Diffusion and Effects of Cyber-Crime in Developing Economies

By: Nir Kshetri

Kshetri, N. (2010) "Diffusion and Effects of Cybercrime in Developing Economies," Third World Quarterly, 31(7), 1057 – 1079.

***** Tables are missing from this format of the document.*****

Abstract:

Cyber-crime's footprints across the developing world are getting bigger. The aim of this article is to examine the structure of cyber-crimes in developing economies. Its central idea is that economic and institutional factors facing cyber-criminals and potential victims in the developing world are different from those in the developed world. In economies characterised by low internet penetration rates and few resources devoted to fighting cyber-crimes, formal institutions related to such crimes tend to be thin and dysfunctional. A cyber-criminal is less likely to be stigmatised in such economies. Moreover, organisations' and individuals' technological and behavioural defence mechanisms are likely to be weaker. Many people in developing economies are also attracted into cyber-crime because of high unemployment and low wages.

Keywords: developing economies | cybercrime | crime in developing countries | cyber-criminals

Article:

Cyber-crime's footprints across the developing world are getting bigger. The aim of this article is to examine the structure of cyber-crimes in developing economies. Its central idea is that economic and institutional factors facing cyber-criminals and potential victims in the developing world are different from those in the developed world. In economies characterised by low internet penetration rates and few resources devoted to fighting cyber-crimes, formal institutions related to such crimes tend to be thin and dysfunctional. A cyber-criminal is less likely to be stigmatised in such economies. Moreover, organisations' and individuals' technological and behavioural defence mechanisms are likely to be weaker. Many people in developing economies are also attracted into cyber-crime because of high unemployment and low wages.

With the internet's rapid diffusion and the digitisation of economic activities cyber-crime has gained momentum in developing economies. According to some estimates, the global cyber-crime industry has been generating US$1 trillion annually in recent years. Developing world-based criminals are playing important roles in the cyberworld's criminal value chain. There are also reports that traditional organised crime groups in developing countries have been involved in cyber-crime. For instance, Chinese gangs, Colombian cartels and Russian and Malaysian organised crime groups have reportedly employed hackers, diverted their efforts from traditional activities to cyber-crime and expanded their businesses globally.1

Cyber-crimes originating from some developing economies have also opened up new discourses in international relations. For instance, an FBI assistant director noted: ‘Cybercrime … is the fastest-growing problem faced by China–US cooperation’.2 In early 2010, reports of attacks on Google's Gmail accounts by China-based hackers raised the ire of many internet users.

Some developing countries are top cyber-crime sources (see Tables 1 –3). According to Kaspersky Labs, in 2009 seven of the top 10 countries for creating trojans designed to steal passwords were developing countries, which accounted for 92 per cent of such trojans globally (see Table 2).3 Businesses and consumers in developing countries have also become victims of domestic as well as international cyber-crimes. Since most of the growth in the global PC market in the near future is likely to come from developing countries, cyber-crimes in these countries deserve special attention. Analysing the trend of cyber-crime activities across countries, analysts have suggested 10–15 per cent internet penetration as the threshold level for the generation of significant hacking activities.4 Internet penetration in many developing countries has reached this level.

*****TABLES 1-3 ARE OMITTED FROM THIS FORMATTED DOCUMENT*****

The underlying notion in this paper is that cyber-crimes are characterised by important structural differences in developing and developed countries. The sources, targets and other ingredients differ structurally between the two types of country. First, as we have demonstrated, economic factors facing cyber-criminal and cyber-crime victims are significantly different in developing and developed countries. They include the nature and quality of hardware, software and infrastructure, targetability of victims, stock of cyber-crime skills and associated opportunity costs and benefits.

A second, probably more significant factor, relates to formal and informal institutions in these economies. Cyber-criminals' activities can be explained in terms of destructive entrepreneurship.5 The society's ‘rules of the game’, known as institutions affect the extent of such activities.6

Institutions can be better understood in the context of the tasks for which they were created.7 Relevant institutions from the standpoint of cyber-crime include the availability of jurisdictional

arbitrage and strength of rule of law and stigmatisation issues associated with becoming a cyber-criminal or a cyber-crime victim.

A final reason why cyber-crimes are likely to differ in developing and developed countries is related to cognitive factors. Cyber-criminals and victims in developing countries are likely to differ in their cognitive assessment of crimes as well as in confidence, skills and experiences.

A brief survey of cyber-crimes in developing countries

Tables 1 and 2 present some indicators related to cyber-crimes in developing countries. Table 3 presents qualitative indicators for selected countries. In some cities, such as Mumbai in India, more cyber-crime cases are being registered with the police than conventional crimes such as murder, burglary and arson.8

An increasing number of cyber-attacks targeting developing countries are international in nature. For instance, it is reported that cyber-criminals from Malaysia, Japan, Korea, the US and China have targeted computers in the Philippines.9 In a well publicised case it was found that Canada-based hackers employed about 100 000 poorly protected ‘zombie’ computers mainly in developing countries such as Poland, Brazil and Mexico and stole $44 million.10 Experts argue that this is an indication of a change in the victim/victimiser pattern and an unusual case of role reversal.

Gordon and Ford have discussed Type I and Type II cyber-crimes. Because of their lower digitisation, Type II cyber-crimes, which mainly involve human elements, are likely to be proportionately higher in developing countries than in industrialised countries.11 For instance, many Indians are reported to be victims of various versions of ‘Nigerian 419’ fraud,12 which involve criminal–victim interaction.13

Broadband connections and increase in cyber-crime

In a discussion of cyber-crime in developing economies the rapid proliferation of broadband connections in these economies deserves special attention. At this point we should emphasise that one reason why US computers are attractive targets for cyber-criminals is because they are always online and have broadband connections. Note that serious cyber-crimes require bandwidth-intensive applications. A related point is that African networks do not attract the same level of attention from hackers as other regions of the world because of the low level of connectivity of the region and low broadband penetration. From the criminal's standpoint the African environment is thus highly unreliable for carrying out cyber-attacks effectively.14 Note that typical ‘bot-herders’ control tens of thousands and even millions of ‘zombie’ computers.

Not long ago most African economies lacked fibre-optic cable and relied on slower satellite links, which meant longer time to attack local websites.15 In June 2009 East Africa got its first fibre-optic submarine cable. Two additional companies were expected to complete similar

projects by the end of 2009. This would speed up the connections in Kenya, Burundi, Rwanda, Tanzania and Uganda, Somalia, Ethiopia and Sudan. Analysts argue that Africa and other developing countries are likely to experience a rapid cyber-crime growth as broadband technology takes off.16 For instance, Kenya experienced about 800 bot attacks per day in July 2009, which is projected to increase to 50 000 per day after the fibre connectivity goes live.17

Cyber-crime proliferation is associated with and facilitated by the growth of broadband networks. In the early 2000s estimates suggested that about one-third of all spam came from zombie computers with broadband connections.18 Estimates suggested that in recent years most zombie computers are connected to broadband internet.

A number of developing countries is experiencing rapid broadband growth. Analysts argue that increased penetration of broadband in developing countries is likely to make these countries a fertile ground for hackers. It is argued that rise of cyber-crime in China can be mainly attributed to the rapid growth of broadband users in the country.19 China's broadband subscriber base grew by 114 per cent in 2004, 57 per cent in 2005 and 38 per cent in 2006 and is expected to experience double-digit growth for the next few years. China's broadband subscriber base surpassed that of the US in 2008.20

Likewise, broadband connections in Latin America increased by 41 per cent in 2007 and, by 2013, average consumer broadband penetration in the region is expected to reach 30 per cent.21 In Peru the number of broadband subscribers rose by over 80 per cent annually during 2001–06.22

Economic and institutional factors related to cyber-crime in developing economies

Formal institutions: permissiveness of regulatory regimes

Most cyber-crimes are committed by organised criminal groups. To understand organised criminal groups' operations, it may be helpful to consider them as rational economic actors with a goal of profit maximisation.23 Their profit depends upon the capability to emulate market mechanisms. This may require formation of strategic alliances, making appropriate capital investment decisions, identifying new growth areas, investing in R&D, adopting modern accounting systems and insuring against risks.24

The research literature provides abundant evidence that, like multinational firms, organised crime groups consider a number of factors when making decisions related to geographic location of their activities. Perhaps the most important factor influencing the location decision is the strength of the rule of law. A person's decision to participate in an illegal activity is a function of the expected probability of apprehension and conviction and the expected penalty if convicted.25 Many developing countries' weak rule of law and permissive regulatory regimes provide a fertile ground for criminal activities.26

Developing economies vary in their degrees of readiness in terms of regulatory institutions to deal with cyber-crime. In Africa, for instance, as of September 2009 Kenya and Rwanda recognised electronic signature and electronic crimes. In Tanzania and Uganda, on the other hand, the bills to recognise electronic signature and electronic crimes were at the parliament level.27

While an increasing number of developing economies has enacted laws to deal with cyber-crime, they lack enforcement mechanisms. As one might expect, developing countries lack judges, lawyers and other law enforcement personnel who understand cyber-crimes. For instance, the director of Malaysia's HeiTech Padu Berhad noted that out of the country's 40 000 lawyers, only four were able to handle cyber-crime.28 Similarly, in 2004, of the 4400 police officers in Mumbai, only five worked in the cyber-crime division.29

Cyber-crime awareness is low among the law enforcement community. It was reported that, when a police officer was asked to seize the hacker's computer in an investigation of a cyber-crime in India, he brought the hacker's monitor. In another cyber-crime case, the police seized the CD-ROM drive from a hacker's computer instead of the hard disk.30 Likewise, eBay's Albena Spasova, who worked to promote law reform in Moldova and Bulgaria noted: ‘Even in 2001, I was meeting judges who thought cyber-crime was someone stealing a computer’.31

Regulatory institutions in developing economies are also insufficient and impractical for dealing with cyber-crimes. Experts say that Indian law on computer crime is ‘fuzzy’.32 India's IT Act 2000 did not cover phishing, cyber-stalking or cyber-harassment.33 The it (Amendment) Act 2008, however, has specific provisions on how various cyber-crimes such as publishing sexually explicit material, cyber-terrorism, Wi-Fi hacking, sending and viewing child pornography, identity theft and spam creation are punished.34

Similarly, because of a lack of cybercrime laws, Indonesian police have been using a ‘red book’, a manual to conduct credit card investigations available since 1997, to handle internet credit card fraud.35 Likewise, according to Brazil's legislation enacted in 1988, a hacker cannot be charged for breaking into a site, or distributing a virus, unless it is proven that the action resulted in a crime.36 In the same vein, Romanian law requires cyber-crime victims to send police a signed complaint and be represented at the hearing.37 It is thus highly impractical for most US-based eBay fraud victims to bring a case in the Romanian courts.

In Indonesia only 15 per cent of reported incidents are actually investigated.38 In India about 10 per cent of cyber-crimes are reported and, of those reported, about two per cent are actually registered. The conviction rate is as low as two per cent.39 As of 2006 no one charged with data fraud in India had been convicted.40 As of August 2009 only four people had been convicted of cyber-crime.41

Industrialised economies are also forced to develop regulatory infrastructures to deal with cyber-crimes because they experience more of them. In these countries some laws also require

businesses to enhance their defences against cyber-crimes. One estimate suggested that US banks spent $60 million in 2002 on technology to comply with the requirements of the Patriot Act.42

Although criminals are emboldened if laws are weak, a much higher degree of jurisdictional arbitrage is available where digital crimes are concerned. Not surprisingly organised cyber-crimes are initiated from countries that have few or no laws directed against cyber-crimes and little capacity and willingness to enforce existing laws. Commenting on Africa's currently low level but high growth potential of cyber-crimes, Hamadoun Toure, secretary-general of the International Telecommunication Union (ITU) put it this way: ‘At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity’.43

We noted above that national level institutions dealing with cyber-crime in developing countries are thin and dysfunctional. Equally problematic are institutions at industry and inter-organisational levels. For instance, there is no insurance company in India that offers a comprehensive anti-cybercrime policy for a company.44

Resources to fight cyber-crimes

Developing economies lack the resources to build institutions to combat cyber-crime.45 Consider, for example, the town of Ramnicu Valcea in Romania, where a large number of eBay fraud cases originate. In 2005 two law enforcement officers in the town were dealing with over 200 eBay cases with a nine-year-old computer that had no internet connection. To connect to the internet they had to use the same cafes used by cyber-criminals for eBay fraud.46 Similarly, in the ITU Regional Cyber-security Forum for Eastern and Southern Africa held in Zambia in 2008, an expert from the Democratic Republic of Congo stated that factors such as the lack of legal experts in information and communication technology (ICT) and poor understanding of ICTs and its added value in the national economy was hindering the adoption of cyber-security-related legislation in the country.47 Likewise, in Bangladesh cellphones with unregistered subscriber identity module (SIM) cards have been increasingly used for extortion activities. However, the cyber-crime unit of the Dhaka Metropolitan Police has not been equipped to handle such crimes.48

Cyber-criminals' confidence

Increased success is sending positive cognitive messages and making cyber-criminals more brash and disrespectful of law enforcement agencies.49 Because of weak law enforcement machinery in developing countries, cyber-criminals in these countries are more confident than those in developed countries. A Brazilian computer forensics expert in Sao Paolo, noted that internet crime gangs in the country do not use techniques to hide themselves.50 Likewise it is reported that many developing world-based hackers targeting US networks do not conceal their real identities or the origins of their emails.51

Informal institutions: social legitimacy and cyber-crime

We noted above how regulatory permissiveness has been a driving force behind the growth of the crime industry. But the more immediate—and also the more foundational—reason behind rapidly rising global cyber-crime relates to the degree of social legitimacy of such crimes. Condemnation of an act such as a cyber-crime leads to internalisation of norms against the act among the 'condemners' as well as the 'condemned.52 Proponents of 'gay rights' legislation, for instance, argue that the real battle centres on gaining social and cultural acceptability, achieving social legitimacy of such rights,53 and stigmatising 'orthodox religious believers'.54

Various factors lead to less guilt in cyber-crimes compared with conventional crimes.55 Most obviously, these conditions are more pervasive in developing countries as many internet users in these countries are connected to the internet for the first time.56 A related point is that developing and developed countries may also differ in terms of social stigma associated with becoming a cyber-crime victim. In sum, cyber-crimes tend to be more justifiable in developing countries than in developed countries.

Defence mechanisms against cyber-crimes

Countries across the world differ in the deployment of security products to address such holes. In 2002 North America accounted for 58 per cent of the global security product market.57 An estimate suggested that in 2006, about three million of Brazil's small and medium sized enterprises (SMEs) lacked anti-virus software in their PCs.58 Sixty percent of Kenyan banks are reported to have insecure systems.59

The concept of 'hollow diffusion' of internet and e-commerce technologies among firms in developing economies such as China may help us understand weak defence mechanisms.60 The basic idea behind 'hollow diffusion' is simple: many companies adopting e-commerce, especially in developing countries, lack technological and human resources, and other fundamental ingredients needed for long-term success. In short, they lack true depth of internet adoption. 'Hollow diffusion' can take place in human terms (lack of skills and experience) as well as in technological terms (failure to use security products).61 It is argued that organisations that adopt internet technologies without considering the costs and efforts needed to maintain those systems generate a negative externality.62 A related point is that, compared with dominant multinationals, ICT vendors in developing countries tend to be smaller businesses and later entrants into the global ICT market.63

Hardware and software used in developing economies

Of equal importance in the discussion below of cyber-crime in developing countries is the nature of hardware and software in these countries. According to the product-cycle approach, ICT products are adapted in developing countries to meet the conditions of local markets and processes and to local technological capacity.64 Most ICT products targeted for developing

countries are low-cost versions, as advanced features make them unaffordable.65 At the same time universities and other organisations are taking measures to make products available at low cost. For instance, Universities Allied for Essential Medicines (UAEM) has called for ‘open-access’ patents from universities to increase low income countries’ access to medicines.66 In some cases entirely new products are developed for developing world-based consumers. A case in point is Whirlpool's launch of the world's cheapest automatic washer in the $150–200 price range.67

As an example of entirely new products designed for developing world-based consumers, the One Laptop per Child (OLPC) programme deserves special attention. The programme aims to provide low-cost computers to children in developing countries. The goal of the OLPC project was to deploy 100 million laptops in the first year.68 While this has not materialised, the OLPC programme has made significant progress. As of early 2008 there were an estimated 250 000 children from developing countries across the world who owned laptops under the OLPC programme.69 These computers run on Linux and have a security system called BitFrost.70 BitFrost's built-in features prevent viruses and other programmes from ‘damaging the computer, stealing files, or spying on the user’.71 It has been robust against viruses so far. Analysts argue, however, that hackers may find previously unknown flaws in BitFrost.72 To substantiate this claim, we draw a parallel with the recent intensification of cyber-crime targeting Macs. It is worth noting that cyber-criminals have extended their efforts beyond Windows and such efforts are becoming more sophisticated over time. For instance, while some viruses targeting Macs existed before, Apple's computers experienced financially motivated attacks from organised criminal groups for the first time in 2007.73

The OLPC program is facing competition from Intel's low-cost Classmate computers designed for children in developing countries.74 Intel sold ‘tens of thousands’ of its first generation of Classmate PCs, which were launched in early 2007.75 The company announced its plan to start selling a new generation of Classmate PCs in April 2008. The Classmate computers operate on Windows' cut-down versions.76 As noted above, most viruses and botnets attack Windows.

Internet users' skills

Another problem is related to lack of skills. Many internet users in developing economies are inexperienced and not technically savvy. A high proportion of them are getting computers and connecting them to the internet for the first time.77 A majority of new internet users in developing countries also lack fluency in the English language. While the developments of user-friendly software and interfaces have reduced the complexity and consumer learning requirements for computer and internet use,78 such developments have not taken place in the development of security products.

Most of the information, instructions, and other content for security products are available in English only.79 Many internet users in developing countries are thus unable to use IT security

products. Even if Microsoft publishes a security bulletin in Chinese, say, it is unlikely to do so in all the 20 Chinese dialects.80

International hierarchical pattern in the diffusion of security products

It is also important, in this context, to look at the connection between a country's market size and the availability of technology products in the country. Most developing countries lack market and infrastructures for such products.81 Put differently, international diffusion of technology products exhibits a ‘hierarchical pattern’.82 As is the case with other technologies, commercial distributors of IT security products often find developing countries unprofitable for their markets, which leads to adverse international hierarchical patterns of such products. A related point is that the international hierarchical pattern is more adverse for security products. While the top security software firms are US-based, businesses and consumers in some developing countries (eg Southeast Asia) prefer to buy domestically manufactured software for reasons of nationalism.83

Concentration of crimes

Deutsch et al have suggested that the return to crime is positively related to the concentration of criminals in a neighbuorhood.84 Criminals tend to focus their efforts in a few neighbourhoods, or crime hot spots, ‘overwhelming’ the law enforcement agencies and police forces there.85 As middle classes tend to avoid ‘high crime areas’, crime hot spots tend to be inner city, low-income neighbourhoods.86 It is also suggested that sparsely populated neighbourhoods are associated with a high rate of violent crimes.87 Note that in the conventional world most crimes are committed close to home. Criminals travel long distances only if there are sufficient incentives to leave known territory.88

It was apparent from our review that cyber-crimes targeting developing economies exhibit a heavy concentration in specific industry sectors. In China businesses in the online gaming industry and gamers have been attractive targets for hackers.89 These hackers steal gamers' passwords and login information (eg World of Warcraft). The stolen virtual items and identities are then auctioned online.90 Experts say that an online gaming account in China can be sold for up to $1000, compared with $5–10 for stolen credit card data.91

In Brazil a large number of cyber-crimes involves malicious codes, most notably keylogging viruses, designed to steal banking passwords.92 Email spam is becoming more personalised.93 Cyber-criminals also use sophisticated social engineering scams to trick Brazilians. According to the Brazilian Banks Association, estimated losses associated with virtual fraud in 2005 were $165 million.94 Cyber-criminals make a rapid adaptation in password-stealing malware to the changes made by banks.95

Most high-profile and widely publicised cyber-crimes in India are concentrated in the offshore sector.96 It was reported in February 2010 that an employee in the IT giant Wipro used his

colleague's password to steal some $4 million from the company's bank account.97 Data frauds have been reported in call centres in Pune, Hyderabad, Bangalore and Gurgaon. The British tabloid newspaper, The Sun, reported that an Indian call centre employee sold confidential information on 1000 bank accounts to its reporter working undercover.98 In another case, call-centre workers at a Pune subsidiary of Mphasis, a provider of outsourcing services, transferred about $500 000 from four Citibank customers' accounts to their personal accounts.99 It is reported that in major Indian cities there are ‘data brokers’, who obtain data illegally from people working in offshore companies.100

The common denominator to the above examples is that businesses and consumers in leading e-commerce sectors in a developing economy are more likely to be cyber-crime targets compared with other less e-commerce-ready industries. In China, for instance, online games generated $1.8 billion in 2007,101 and the buying and selling of virtual items has been a ‘mini-economy’ in China.102

Similarly, a majority of Brazilians conduct their banking activities online.103 Indeed, financial services are among the leading e-commerce sectors and banks are positioned to be leaders in e-marketplaces and in e-payment solutions in Brazil and other Latin American countries.104 Similarly the Indian offshore industry's revenue grew from $4.8 billion in fiscal year 1997–98 to $47.8 billion in 2006–07.105

Path dependence externalities generated by conventional crimes and cyber-crimes

As a result of path dependence, other things being equal, the more a particular type of crime a society has had in the past, the higher the odds of observing crimes of that type in that society.

Given the cyber-crime environment and feedback loops, increasing returns could manifest themselves in many ways. For instance, cyber-criminals may ‘invent’ sophisticated and new tools that law enforcement agencies face increased difficulty in tracing. Cyber- criminals could also operate from countries with weak cyber-crime laws.106 The externality could also arise because, at a given level of law enforcement resources, an increase in the number of cyber-criminals reduces the probability that any one cyber-criminal will be caught.107

Developing countries also differ in the patterns of cyber-crimes originated from these countries. More fully developed examples of cyber-crimes are found in Eastern European countries. Romanian and Ukrainian cyber-criminals have reportedly specialised in internet auction frauds and online credit card-related crimes.108 Observers have noted that Bulgarian and Chinese cyber-criminals have specialised in intellectual property (IP) theft.109 For instance, in 2005, a Trojan horse code named Myfip was reported to be sending data from the networks of US-based companies to an internet user in Tianjin, China. Myfip sent sensitive documents such as CAD/CAM files that stored mechanical designs, electronic circuit board schematics and layouts.110 In 2005 a Chinese intern working in Valeo was detained in France for alleged ‘illegal database intrusion’ aimed at IP theft.111

Cyber-crime business models in developing economies

While the developing world in general lags behind in the availability of IT skills, there are highly skilful organised crime groups in some developing countries. Organised crime groups are increasingly engaged in cyber-crime activities.112 Indeed, cyber-crime has been one of the most important revenue sectors for global organised crime groups.113 In many cases organised criminals also buy high-skilled coders as well as having a low-skilled IT workforce to engage in cyber-crimes.

To launder funds stolen through cyber-crime operations, organised crime groups often lure and recruit money mules. The mules help to move stolen money from one account to another. Most often they take the stolen funds into their own account before sending it as a wire transfer to the criminal groups.114 For instance, the victims of most Romanian cyber-criminals' auction fraud are in the US, Canada, UK, Spain and Italy. Romanian mules have been found picking up money in these countries. In 2006 US law enforcement agencies arrested an eBay fraud ring in Chicago, which was found to have connections with cyber-criminals in Pitesti, Romania.115

Cyber-criminals know that credit card transactions initiated from Eastern Europe and some developing countries have a low probability of success. In such cases they recruit money mules in countries where the credit card holder is located (eg the US). A US-based money mule then uses the stolen credit card to make a transaction in a US bank and then sends the money to the cyber-criminal. One estimate suggested that international cyber-crime groups had set up about 44 000 post office boxes and residential addresses in the US in 2004.116 US-based online retailers are cautious of shipping across borders. Cyber-crime groups, however, know that if an online transaction is approved, shipments inside the US are rarely scrutinised. They thus recruit US residents as mules, whose homes are used as shipment drop points.

Some mules are unaware that they are engaged in illegal activities and some become scam victims themselves.117 Consider the Nigerian check scam. In this type of scam, Nigerians send fake documents, which look like Wal-Mart money orders, Bank of America cheques, US Postal Service cheques or American Express travellers' cheques.118 They provide a mule with instructions on filling out the cheques and where they are to go. The mule cashes the cheques and sends most of the amount to Nigerian cyber-criminals. However, when the cheque is found to be a fake, the mule becomes responsible for the entire amount.

The location and number of money mules and functions they perform also vary across cyber-crimes. Some transactions involve money mules from a number of countries. In a case reported in Sullivan a cyber-crime victim, an online CD and DVD retailer, paid a ransom of $40 000 to a hacker based in Balakov, western Russia. The fund was wired to 10 different bank accounts in Riga, Latvia. The mules then wired the money to accounts in St Petersburg and Moscow. Another set of mules brought the money to Balakov. The computer server used by the Balakov-based hacker to launch the botnet attacks was in Houston.119

In an interesting pattern of international division of labour, in early 2008 a criminal group involved in botnet attacks set up offices in India to process applications that cannot be completed automatically.120 IT workers in India offered help to facilitate the signing up of free email accounts.

Motivations behind cyber-crimes

Crime rates are tightly linked to a lack of economic opportunities. A large number of cyber-attacks originate from Eastern Europe and Russia because there are a large number of students good at mathematics, physics and computing.121 Speaking of the social emphasis on mathematics skills among Romanians, a senior research scientist at the Institute of Mathematics in Bucharest put the issue this way: “The respect for math is inside every family, even simple families, who are very proud to say their children are good at mathematics”.122

Consistent with history and theory bot herders and other cyber-criminals tend to be from locations where high-paying legitimate IT jobs are unavailable.123 In industrialised countries, people with IT skills can usually find legitimate IT jobs. In many developing economies, IT job growth is lower than internet penetration growth.124 The primary reason why some people are attracted to cyber-crime in Eastern Europe and Russia is because of high unemployment and low wages. Organised crime groups in countries such as Russia, Romania and Brazil are thus tapping into the technical skills available in those countries to expand their operations.

The combination of over-educated and under-employed computer experts has made Russia and other Eastern European countries fertile ground for hackers. In these economies the growth rate of IT industries is far from enough to absorb the IT workforce.125 Beyond all that, a financial crash in Russia in 1998 left many computer programmers unemployed. In Russia top university graduates are paid up to 10 times as much as they would earn from legitimate IT jobs by organised criminals.126

A related point is that, notwithstanding India's huge IT talents, the country accounts for proportionately fewer cyber-crimes compared with other developing countries. For instance, according to Sophos researchers, the UK and India together contributed 1.3 per cent of the world's malware. While they could not separate malware originated from the UK and India, as both use British English, the UK is considered to account for more crimes than India.127 The primary reason behind India's low cyber-crime profile is the development of a legitimate IT industry in the country. Speaking of the low rate of cyber-crimes in the country, Nandkumar Saravade, director of cyber security for India's National Association of Software and Service Companies noted: ‘Today … any person in India with marketable computer skills has a few job offers in hand’.128

Concluding comments

This article has contributed to the conceptual and empirical understanding of the structure of cyber-crimes in the context of the developing world. The analyses have indicated that the nature of the source of a web attack is a function of the nature of institutional legitimacy to a cyber-criminal; to stocks of hacking skills relative to the availability of economic opportunities; and to potential victims' defence mechanisms. Table 4 presents the economic and institutional factors facing cyber-crime offenders and victims in a developing economy.

TABLE 4 IS OMITTED FROM THIS FORMATTED DOCUMENT

Anti-cyber-crime institutions are developing rapidly in industrialised economies because of exogenous shocks, pressure to change organisational logics and other forces of gradual change. In many developing economies, on the other hand, formal institutions are weak because these countries lack laws that recognise cyber-crime, they lack judges, lawyers and other law enforcement personnel who understand cyber-crime, and they lack resources to build institutions to combat it. Governments' measures to combat cyber-crime too often remain pure lip service. One reason for this is a lack of resources to build formal institutions to deal with cyber-crime.129 Equally problematic are institutions at industry and inter-organisational levels. Because of weak law enforcement machinery in developing countries, cyber-criminals in these countries are more confident than those in developed countries.

Cybercrimes may be more justifiable if informal institutions (or social and internalised norms) against them are weaker in a society. These conditions are more pervasive in economies, in which many internet users are connected to the internet for the first time.130 Moreover, the cyber-crime victimisation level is relatively low in these economies.

As noted earlier, most people involved in using computer networks unethically and illegally do not perceive their actions' ethical implications. Factors giving rise to such conditions are stronger in developing countries. This is because the internet is new for many users in developing countries. A related point is that many organisations and individuals are unaware of cyber-crimes. Cyber-crimes are more justifiable in developing countries than in developed countries. As pointed out by social identity theory,131 as more and more individuals and organisations become cyber-crime victims and thus belong to the in-group of cyber-crime victims, the perceived social stigma associated with a cyber-criminal may increase and that of becoming a cyber-crime victim may reduce. Based on the above discussion, the following proposition is presented.

Many internet users in developing economies are inexperienced and not technically savvy. Most organisations adopt these technologies without considering security and other related problems. Even if organisations are willing to secure their systems, because of the adverse international ‘hierarchical pattern’ for security products, these products are less likely to be available in these economies.

Thin and dysfunctional institutions and a lack of resources are among the biggest roadblocks for combating cyber-crime in developing countries. A lack of international co-operation and co-ordination is equally problematic in fighting cyber-crimes originating in developing countries.

Yet, notwithstanding the political, legal, cultural and economic barriers, some economies are making great leaps. Some developing countries are also modernising their crime-fighting efforts. For example, it was reported in 2006 that Kenya was in the advanced stages of assembling a cyber-crime laboratory, which could be used by the police in East Africa.132 In September 2009 Antigua opened a state-of-the-art cyber-forensics facility to serve the entire Caribbean region. Montserrat, Barbados, St Kitts & Nevis and Antigua and Barbuda will use the lab. The US provided over $500 000 to establish the lab and $200 000 to train the workforce.133

The Indian offshore industry provides a remarkable example of industry–government collaboration in combating cyber-crime. In particular, the National Association of Software and Services Companies (NASSCOM) has played an exemplary role in bringing institutional changes in cyber-crime-related institutions.134

We noted above that the growth of internet and broadband penetration in developing countries is likely to lead to a more rapid growth of cyber-crimes in these countries than in developed countries. Other economic factors related to cyber-crime, such as the availability of resources to fight it and of economic opportunities, are likely to change at slower rates. Institutions related to cyber-crime are even slower to change, especially informal institutions.

On the bright side developing world-based firms have also increased their investments in security. The security market in China increased by 24 per cent in 2006.135 Factors such as the 2008 Olympics in Beijing, the 2010 World Expo in Shanghai and a steady rise in broadband usage as a vehicle for online entertainment have boosted this growth.136 Small and medium businesses in Brazil spent $260 million on IT security solutions in 2007.137

The fact that cyber-crime has been catching international attention has been an important trigger for the strengthening of cyber-crime laws in some economies. For instance, the Philippine Republic Act 8792 was established as a result of the love bug virus attack. The act laid out how cyber-crimes in the country should be punished.138

Other developing countries are also taking measures against cyber-crime. In November 2006 Bangladesh hosted a cyber-crime seminar to exchange experiences on combating cyber-crime and foster future co-operation. Experts dealing with cyber-crime issues from Australia, Hong Kong, Sri Lanka and Nepal participated. The Australian Federal Police supported the seminar.139

It is also important to include developing economies in international level policy initiatives. In the first UN forum on internet governance some developing countries such as Iran and South

Africa complained that they had not been given an opportunity to adequately express their views on ethical issues and other concerns.140

Economic factors related to cyber-crimes such as hardware and software used, broadband connections, stock of cyber-crime skills, availability of economic opportunities and diffusion of security products are changing in developing economies. Institutions related to cyber-crimes, on the other hand, tend to be persistent,141 durable,142 and stable and hence are slower to change. Moreover, in most cases, compared to formal institutions, de-institutionalisation and re-institutionalisation of social practices, cultural values and beliefs occur very slowly.143 Informal institutions such as those related to the stigmatisation of a cyber-criminal and a cyber-crime victim are thus likely to change more slowly than formal institutions such as strength of rule of law.

Notes on contributor

Nir Kshetri is associate professor at the Bryan School of Business and Economics, University of North Carolina–Greensboro and visiting professor at Bad Mergentheim Business School, Baden-Württemberg. His recent publications are *The Global Cyber-Crime Industry: Economic, Institutional and Strategic Perspectives* (2010) and *The Rapidly Transforming Chinese High Technology Industry and Market: Institutions, Ingredients, Mechanisms and Modus Operandi* (2008).

Notes

1 RE Bell, ‘The prosecution of computer crime’, *Journal of Financial Crime*, 9(4), 2002, pp 308–325; ‘It may make life easier and cheaper: East Africa gets broadband’, *The Economist*, 391(8636), 2009, p 46; and I Ismail, ‘Understanding cybercriminals’, *New Straits Times* (Malaysia), 2008, p 12.

2 S Schafer, ‘A Piracy culture. Beijing continues to defy US and European efforts to stop IP theft', 16 January 2006,*Newsweek (International Edition)*, at http://www.msnbc.msn.com/id/10756810/site/newsweek/, accessed 1 October 2010.

3 V Menon, ‘Egypt identified as one of top Trojan creating countries’, *itp.net*, 29 January 2010, athttp://www.itp.net/579126-egypt-named-in-list-of-top-trojan-creating-countries, accessed 20 February 2010.

4 M Reilly, ‘Beware, botnets have your PC in their sights’, *New Scientist*, 196(2634), 2007, pp 22–23.

5 WJ Baumol, ‘Entrepreneurship: productive, unproductive, and destructive’, *Journal of Political Economy*, 98(5), 1990, pp 893–921.

6 *Ibid*, pp 893–921; DC North, *Institutions, Institutional Change and Economic Performance*, Cambridge, MA: Harvard University Press, 1990; and North, ‘Epilogue: economic performance through time’, in LJ Alston, T Eggertsson & DC North (eds), *Empirical Studies in Institutional Change*, Cambridge, PA: Cambridge University Press, 1996, pp 342–355.

7 P Holm, ‘The dynamics of institutionalization: transformation processes in Norwegian fisheries’, *Administrative Science Quarterly*, 40(3), 1995, pp 398–422.

8 ‘Wired for trouble’, *Hindustan Times*, 24 October 2009, at http://www.tmcnet.com/usubmit/2009/10/24/4442635.htm, accessed 29 October 2009.

9 MK Conti, ‘Firms warned vs cybercrimes’, *BusinessWorld*, S1/7, 2007.

10 M Harwood, ‘Quebec police break up hacking syndicate’, *Security Management*, 22 February 2008, athttp://www.securitymanagement.com/news/quebec-police-break-hacking-syndicate, accessed 28 October 2009.

11 Gordon & Ford, ‘On the definition and classification of cybercrime', *Journal in Computer Virology*, 2, 2006, pp 13–20.

12 Nigerian 419 fraud is named for a section of the Nigerian criminal code.

13 M Srivastava, ‘Pros of con: from credit card fraud to drug peddling and job scams, Nigerians seem to be everywhere in the crime business’, *India Today*, 14 September 2009, at http://indiatoday.intoday.in/index.php?option=com_magazine&opt=section&sectionid=36&issueid=127&Itemid=1, accessed 27 October 2009.

14 Reilly, ‘Beware, botnets have your PC in their sights’.

15 K Kinyanjui, ‘High speed internet exposes Kenya to cybercrime’, 2009, at http://www.businessdailyafrica.com/-/539444/638794/-/rx1rgv/-/, accessed 5 October 2009.

16 ‘South Africa: internet banking fraud on the increase’, *Africa News*, 24 October 2007; and ‘It may make life easier and cheaper’, p 46.

17 K Kinyanjui, ‘Watchdog warns of increased cybercrime threat’, 8 September 2009, athttp://www.businessdailyafrica.com/Company%20Industry/-/539550/654440/-/u765i9z/-/, accessed 5 October 2009.

18 M Kotadia, ‘Report: a third of spam spread by RAT-infested PCs’, *CNET News.com*, 3 December 2003, athttp://www.news.com/Report-A-third-of-spam-spread-by-RAT-infested-PCs/2100-7355_3-5113080.html, accessed 27 October 2005.

19 ‘China tops globe in robot PCs’, *Business Daily Update*, 28 September 2006.

20 I Chan, ‘China's disturbing broadband decline: a digital divide between saturated urban areas and underserved rural markets is behind the slowdown’, 26 July 2007, athttp://www.businessweek.com/globalbiz/content/jul2007/gb20070726_579284.htm?campaign_id=rss_as, accessed 27 October 2009.

21 ‘Telefonica takes the lead in Latin America’, *Screen Digest*, 2008, athttp://www.screendigest.com/press/releases/press_releases_22_00_2008/view.html, accessed 25 October 2009.

22 International Telecommunication Union (ITU), *World Information Society Report 2007*, athttp://www.itu.int/osg/spu/publications/worldinformationsociety/2007, accessed 27 October 2009.

23 GS Becker, ‘Crime and punishment: an economic approach’, *Journal of Political Economy*, 76, 1968, pp 169–217; I Ehrlich, ‘Participation in illegitimate activities: a theoretical and empirical investigation’, *Journal of Political Economy*, 81, 1973, pp 521–565; S Freeman, J Grogger & J Sonstelie, ‘The spatial concentration of crime’, *Journal of Urban Economics*, 40(2), 1996, pp 216–231; DL Sjoquist, ‘Property crime and economic behavior’, *American Economic Review*, 63, 1973, pp 439–446; and EC Viano, *Global Organized Crime and International Security*, Burlington, VT: Ashgate, 1999.

24 JH Mittelman & R Johnston, ‘The globalization of organized crime, the courtesan state, and the corruption of civil society’, *Global Governance*, 5(1), 1999, pp 103–126.

25 I Ehrlich, ‘Crime, punishment, and the market for offenses?’, *Journal of Economic Perspectives*, 10(1), 1996, pp 43–67.

26 Mittelman & Johnston, ‘The globalization of organized crime’; and R Vassilev, ‘De-development problems in Bulgaria’, *East European Quarterly*, 37(3), 2003, p 345.

27 O Mark, ‘ICT experts gear up for war against e-crime’, 2009, athttp://www.businessdailyafrica.com/Company%20Industry/-/539550/655032/-/u75jcqz/-/, accessed 5 October 2009.

28 Ismail, ‘Understanding cybercriminals’, p 12.

29 P Duggal, ‘What's wrong with our cyber laws?’, 2004, athttp://www.expresscomputeronline.com/20040705/newsanalysis01.shtml, accessed 28 October 2009.

30 V Aggarwal, ‘Cyber crime's rampant’, *Express Computer*, 2009, athttp://www.expresscomputeronline.com/20090803/market01.shtml, accessed 27 October 2009.

31 I Wylie, ‘Internet: Romania home base for eBay scammers—the auction website has dispatched its own cyber-sleuth to help police crack fraud rings’, *Los Angeles Times*, 26 December 2007, p C1.

32 J Ribeiro, ‘India's Nasscom calls for special cybercrimes court’, *Network World*, 7 September 2006, athttp://www.networkworld.com/news/2006/090706-indias-nasscom-calls-for-special.html, accessed 27 October 2007.

33 ‘Securing the web’, *Hindustan Times*, 22 October 2006.

34 S Deshpande, ‘New cyber law casts its net wide’, *Economic Times*, 28 October 2009, athttp://economictimes.indiatimes.com/infotech/internet/New-cyber-law-casts-its-net-wide-/articleshow/5170897.cms, accessed 29 October 2009.

35 S Darmosumarto, ‘Battle on internet credit card fraud still long’, *Jakarta Post*, 2003, at http://www.crime-research.org/news/2003/12/Mess0802.html, accessed 27 October 2005.

36 T Smith, ‘Technology: Brazil becomes a cybercrime lab’, 27 October 2003, athttp://query.nytimes.com/gst/fullpage.html?res=9F02E3DA1131F934A15753C1A9659C8B63&sec=&spon=&pagewanted=2, accessed 27 October 2005.

37 Wylie, ‘Romania home base for eBay scammers’.

38 A Shubert, ‘Taking a swipe at cyber card fraud’, *CNN.com*, 6 February 2003, athttp://www.cnn.com/2003/WORLD/asiapcf/southeast/02/06/indonesia.fraud, accessed 27 October 2005.

39 ‘Securing the web’.

40 Ribeiro, ‘India's Nasscom calls for special cybercrimes court’.

41 Aggarwal, ‘Cyber crime's rampant’.

42 B McGeer, ‘Security: bankers fight a new battle IT adjustments, purchases part of Patriot Act’, *Bank Technology News*, 15(11), 2002, p 1.

43 ‘South Africa: internet banking fraud on the increase’.

44 F Syed & L D'monte, ‘India lags in cybercrime insurance’, 7 April 2008, athttp://www.rediff.com/money/2008/apr/07cyber.htm, accessed 27 October 2009.

45 M Cuéllar, ‘The mismatch between state power and state capacity in transnational law enforcement’, *Berkeley Journal of International Law*, 22(1), 2004, pp 15–58.

46 Wylie, ‘Romania home base for eBay scammers’.

47 ITU, 'ITU Regional Cybersecurity Forum 2008 Lusaka, Zambia, Meeting Report: ITU Regional Cybersecurity Forum for Eastern and Southern Africa, Lusaka, Zambia', 25–28 August 2008, 29 August 2008, at http://www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-report-aug-08.pdf, accessed 5 October 2009.

48 'Cell phone crime rise: extortions go on unabated', *The New Nation* (internet edition), 5 October 2009, athttp://nation.ittefaq.com/issues/2009/10/05/news0827.htm, accessed 5 October 2009.

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

50 P Warren, 'Hunt for Russia's web criminals: the Russian business network—which some blame for 60% of all internet crime—appears to have gone to ground', *Guardian*, 15 November 2007, athttp://www.guardian.co.uk/technology/2007/nov/15/news.crime, accessed 5 October 2009.

51 N Vardi, 'Chinese take out', *Forbes*, 25 July 2005, p 54.

52 DM Kahan, 'What do alternative sanctions mean?', *63 University of Chicago Law Review*, 591, 1996, pp 603–604.

53 VT Hu, 'Nondiscrimination or secular orthodoxy? Religious freedom and breach of contract at Tufts University',*Texas Review of Law & Politics*, 6(1), 2001, pp 289–333; and R Shilts, 'The queering of America', *The Advocate*, 1 January 1991.

54 R Duncan, 'Who wants to stop the church? Homosexual rights, legislation, public policy, and religious freedom',*Notre Dame Law Review*, 69, 1994, p 393.

55 EA Kallman & JP Grillo, *Ethical Decision Making and Information Technology*, New York: McGraw Hill, 1996; and S Phukan, 'IT ethics in the internet age: new dimensions', *InSITE*, June 2002, athttp://proceedings.informingscience.org/IS2002Proceedings/papers/phuka037iteth.pd, accessed 27 October 2005.

56 'China's zombie PCs', *redherring.com*, 5 April 2005, at http://www.redherring.com/Home/11708, accessed 27 October 2006.

57 'Terrorist attacks mean bid e-security spending', *Europemedia*, 13 June 2002, p 1.

58 'SMBs in Brazil to spend $260USM on IT security in 2007: up to 72% of Brazil-based MBs cited enhanced data security and privacy as key factors influencing IT purchases, AMI Partners study finds', *Business Wire*, 20 November 2006.

59 Kinyanjui, 'Watchdog warns of increased cybercrime threat'.

60 C Otis & P Evans, 'The internet and Asia-Pacific security: old conflicts and new behavior', *Pacific Review*, 16(4), 2003, pp 549–550.

61 *Ibid*.

62 *Ibid*.

63 L Denardis, 'Internet standards and developing countries: problems and opportunities', Giganet Second Annual Symposium, Rio De Janeiro, 11 November 2007, at http://www.igloo.org/community.igloo?r0=community-download&r0_script=/scripts/document/download.script&r0_pathinfo=%2F%7B58dacb33-31ea-4219-9124-89a75ffe71d0%7D%2FPublic%20Library%2Fpapers~1%2Fdenardis&r0_output=xml, accessed 27 October 2009.

64 HK Nordas, 'South African manufacturing industries—catching up or falling behind?', *Journal of Development Studies*, 32(5), 1996, pp 715–733.

65 'No fuss printing basics assist third world trade', *Dairy Industries International*, 63(2), 1998, p 48.

66 JY Kim, 'Toward a Golden Age', *Harvard International Review*, 29(2), 2007, pp 20–25.

67 M Jordan & J Karp, 'Machines for the masses: Whirlpool aims cheap washer at Brazil, India and China—making due with slower spin', *Wall Street Journal*, 9 December 2003, p A19.

68 R Naraine, 'Money bots: hackers cash in—research group details how lucrative PC hijacking can be', *eWeek*, 18 September 2008, p 27.

69 'SA kids benefit from One Laptop Per Child campaign', *South Africa: The Good News*, 8 April 2008, athttp://www.sagoodnews.co.za/education/sa_kids_benefit_from_one_laptop_per_child_campaign_.html, accessed 27 October 2008.

70 Reilly, 'Beware, botnets have your PC in their sights'.

71 RL Brandt, 'Ivan Krstic, 21', *Technology Review*, 110(5), 2007, pp 54–55.

72 Reilly, 'Beware, botnets have your PC in their sights'.

73 sophos.com, 'Police crack suspected online extortion ring', Sophos reports, 23 July 2008, athttp://www.sophos.com/virusinfo/articles/extortion.html, accessed 27 October 2009.

74 D Clark, 'PC makers race to market with low-cost "netbooks"', *Wall Street Journal* (Eastern edition), 8 April 2008, B1.

75 ‘Intel adds new features to low-cost laptops, *thestate.com*, 15 April 2008, athttp://www.thestate.com/business/story/376162.html, accessed 27 October 2009.

76 Reilly, ‘Beware, botnets have your PC in their sights’.

77 ‘China's zombie PCs’.

78 H Gatignon & TS Robertson, ‘A propositional inventory for new diffusion research’, *Journal of Consumer Research*, 11, 2005, pp 849–867.

79 ‘Challenges in the East’, *Information Today*, 25(2), 2008, p 22.

80 ‘China's zombie PCs’.

81 L Brown, E Malecki & A Spector, ‘Adopter categories in a spatial context: alternative explanations for an empirical regularity’, *Rural Sociology*, 41, 1976, pp 99–118.

82 Gatignon & Robertson, ‘A propositional inventory for new diffusion research’, p 858.

83 ‘Challenges in the East’.

84 J Deutsch, S Hakim & J Weinblatt, ‘Interjurisdictional criminal mobility: a theoretical perspective’, *Urban Studies*, 21, 1984, pp 451–458.

85 Freeman *et al*, ‘The spatial concentration of crime’; and D Weisburd, S Bushway, C Lum & SM Yang, ‘Trajectories of crime at places: a longitudinal study of street segments in the city of Seattle’, *Criminology*, 42(2), 2004, pp 283–320.

86 M Lianos & M Douglas, ‘Dangerization and the end of deviance’, *British Journal of Criminology*, 40(2), 2000, pp 261–278.

87 CR Browning, SL Feinberg & RD Dietz, ‘The paradox of social organization: networks, collective efficacy, and violent crime in urban neighborhoods’, *Social Forces*, 83(2), 2004, pp 503–534; and WJ Wilson, *The Truly Disadvantaged*, Chicago, IL: University of Chicago Press, 1987.

88 PJ Van Koppen & RW Jansen, ‘The road to the robbery: travel patterns in commercial robberies’, *British Journal of Criminology*, 38(2), 1998, pp 230–246.

89 N Kshetri, ‘The evolution of the Chinese online gaming industry’, *Journal of Technology Management in China*, 4(2), 2009, pp 158–179.

90 A Greenberg, ‘The top countries for cybercrime’, *Forbes.com*, 17 July 2007, athttp://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html, accessed 9 April 2008.

91 C Fong, ‘Fighting the agents of organized cybercrime’, 8 May 2008, athttp://www.cnn.com/2008/TECH/05/08/digitalbiz.cybercrime, accessed 27 October 2009.

92 Greenberg, ‘The top countries for cyber crime’; and D Miller, ‘Commentary: the embeddedness of corporate strategy: isomorphism vs differentiation’, *Advances in Strategic Management*, 13, 1996, pp 283–291.

93 ITU, *World Information Society Report 2007*.

94 ‘New McAfee research shows regionalized malware rising, more attacks tailored to different cultures and technologies’, *PR Newswire*, 21 February 2008.

95 *Ibid*.

96 ‘Securing the web’.

97 BR Mishra, ‘Wipro unlikely to take fraud accused to court’, *business-standard.com*, 19 February 2010, athttp://www.business-standard.com/india/news/wipro-unlikely-to-take-fraud-accused-to-court/386181/, accessed 1 March 2008.

98 ‘Outsourcing crime. Call centre expose can wreak havoc’, *tribuneindia.com*, 25 June 2005, athttp://www.tribuneindia.com/2005/20050625/edit.htm, accessed 27 October 2006; and ‘Securing the web’.

99 KD Schwartz, ‘The background-check challenge’, *InformationWeek*, 18 July 2005, pp 59–61; and G Fest, ‘Offshoring: Feds take fresh look at India BPOs—major theft has raised more than a few eyebrows’, *Bank Technology News*, 18(9), 2005, p 1.

100 Aggarwal, ‘Cyber crime's rampant’.

101 ‘China gets its game on’, *China Daily*, 5 May 2008’, at http://www.chinadaily.com.cn/bizchina/2008-05/05/content_6661519.htm, accessed 2 October 2008.

102 D Nystedt, ‘Online gaming growing fast in China, study says’, 2004, athttp://archive.thestandard.com/movabletype/datadigest/archives/003210.php, accessed 27 October 2005.

103 ‘New McAfee research shows regionalized malware rising’.

104 N Kshetri & N Dholakia, ‘Determinants of the global diffusion of B2B E-commerce’, *Electronic Markets*, 12(2), 2002, pp 120–129.

105 ‘Indian IT revenue grows 10-fold in decade’, *Indo-Asian News Service*, NASSCOM, 23 January 2007.

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

107 Freeman *et al*, ‘The spatial concentration of crime’.

108 Wylie, ‘Romania home base for eBay scammers’.

109 Vardi, ‘Chinese take out’.

110 *Ibid*.

111 T Luard, ‘China's spies come out from the cold’, 22 July 2005, at http://news.bbc.co.uk/2/hi/asia-pacific/4704691.stm, accessed 27 October 2007.

112 A Hawser, ‘Banks on the spot over internet fraud’, *Global Finance*, 21(8), 2007, p 8; and M Giannangeli, ‘Are we ready for Russian mafia's crime revolution?’, *Sunday Express* (Scottish edition), 8 June 2008, p 4.

113 ‘Frost & Sullivan: correction—cybercrime drives growth and increased competition in the global anti-malware market’, *M2 Presswire*, 13 July 2007.

114 B Sullivan, ‘Who's behind criminal bot networks?’, 10 April 2007, athttp://redtape.msnbc.com/2007/04/whos_behind_cri.html, accessed 27 October 2009.

115 Wylie, ‘Romania home base for eBay scammers’.

116 B Acohido & J Swartz, ‘Cybercrooks lure citizens into international crime’, *USA Today*, 2005, athttp://www.usatoday.com/tech/news/2005-07-10-cyber-mules-cover_x.htm, accessed 5 October 2009.

117 T Claburn, ‘The cybercrime economy’, 2008, athttp://www.informationweek.com/blog/main/archives/2008/04/the_cyber_crime.html, accessed 7 October 2008.

118 N Gohring, ‘Woman gets two years for aiding Nigerian internet check scam’, *PC World*, 25 June 2008, athttp://www.pcworld.com/businesscenter/article/147575/woman_gets_two_years_for_aiding_nigerian_internet_check_scam.html, accessed 27 October 2009.

119 Sullivan, ‘Who's behind criminal bot networks?’.

120 S Arnott, ‘Cyber crime stays one step ahead’, *Independent*, 2008, athttp://www.independent.co.uk/news/business/analysis-and-features/cyber-crime-stays-one-step-ahead-799395.html, accessed 27 October 2009.

121 J Blau, ‘Viruses: from Russia, with love?’, *IDG News Service*, 2004, athttp://www.pcworld.com/news/article/0,aid,116304,00.asp, accessed 27 October 2005.

122 Wylie, ‘Romania home base for eBay scammers’.

123 Sullivan, ‘Who's behind criminal bot networks?’.

124 H Sulaiman, ‘Quest to fight cybercrime’, *New Straits Times*, 15 October 2007, p 13.

125 Blau, ‘Viruses’.

126 Warren, ‘Hunt for Russia's web criminals’.

127 Greenberg, ‘The top countries for cybercrime’.

128 *Ibid*.

129 Cuéllar, ‘The mismatch between state power and state capacity in transnational law enforcement’.

130 ‘China's zombie PCs’.

131 KM Hamner, ‘Gay-bashing: a social identity analysis of violence against lesbians and gay men’, in GM Herek & K Berrill (eds), *Hate Crimes: Confronting Violence against Lesbians and Gay Men*, Newbury Park, CA: Sage, 1992, pp 179–190; and H Tajfel & JC Turner, ‘The social identity theory of intergroup behavior’, in S Worchel & WG Austin (eds),*Psychology of Intergroup Relations*, Chicago, IL: Nelson-Hall, 1986, pp 7–24.

132 K Kornakov, ‘Police forces in East Africa will have a new hi-tech lab’, 8 September 2006, athttp://www.viruslist.com/en/viruses/news?id=197753850, accessed 27 October 2007.

133 ‘Regional cyber lab opens in Antigua’, *caribbean360.com*, 28 September 2009, athttp://www.caribbean360.com/News/Caribbean/Stories/2009/09/28/NEWS0000008964.html, accessed 27 October 2009.

134 N Kshetri & N Dholakia, ‘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), 2009, pp 225–239.

135 C Hope, ‘UK security threat from cyber crime’, *Daily Telegraph*, 20 March 2008, athttp://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/03/19/nterror319.xml, accessed 27 October 2008.

136 *Ibid*.

137 ‘SMBs in Brazil to spend $260USM on IT security in 2007’.

138 J Evans, ‘Cyber-crime laws emerge, but slowly’, 2000, athttp://archives.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg, accessed 27 October 2005.

139 ‘Cybercrime cost is a burden on developing countries: Bangladesh’, *Asia Pulse*, 6 November 2007.

140 RTE, ‘Global forum on web bridges “cultural gap”’, *RTE Commercial Enterprises*, 2 November 2006, athttp://www.rte.ie/business/2006/1102/internet.html, accessed 1 October 2009.

141 S Parto, ‘Economic activity and institutions: taking stock’, *Journal of Economic Issues*, 39(1), 2005, pp 21–52.

142 GM Hodgson, ‘The hidden persuaders: institutions and individuals in economic theory’, *Cambridge Journal of Economics*, 27, 2003, pp 159–175.

143 E Clark & A Soulsby, *Organisational Change in Post-Communist Europe*, London: Routledge, 1999; G Ibrahim & V Galt, ‘Bye-bye central planning, hello market hiccups: institutional transition in Romania’, *Cambridge Journal of Economics*, 26(1), 2002, p 105; North, *Institutions, Institutional Change and Economic Performance*; and J Zweynert & N Goldschmidt, ‘The two transitions in Central and Eastern Europe as processes of institutional transplantation’, *Journal of Economic Issues*, 40(4), 2006, pp 895–918.