.uk/news/article-2116649/Indian-centres-selling-YOUR-credit-card-details-medical-records-just-2p.html.

91. Economist.com (2007). Imitate or die. http://www.economist.com/node/10053234/ .

92. Robinson, G. E. (1998). Elite cohesion, regime succession and political instability. *Syria Middle East Policy, 5*(4), 159–179.

93. Kshetri, N. (2011). Cloud computing in the global south: drivers, effects and policy measures. *Third World Quarterly, 32*(6), 995–1012.

94. Borland, J . (2010). *A Four-Day Dive Into Stuxnet's Heart, December 27*. Retrieved 1 September 2016 from https://www.wired.com/2010/12/a-four-day-dive-into-stuxnets-heart/.

95. Halsey, M. (2011). *How is IE6 contributing to China's growing Cyber-Crimewave?*Retrieved from http://www.windows7news.com/2011/12/30/ie6-contributing-chinas-growing-cybercrimewave/.

96. Greenberg, A. (2007). The top countries for cybercrime. *Forbes.com*. Retrieved April 9, 2008, from http://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html.

97. Arnott, S. (2008). *Cyber crime stays one step ahead*. Retrieved October 27,2009, from http://www.independent.co.uk/news/business/analysis-and-features/cyber-crime-stays-one-step-ahead-799395.html.

98. Paget, F. (2010). McAfee helps FTC, FBI in case against 'scareware' outfit. Retrieved January 26, 2011, from http://blogs.mcafee.com/mcafee-labs/mcafee-helps-ftc-fbi-in-case-against-scareware-outfit.

99. Fest, G. (2005). Offshoring: feds take fresh look at India BPOs; major theft has raised more than a few eyebrows. *Bank Technology News, 18*(9), 1.

100. Engardio, P., Puliyenthuruthel, J., & Kripalani, M. (2004). Fortress India? *Business Week, 3896,* 42–43.

101. King, A. A., & Lenox, M. J. (2000). Industry self-regulation without sanctions: the chemical industry's responsible care program. *Academy of Management Journal, 43*(4), 698–716.

102. Vinogradova, E. (2006). Working around the state: contract enforcement in the Russian context. *Socio-Economic Review, 4*(3), 447–482.

103. Walzer, M. (1993). Between nation and world: welcome to some new ideologies. *The Economist, 328*(7828), 49–52. **September 11**.

104. Greenwood, R., Suddaby, R., & Hinings, C. R. (2002). Theorizing change: the role of professional associations in the transformation of institutionalized fields. *Academy of Management Journal, 45*(1), 58–80.

105. Marshall, R. S., Cordano, M., & Silverman, M. (2005). Exploring individual and institutional drivers of proactive environmentalism in the US wine industry. *Business Strategy and the Environment*, *14*(2), 92–109.

106. Ahlstrom, D., & Bruton, G. D. (2001). Learning from successful local private firms in China: establishing legitimacy. *Academy of Management Executive, 15*(4), 72–83.

107. Scott, W.R. (1992). *Organizations: Rational, natural and open systems*. Prentice Hall.

108. Trombly, M. (2006). India tightens security. *Insurance Networking & Data Management, 10*(1), 9.

109. Dickson, M., BeShers, R., & Gupta, V. (2004). The impact of societal culture and industry on organizational culture: Theoretical explanations. In R. J. House, P. J. Hanges, M. Javidan, P. W. Dorfman, & V. Gupta (Eds.), *Culture, leadership, and organizations: the GLOBE study of 62 societies*. Thousand Oaks: Sage Publications.

110. Lawrence, T. B., Winn, M. I., & Jennings, P. D. (2001). The temporal dynamics of institutionalization. *Academy of Management Review, 26*(4), 624–644.

111. Audretsch, D., & Stephan, P. (1996). Company scientist locational links: the case of biotechnology. *American Economic Review, 30*, 641–652.

112. Feldman, M. (1999). The new economics of innovation, spillovers and agglomeration: a review of empirical studies. *Economics of Innovation and New Technology, 8,* 5–25.

113. Niosi, J., & Banic, M. (2005). The evolution and performance of biotechnology regional systems of innovation. *Cambridge Journal of Economics, 29,* 343–357.

114. Rao, H.S. (2006). *Outsourcing thriving in Britain despite India bashing*. Retrieve from http://www.rediff.com/money/2006/oct/07bpo.htm.

115. AFX News (2006). *India could process 30 pct of US bank transactions by 2010 - report*. Retrieve from http://www.finanznachrichten.de/nachrichten-2006-09/7050839-india-could-process-30-pct-of-us-bank-transactions-by-2010-report-020.htm.

116. Hazelwood, S. E., Hazelwood, A. C., & Cook, E. D. (2005). Possibilities and pitfalls of outsourcing. *Healthcare Financial Management, 59*(10), 44–48.

117. Das, G. (2011). *Panel to advise govt, IT cos on cloud security on the cards.* Retrieved from http://www.financialexpress.com/news/Panel-to-advise-govt--IT-cos-on-cloud-security-on-the-cards/809960/.

118. Schwartz, K. D. (2005). The background-check challenge. *InformationWeek*, 59–61.

119. Indo-Asian News Service (2006). Nasscom to set up self-regulatory organization. September 26.

120. Cone, E. (2005). Is offshore BPO running aground? *CIO Insight, 53*, 22.

121. COMMWEB (2007). India will train police to catch cybercriminals.

122. DSCI (2014). *Cyber Labs.* Retrieve from http://www.dsci.in/cyber-labs.

123. Tribuneindia.com (2005). Outsourcing crime call centre expose can wreak havoc, June 25. Retrieved from http://www.tribuneindia.com/2005/20050625/edit.htm.

124. Jaishankar, K. (2008). Identity related crime in the cyberspace: examining phishing and its impact. *International Journal of Cyber Criminology, 2*(1), 10–15.

125. Segal, A. (2012). Chinese computer games. *Foreign Affairs, 91*(2), 14–20. **7**.

126. dhs.gov (2011). *United States and India Sign Cybersecurity Agreement*. Retrieved from http://www.dhs.gov/ynews/releases/20110719-us-india-cybersecurity-agreement.shtm.

127. Bhaumik, A. (2012). India, allies to combat cybercrime. Retrieved from http://www.deccanherald.com/content/249937/india-allies-combat-cybercrime.html.

128. Riley, M. (2011). *Stolen Credit Cards Go for $3.50 at Amazon-Like Online Bazaar*. Retrieved on 1 September 2016 from http://www.bloomberg.com/news/articles/2011-12-20/stolen-creditcards-go-for-3-50-each-at-online-bazaar-that-mimics-amazon.

129. Trend Micro Incorporated (2011). *Trend micro third quarter threat report: Google and oracle surpass microsoft in most vulnerabilities.* Retrieved from http://www.sacbee.com/2011/11/14/4053420/trend-micro-third-quarter-threat.html.

130. Vidyasagar, N. (2004). *India's secret army of online ad 'clickers'*. Retrieved October 27,2008, from http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms.

131. Kehaulani, S. (2006). 'Click Fraud' threatens foundation of web ads; Google faces another lawsuit by businesses claiming overcharges. *The Washington Post*, A.1.

132. Frankel, R. (2006). *Associations in China and India: An overview, European Society of Association Executives*. Retrieved from http://www.esae.org/articles/2006_07_004.pdf.

133. Tandon, N. (2007). Secondary victimization of children by the media: an analysis of perceptions of victims and journalists. *International Journal of Criminal Justice Sciences, 2*(2), 119–135.

134. Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: a comparative analysis of US, UK and India. *Victims and Offenders, 6*(4), 386–398.

135. Halder, D., & Jaishankar, K. (2015). Irrational coping theory and positive criminology: A frame work to protect victims of cyber crime. In N. Ronel & D. Segev (Eds.), *Positive criminology* (pp. 276–291).

136. Wiesenfeld, B. M., Wurthmann, K. A., & Hambrick, D. C. (2008). The stigmatization and devaluation of elites associated with corporate failures: a process model. *Academy of Management Review*, *33*(1), 231–251.

137. Hettigei, N.T. (2005). The Auditor's role in IT development projects. Retrieve from http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Pages/The-Auditors-Role-in-IT-Development-Projects1.aspx.

138. Bradbury, D. (2013). India's Cybersecurity challenge. Retrieve from http://www.infosecurity-magazine.com/view/34549/indias-cybersecurity-challenge/.