Cybersecurity and Development

By: Nir Kshetri

Kshetri, Nir (2016) "Cybersecurity and Development," *Markets, Globalization & Development Review*, 1(2), Article 3: http://digitalcommons.uri.edu/mgdr/vol1/iss2/3

Made available courtesy of DigitalCommons@URI: http://dx.doi.org/10.23860/MGDR-2016-01-02-03

Abstract:

While scholars and policymakers have realized the importance of information and communication technologies in economic development, relatively less attention has been given to the role of cybersecurity. This research sheds light on issues associated with the "dark side" of digitization in the Global South. We examine the hollowness in the Global South's digitization initiatives that is associated with a poor cybersecurity. The article also advances our understanding of how institutional and structural characteristics of the Global South influence cybersecurity.

Keywords: cyber-control | cybercrime | cybersecurity | development | hollowness | institutional bottlenecks | "slowmoving" and "fast moving" institutions | Global South

Article:

Introduction

While the rapid growth in Internet penetration has a potential to contribute to economic and social development of the Global South (hereinafter: GS), analysts are concerned about the dark side of this rapid digitization. The spread of the Internet's penetration to more and more people in the GS has the potential to fundamentally alter the global cybercrime and cybersecurity landscapes. Referring to the emerging nature of the new threats with the entry into the cyberworld of yet unconnected population in the GS, Victoria Baines, Europol's Strategic Advisor on Cybercrime noted: "With two-thirds of the world yet to join the Internet, we can expect to see new criminals, new victims and new kinds of threats" (icspa.org 2012). Gady (2010) has put it most strongly in his argument that Africa's "Cyber [weapon of mass destruction] WMD" potentially poses a direct threat to the world. This analogy is especially relevant for many GS countries such as those in Africa, which have a large proportion of

unprotected computers. For instance, in 2010, 80% PCs used in Africa were infected with viruses and malware (Gady 2010). Cybercriminals often use these unprotected computers to launch cyberattacks against targets all over the world. Unsurprisingly some GS countries are top cyber-crime sources. According to Kaspersky Labs, in 2009 seven of the top 10 countries for creating trojans designed to steal passwords were GS countries, which accounted for 92% of such trojans globally (Kshetri 2010b).

Some of the key economic and social characteristics of the GS include low level of human development index, high unemployment rate, high degree of income inequality, low level of education, and weak democratic institutions (UNDP 2006). These characteristics have important implications and consequences for cybersecurity (Kshetri 2013a, c, 2016a). The objective of this paper is to provide insights into the dark side of digitalization associated with the GS.

Rapidly escalating cybercrime is one of the most pressing global challenges shared by both the Global North and GS (Nye 2011). In terms of the roles in facilitating illicit transnational economic activities, Andreas (2011) describes the Internet as "simply the latest—and not necessarily the most important—chapter in an old story". Many analysts, however, have suggested that the Internet has potentially dramatic consequences in terms of stimulating illicit cross-border activities that are unmatched by any other previous technologies (See Kshetri 2013a for review). There are a number of considerations that merit special attention in cybercrime and cybersecurity issues associated with the GS. Since most of the global demand for digital technologies is likely to be from the GS in the near future, cybercrimes in these countries deserve special attention (Kshetri 2013a). Analysing the trend of cybercrimes across countries, analysts have suggested 10–15% Internet penetration as the threshold level for the generation of significant hacking activities (Reilly 2007). Internet penetrations in many GS economies have reached this level. From our perspective, the most important aspect of the global cybercrime industry is that the highest incidences of cybercrime as well as growth rates have been reported in some of the economies of the GS. For instance, among the 12 countries that experienced the highest increases in their share of cyberattacks during 2005–2009, 11 were from the GS: Romania (1,501%), Colombia (749%), Indonesia (675%), Thailand (570%), Bangladesh (416%), Iran (370%), Zimbabwe (361%), Saudi Arabia (237%), Nigeria (214%), Vietnam (193%) and Kenya (161%) (Kim et al. 2012).

The GS not only accounts for the origination of a significant proportion of the most high-profile cybercrimes, but has also been a target of some of the most sophisticated cyberattacks. A case in point is the Stuxnet worm discussed above, which appeared in the second half (H2) of 2010 and crashed industrial control computers in a number of GS economies. A highly visible and unambiguous target was the Iranian nuclear programme. Nonetheless, the worm also disrupted the operations of industrial control computers in plants in China, India and Indonesia (Fildes 2010).

There are also reports that traditional organized crime groups in the GS have been involved in cybercrime. For instance, Chinese gangs, Colombian cartels and Russian and Malaysian organized crime groups have reportedly employed hackers, diverted their efforts from traditional activities to cybercrime and expanded their businesses globally (Kshetri 2010b).

Finally, due to cybersecurity related concerns, GS-based firms have faced barriers to international trade and investment in a broad range of countries. For instance, Australian, Indian, and the U.S. governments have accused the Chinese company, Huawei Technologies of cyberespionage, which hindered the company's internationalization (Kshetri 2016b).

The above observations suggest that cybersecurity-related issues are rapidly emerging in the GS, which have important economic, social and political implications. Nonetheless, in little research have scholars directly considered factors associated with cybersecurity in the developing world. In order to contribute to filling this gap, this research seeks to explain how structural and institutional forces influence cybersecurity in the GS.

Before proceeding, some clarifying definitions are offered. For the purpose of this article, the United Nations Development Program's (UNDP) Human Development Index (HDI) is used to classify economies into the Global South and the Global North. More specifically, in the 2009 UNDP Human Development Report, the "South" is used to refer to economies that had a HDI of less than 0.9 (Bakewell 2009). Institutions are "macro-level rules of the game" (North 1990, p. 27), which include: a) formal institutions such as rules, laws, constitutions; and b) informal institutions such as social norms, conventions and self-imposed codes (North 1996). A cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations (Kshetri 2009). The International Telecommunications Union's (ITU's) definition of cybersecurity is followed: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment" (ITU, U.D.)

The paper is structured as follows. The article proceeds by first examining the hollowness in the Global South's digitization initiatives. Next, institutions related to cybersecurity in the Global South are analyzed. Then, institutional bottlenecks that affect cybersecurity in the Global South are examined. It is followed by a section on discussion and implications. The final section provides concluding comments.

Hollowness in the Global South's digitization initiatives

The concept of "hollow diffusion" of Internet and e-commerce technologies among firms in GS economies may help understand weak defense mechanisms (Otis and Evans 2003, p. 49). The basic idea behind "hollow diffusion" is simple: Many organizations digitizing their activities lack organizational, technological and human resources, and other fundamental ingredients needed to secure their system, which is the key for the long-term success of online businesses. To take an example is the Central Bank of Nigeria's (CBN) cashless policy planned in January 2012. Stakeholders expressed concerns related to broadband infrastructure, tested and accredited application software, trust economy, legislation, human skill capacities, call centre backbone,

consumers' profile data, data protection as well as credible regulations security (allafrica.com 2011). In short, the failure on the cybersecurity front hinders their ability to utilize the Internet productively. According to the online review site, Ecommerce Platforms, showing that the website is "secure and trustworthy" is the key to creating a successful online business (Zorzini 2016).

"Hollow diffusion" can take place in human (lack of skill and experience) and technological terms (failure to use security products). It is argued that organizations that adopt Internet technologies without considering the costs and efforts needed to maintain those systems generate a negative externality (Kshetri 2010b, d, 2013). Note that the presence of negative externalities means that the failure of firms to secure their systems have high social costs. In order to illustrate this point one can take an example of Overture South Korea's "continental cut-off" services, which according to a chosun.com article, disregard clicks originated from Africa (Kshetri 2010a). In general, some ISPs in the industrialized world block contents originated from problematic networks based in Africa (Garfinkel 2002). In an attempt to fight click frauds, advertisers and pay per click (PPC) search engines activate geo-targeting and monitor traffic originated from unusual geographical locations that associated with cybercrime activities. Note that many clicks are generated by robots which use infected computers in Africa and other parts of the world. To take another example, annual surveys by *CyberSource* conducted among North American merchants and released in 2006 and 2008 indicated that Nigeria and Ghana were perceived as the world's riskiest countries for online transactions. A high proportion of online orders originated from these countries were rejected by North American merchants (Dogbevi 2009).

While the hollowness can involve many dimensions, and has different implications for different entities, it can be understood, from our perspective, in terms of the lack of defense mechanisms at various levels. That is, hollowness is related to the lack of capacity to manage risks and vulnerabilities. Three dimensional of hollowness can be identified that lead to a low degree of cybersecurity orientation: technological, human and organizational structure.

Technological dimension of hollowness

In most GS economies there has been a lack of indigenous technology and patents related to cybersecurity (Kshetri 2016a). A related point is that while GS economies have generated some innovations, they have failed to give sufficient attention to security problems. At the same time while there has been a steep decline in the prices of most information and communication technology (ICT) products, anti-virus products are unaffordable for most consumers. For instance, 60% of Kenyan banks were reported to have insecure systems in 2009 (Kinyanjui 2009). Cybercriminals are taking advantage of the hollowness by targeting unprotected devices and luring unsuspecting customers to fake sites.

Human dimension of hollowness

GS economies are facing a shortage of CS professionals. For instance, consider the government of India (GoI). 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 (Hettigei 2005). An estimate suggested that in 2013, India had only 60 auditors (Doval 2013). 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. Likewise, in 2011, India's 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. The country is finding it difficult to enforce the RBI guidelines due to the lack of IT security auditors to validate banks' cybersecurity practices (Bradbury 2013).

Organizational structure-related dimension of hollowness

Organizational structure involves formally allocating various work roles into distinct tasks as well as associated administrative mechanisms in order to control, govern coordinate and integrate work activities (Child 1972; Mintzberg 1993). Such activities may also cross formal organizational boundaries. On the cybersecurity, one key global trend in organizational structure involves the tendency to create the position of Chief Information Security Officer (CISO). For instance, a 2014 PwC survey found that only 28% of over 500 companies surveyed had a CISO or Chief Security Officer (Damouni 2014). CEOs and board often consult CISOs to understand cyber risk, implement appropriate security controls and promote a culture of defense. One study suggested that 90% of CISOs are connected directly to their organizations' top leadership team, and half of them were on the leadership team (Sweeney 2016). Most GS-based organizations have not yet adopted such a structure. For instance, in India, except for few firms in banking, financial services and insurance, telecom, and business process outsourcing (BPO) it is rare to have a CISO in organizations (Pandya 2009).

Institutions affecting cybersecurity in the Global South

It can be argued that like any other economic phenomenon (Parto 2005), cybersecurity has institutional components and implications. Building on the work of Roland (2004), de Laiglesia (2006) classifies all 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. Such an understanding is important because some of the institutional factors can be more easily changed than others. For instance, laws and rules related to cybersecurity can be easily written on the books in a short period of time. Nonetheless, the development of legal infrastructures such as building a well-functioning cybersecurity-related court system and employing judges and law enforcement professionals well versed in cybersecurity takes a relatively longer time (Kshetri 2016a). Mohammad Khairuddin Abdullah, Malaysia's HeiTech Padu Berhad's director noted: "As long as they [cyber-criminals] are within the country, the criminals can be brought to court, but you'll be lucky if you can find the judge, who can write the warrant and understands the issue. Even though cyberlaws are in place, you need to have people who are able to apply the laws, as most cybercrime cases will get cold in just 24 hours" (Ismail 2008). Likewise, eBay's

Albena Spasova, who worked in promoting law reform in Moldova and Bulgaria noted: “Even in 2001, I was meeting judges who thought cybercrime was someone stealing a computer” (Wylie 2007). There has also been the lack of sufficient law enforcement personnel to fight cybercrimes. For instance, following raids on cyber cafés in major cities in Nigeria, cybercriminals were reported to move to remote areas to carry out their operations (Daily Trust 2010). The porous national borders and a lack of states’ controls on their territories allow cybercriminals to migrate to jurisdictions with a weaker rule of law (Mazzitelli 2007). There are some statistics to show porous national borders’ contribution to inter-jurisdictional arbitrage in West Africa. In 2008, 40% of arrested cybercrime suspects in Ghana were Nigerians, 38% were Ghanaians and the rest were from Liberia, Cote d’Ivoire and Togo (Boateng et al. 2010). A Barrister of Nigeria’s EFCC noted that anticybercrime measures in the country forced cybercriminals to other countries (tmcnet.com 2010).

Culture and social norms

It may be even more challenging to change culture and social norms that may affect cybersecurity. For instance, most GS economies lack domestic anti-virus companies. While top security software firms are based in industrialized economies, businesses and consumers in GS economies, mainly because of nationalism, prefer to buy domestically manufactured software (Kshetri 2010c).

In order to further illustrate this point, consider firms in the Indian offshoring industry. In an attempt to address their clients’ fear that customer data will be stolen and even sold to criminals, Indian firms engaged in outsourcing have taken measures to prevent attacks on computers by current and former employees. For instance, call center employees have to undergo security checks, which are considered to be “undignified”. Firms have established biometric authentication controls for workers and banned cell phones, pens, paper, and Internet/e-mail access for employees. Computer terminals at Mphasis, an Indian outsourcing firm, lack hard drives, e-mail, CD-ROM drives, or other ways to store, copy, or forward data. The idea here is that while employees may be willing to accept security checks that are considered to be undignified to get high-paying jobs in the offshoring sector, average Indian organizations may not consider implementing such checks that go against the established societal norms.

Conflicting sets of rules of behavior

In some cases, institutional changes are characterized by conflicting sets of rules of behavior, which may lead to the collapse of some of the institutional arrangements (de Laiglesia 2006). For instance, in some authoritarian regimes, cybersecurity measures mainly focus on cybercontrol activities. For instance, it was reported that the governments of Mauritania hired botnet operators to attack their critics’ websites with denial-of-service attacks (Cetron and Davies 2009). Likewise, Chinese government agencies allegedly sent viruses to attack websites that were banned (Guillén and Suárez 2005). Thus for authoritarian governments such as those of China, the goals of strengthening national cybersecurity and maintain control over the society with cyber-control measures are in conflict, and approaching one means to move away from the others. The above point can be further illustrated by focusing on China’s state strategies with regard to ICTs, which seek to balance economic modernization and political control. Stated

simply, this strategy broadly corresponds to China's unique approach and perspective to cybersecurity, and is reflected in the various cyber-control measures.

It is fair to say that China's extensive cyber-control measures are supported by institutional arrangements in the country, which weaken organizations' and citizens' cybersecurity initiatives. For instance, one result of China's weak civil society and strong state is that trade and professional associations are likely to engage in activities that are likely to promote the Chinese Communist Party's (CCP) authoritarian agenda, despite the conflict of such actions with the productive utilization of the Internet. For instance, the Internet Society of China (ISC) announced that it would help strengthen cyber-security orientation of users and Internet companies. If the past actions of the ISC are any indicator, however, its activities are more likely to be prompted by the CCP's need to maintain the dominance. For instance, in 2001, the ISC asked Internet companies to sign a voluntary pledge, which required the signatories not to disseminate information "that might threaten state security or social stability" (Kshetri 2007). In 2009, China's dominant search engine, Baidu, and 19 other Internet companies received the "China Internet Self-Discipline Award". ISC Officials praised them for their roles in fostering, and supporting "harmonious and healthy Internet development" (Kshetri 2013d).

While the Chinese government's cyber-control measures have been relatively successful, it has encountered a host of problems and difficulties to achieve its goals. Unsurprisingly these measures have also faced opposition and suffered setbacks as illustrated in the examples below (Kshetri 2013b).

Consider the Green Dam Youth Escort firewall software program launched in 2008. The Chinese government had announced a plan to make it mandatory to have the Green Dam installed on all new PCs in the country. The stated goal of the mandate was to protect children from violent and pornographic contents. The first problem the Green Dam faced was that while addressing one cybersecurity issue, it created side effects that raised another. For instance, while it successfully blocked politically sensitive contents, many viewed that the software would represent significant risks to users as a single flaw in the Green Dam system would expose the entire Chinese population to cybercriminals. For instance, a hacker able to attack the Green Dam system could have access to the information of all users who had installed the system.

A second problem stemmed from the fact that it increased PC manufacturers' costs, which led to an additional financial burden on consumers. While the Green Dam would be free to users, manufacturers needed to pay license fees to the Ministry of Industry and Information Technology (MIIT) to install the software (Kshetri 2013b).

A third related problem had to do with strong opposition from computer manufacturers and the public. They opposed because the proposed measures lead to increased costs of PC. For example, Lenovo, which is 57% government-owned, and Internet users, who are increasingly acting on a bottom-up approach, participated in collective resistance efforts to abort the Green Dam. Given the national security and economic risks and a strong resistance, the Green Dam program was indefinitely delayed after being installed in 20 million PCs. The unsustainable business model led to the closure of BDLKPRC in the 2010 and the company was near bankruptcy (Kshetri 2013b).

Another example is a 2011 regulation, which required microbloggers to register using their real name. The regulation was introduced so that law enforcement agencies would know the real user's identity in anything objectionable to the Chinese Communist Party was posted. The Nasdaq-listed Chinese online media company, Sina, warned that such a requirement would negatively influence user activity and threaten its popular microblogging service, Sina Weibo. Even after the March 16, 2012 deadline, Sina Weibo continued to allow users, who had not registered their real names to post and use its services (Kshetri 2013b).

Lessons from the above example

What lesson can be learned from the above examples? First, the regulatory infrastructures have not kept pace with the rapid rise in cybercrimes in the GS economies. Second, some of the social and cultural norms are not conducive to cybersecurity. Third, in the case of some GS economies (e.g., China), the diversion of resources to cyber-control has led to only limited progress on the cybersecurity front. There are, however, clear pressures that are likely to promote changes in cybersecurity-friendly institutions. Prior research has suggested that institutional changes can be seen as an outcome of the dynamic interactions of contradictions. Seo and Creed (2002) have proposed four sources of contradictions and "praxis": "(1) legitimacy that undermines functional inefficiency, (2) adaptation that undermines adaptability, (3) intra-institutional conformity that creates inter-institutional incompatibilities, and (4) isomorphism that conflict with divergent interests". Regarding (1), if policy makers see clear economic benefits of cybersecurity (functional/economic efficiency of cybersecurity), they are likely to lead efforts to change relevant regulations. For instance, the Chinese government gave up the requirement to install Green Dam due to economic reasons. Note that China's state strategies toward ICTs have been to balance economic modernization and political control (Kalathil 2003). Likewise, in order to secure high - paying jobs that the Indian outsourcing sector offers (functional/economic efficiency of cybersecurity), workers in the industry are willing to act against their social norms and undergo security checks, which are perceived as undignified.

Institutional bottlenecks and cybersecurity in the Global South

The impacts of "slow-moving" and "fast moving" institutions on cybersecurity can be better explained with the concept of institutional bottlenecks. The idea here is that various institutional factors in the GS are likely to result in bottlenecks and congestions that impede the efforts to fight cybercrimes.

Some elements of "fast-moving" institutions, such as corruption, lack of accountability and weak law enforcement may create bottlenecks for development. In this regard, Indian firms have generally expressed dissatisfaction and frustration with irresponsible and unaccountable law enforcement agencies. For instance, while most BPOs in Gurgaon had been cybercrime victims about 70% of the respondents did not report to the police (indiatimes.com 2011). Most organizations reported doubt about competence, professionalism and integrity of the police in handling cybercrime cases. About 50% of the respondents not reporting thought that the cases were not dealt with professionally and 30% noted that they had "no faith" in Gurgaon police (indiatimes.com 2011).

Institutional bottlenecks and technology-related issues

In a framework proposed by de Laiglesia (2006) for the analysis of institutional bottlenecks in GS, technology-related issues and factors are present at three levels of the framework*:* technological progress and dissemination (institutional outcomes), technology opportunity set (interaction and decision area), technology use, adoption and development (intermediate outcomes). This section analyzes how these elements may affect cybersecurity.

Concerning the technological progress and dissemination, some GS economies' wrong-headed focus on cyber-control as a component of cybersecurity has affected economic development negatively. For instance, China's administrative monopoly, which has excessively focused on serving narrow constituencies and has been largely unresponsive to the needs of the majority of the population, has become one of the largest institutional bottlenecks that has limited the country's capacity to utilize ICTs for economic growth and development. In this way, China's political framing of cybersecurity issues has done a great disservice to organizations in their pursuit of economic activities.

As noted earlier most GS economies lack domestic anti-virus companies. One way to understand the low level of technological progress is the lack of absorptive capacity, which means that many GS economies exhibit a low level of national capabilities in the assimilation of technologies and associated organizational practices (Cohen and Levinthal 1990; Dahlmann and Nelson 1995). This can be attributed to their institutional and social arrangements (Niosi 2008). To put things in context, institutional, social and organizational arrangements in the GS are not capable of coping with the rapid rise in cybercrimes. For instance, in 2004, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division (Duggal 2004). As of 2011, the Delhi police cybercrime cell had only two inspectors (Anand 2011). 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" (Nolen 2012, p. A1). Likewise, Malaysia's HeiTech Padu Berhad's director noted that out of the country's 40,000 lawyers, only four were able to handle cybercrimes (Ismail 2008). In the same vein, 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 ICT and poor understanding of ICTs and its added value in the national economy was hindering the adoption of CS-related legislation in the country (ITU 2008; Kshetri 2010b). Without sufficient measures to secure their computers, GS-based organizations will not be in a position to realize the full benefits of the ICTs.

Concerning the technology opportunity set, GS economies have a tendency to use low cost, yet insecure technologies. While some argue that networks in economies such as China 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" (Hawser 2011). Note that many systems in the industrialized world were developed before cybersecurity was a concern. However, contrary observations have been reported. For instance, China's cyber-victimization can be partly attributed to the country's crime-prone technologies. According to Microsoft's IE6Countdown website (http://www.ie6countdown.com/), as of January 2012, 6th

version of Microsoft's Internet Explorer (IE6) accounted for 27.9% of browsers in China. This compares with IE6's shares 1% in the U.S., and below 0.5% in Scandinavian countries. IE6 is reported to be an inherently insecure and hacker-friendly browser. In 2006, for instance, Internet Explorer was reported to be unsafe for 284 days.

GS economies also tend to use low cost and insecure technologies. Some GS-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 (Kirk 2012). 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 (Kirk 2012).

Finally, concerning the technology use, adoption and development, many Internet users in the GS are inexperienced and not technically savvy. A high proportion of them are getting computers and connecting to the Internet for the first time. A majority of them also lack English language. 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 the GS are thus unable to use IT security products developed in English language.

Discussion and implications

While adoption of technologies and organizational forms developed elsewhere allows poor countries to catch up with opportunities in rich countries, the majority of GS economies have failed to seize these opportunities (Wade 2008, quoting The Economist). This observation is equally evident in the case of cybersecurity. Cybersecurity issues have also brought about a radical challenge to the traditional way of measuring technology adoption and usage by using indicators such as the penetration levels or utilization levels (Easterly and Levine 1997; Veiseh 2010).

The above discussion suggests that technological, human, behavioral and policy-related factors have contributed to the hollowness of the GS economies on the ICT front. Organizations' and consumers' low levels of spending on IT security, in combination with low degree of cybersecurity consciousness, suggest some of the sources of the hollowness of the GS cyberspace (Kshetri 2010b, d, 2013). Cybersecurity orientations of businesses, consumers and the government agencies are determined by a set of factors different from those that are important for the digitalization of economic activities. While the GS is closing its economic gap in relation to the factors contributing to digitization, notable lags are inherent in factors related to cybersecurity.

The above discussion also indicates that cybercrimes originated in the GS have interesting international dimensions. Overture South Korea's "continental cut-off" service and similar other

examples indicate that there are already some signs that online transactions and activities originated in Africa and other GS economies are disregarded or dismissed by economic actors located in industrialized world. To take another example, Bordelinx, a U.S. based international electronic facilitator, stopped its services to clients from Kenya due to cybercrime concerns.

Cybercrime growth in Africa and other GS economies may increase the risk of exclusion of the continent's businesses and consumers from the cyberspace. A Telegraph article has summarized best as to how 419 scams have harbored distrust of Nigerians: "Trust in Nigerian businessmen and princes" is among the "50 things that are being killed by the internet".

An assertion of the dual economy approach is that GS economies are characterized by an uneven development within a sector as well as between various sectors of an economy (Chenery 1975). This uneven and unequal development translates into differential cybersecurity performance and capability. This can be illustrated best by comparing India's outsourcing sector with other economic sectors. Studies conducted by Forrester Research and by the U.K.'s Banking Code Standards Board indicated that cybersecurity standards in Indian call centers were among the best in the world. As noted above, some firms in India's banking, financial services and insurance, telecom, BPO sectors already have CISO in organizations (Pandya 2009). This means that new roles of CISO in organization are defined and rationalized by corporate boards of directors, CS professionals, legislatures, and regulatory agencies. Rowan (1982) refers to this stage as institution building. This stage is often followed by a period of diffusion, in which a large number of organizations may adopt the newly institutionalized organizational roles (Rowan 1982). This is likely to happen if the new roles gain legitimacy and are perceived as useful additions to the existing organizational structure.

Most economic sectors in India and other GS economies, however, have suffered from a poor level of cybersecurity. In this regard, prior research suggests that political, moral or technical crises and competition from alternative structures in other institutional sectors can destabilize the institutional and economic foundation of an existing organizational structure (Rowan 1982). This means that pressure for change in the existing cybersecurity practices is likely to build in the broader economy of the GS. At the same time regulators and policymakers need to be aware of the increasing importance of cybersecurity with increasing digitization and focus on regulation, education and other measures to strengthen cybersecurity and stimulate the institutional change process.

Concluding comments

The above examples are illustrative of how even genuine transactions originated from the GS are rejected by businesses in the industrialized world. This is a result of a hollow digitization of the GS. In this regard, the discussion in this paper suggests that appropriate public policy in the development of the digital society and economy must include steps to strengthen individuals' and organizations' attention and orientation to cybersecurity and enhance absorptive capacity in cybersecurity. A multifaceted and multi-pronged approach to address the dark side of GS economies' digitization is needed. For instance, governments and regulators can increase social trust by punishing people who are engaged in scams. Technological measures include elimination of insecure technologies such as counterfeit software and increasing the use of

cybersecurity applications such as antivirus software. It is also important to promote cybersecurity within organizations with better education and training. GS-based organizations need to embed cybersecurity-oriented culture throughout the workforce.

Acknowledgement

The author is grateful to MGDR editors-in-chief Nikhilesh Dholakia and Deniz Atik; and anonymous reviewers for their generous, insightful and constructive comments on earlier versions, which helped to improve the paper drastically.

References

allafrica.com. (2011) Nigeria: Mixed Feelings Trail CBN Cashless Policy as Date Draws Close, (accessed October 12, 2016), [available at http://allafrica.com/stories/201111101160.html].

Anand, J. (2011), "Cybercrime up by 700% in Capital," (accessed October 12, 2016), (accessed October 12, 2016), [available at http://www.hindustantimes.com/India-news/NewDelhi/Cyber-crimeup-by-700-in-Capital/Article1-766172.aspx].

Andreas, P. (2011), "Illicit Globalization: Myths, Misconceptions, and Historical Lessons," *Political Science Quarterly*, 126 (3), 403-425.

Bakewell, O. (2009), "Human Development Research Paper 2009/07: South–South Migration and Human Development: Reflections on African Experiences," (accessed October 12, 2016), [available at http://hdr.undp.org/en/reports/global/hdr2009/papers/HDRP_2009_07.pdf].

Boateng, R, Longe, O., Mbarika, V., Avevor, I., and Isabalija, S. R. (2010), "Cyber Crime and Criminality in Ghana: Its Forms and Implications," *Americas Conference on Information Systems (AMCIS) 2010 Proceedings*, (accessed October 12, 2016), [available at http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1503&context=amcis2010].

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

Cetron, M. J. and Davies, O. (2009), "Ten Critical Trends for Cyber Security", *Futurist*, 43 (5), 40-49.

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.

Child, J. (1972), "Organizational structure, environment and performance: The role of strategic choice," *Sociology*, 6, 1-22.

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

Dahlman, L. and Nelson, R. (1995), “Social absorption capability, national innovation systems and economic development,” in *Social Capability and Long-Term Growth*, B.H. Koo and D.H. Perkins (eds.) Basingstoke: Macmillan Press, 82-122.

Daily Trust. (2010), “EFCC Develops Software to Combat Cyber Crime In Nigeria,” 423, (accessed October 12, 2016), [available at http://www.balancingact-africa.com/news/en/issue-no-423/computing/efcc-develops-software-to-combat-cyber-crime-innigeria].

Damouni, N. (2014), Exclusive: U.S. companies seek cyber experts for top jobs, board seats, May 30. Reuters, [available at http://www.reuters.com/article/us-usa-companies-cybersecurityexclusive-idUSKBN0EA0BX20140530].

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, (accessed October 12, 2016), [available at http://www.oecd.org/dev/36309029.pdf].

Dogbevi, E. K. (2009), *Ghana to introduce Cyber Security Bill to Check Cyber Crimes,* [available at http://www.ghanabusinessnews.com/2009/05/19/ghana-tointroduce-cyber-security-bill-to-check-cyber-crimes/

Doval, P. (2013). Govt orders security audit of IT infrastructure, (accessed October 12, 2016), [available at http://timesofindia.indiatimes.com/tech/tech-news/Govt-orderssecurity-audit-of-IT-infrastructure/articleshow/38398644.cms]

Duggal, P. (2004), “What’s wrong with our cyber laws?” (accessed October 12, 2016), [available at http://www.expresscomputeronline.com/20040705/newsanalysis01.shtml].

Easterly, W. and Levine, R. (1997), “Africa's Growth Tragedy: Policies and Ethnic Divisions,” *The Quarterly Journal of Economics*, 112 (4), 8.

Fildes, J. (2010), “Stuxnet worm “targeted high-value Iranian assets,” (accessed October 12, 2016), [available at http://www.bbc.co.uk/news/technology-11388018].

Gady, F. S. (2010), “Africa's Cyber WMD,” March 24, (accessed October 12, 2016), [available at http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd?page=0,0].

Guillén, M. F. and Suárez, S. L. (2005), “Explaining the global digital divide: economic, political and sociological drivers of cross-national Internet use”, *Social Forces*, 84 (2), 681-708.

Hawser, A. (2011), “Hidden Threat,” *Global Finance*, 25 (2), 44-37

Hettigei, N.T. (2005), The Auditor's role in IT development projects, (accessed July 3, 2016) [available at: http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Pages/The-Auditors-Role-in-IT-Development-Projects1.aspx]

icspa.org, (2012), “Europol to lead International Cyber Security Protection Alliance consultation into the future of Cybercrime,” July 19, (accessed October 12, 2016), [available at https://www.icspa.org/media/icspa-news/newssingle/article/europol-to-lead-international-cyber-security-protectionalliance-consultation-into-the-future-of-cyb/abp/2/].

indiatimes.com, (2011), “Most Gurgaon IT, BPO companies victims of cybercrime: Survey,” November 6, (accessed October 12, 2016), [available at http://timesofindia.indiatimes.com/city/gurgaon/Most-Gurgaon-IT-BPO-companies-victims-of-cybercrime-Survey/articleshow/10626059.cms].

Ismail, I. (2008), “Understanding cybercriminals,” New Straits Times, Malaysia, 12.

ITU (2008), 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, International Telecommunications Union, (accessed 5 October 2009), [available at http://www.itu.int/ITUD/cyb/events/2008/lusaka/docs/lusaka-cybersecurity-forum-reportaug-08.pdf].

ITU. (U.D.), “Definition of Cybersecurity,” International Telecommunications Union (ITU), (accessed October 12, 2016), [available at http://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx].

Kalathil, S. (2003), “China’s New Media Sector: Keeping the State in,” *Pacific Review*, 16 (4), 489-501.

Kim, S. H., Wang, Q. and Ullrich, J. B. (2012), “A Comparative Study of Cyberattacks,” *Communications of the ACM*, 55 (3), 66-73.

Kinyanjui, K. (2009), “Watchdog warns of increased cybercrime threat”, 8 September, [available at http://www.businessdailyafrica.com/Company%20Industry/-/539550/654440/-/u765i9z/-/].

Kirk, J. (2012), “Microsoft finds new PCs in China preinstalled with malware,” (accessed October 12,2016), [available at http://www.pcworld.com/article/262308/microsoft_finds_new_computers_in_china_preinstalled_with_malware.html].

Kshetri, N. (2007), “The Adoption of E-Business by Organizations in China: An Institutional Perspective,” *Electronic Markets*, 17 (2), 113-125.

Kshetri, N. (2009), “Positive Externality, Increasing Returns and the Rise in Cybercrimes”, *Communications of the ACM*, 52 (12), 141-144.

Kshetri, N. (2010a), "The Economics of Click Fraud”, *IEEE Security & Privacy*, 8 (3), 45-53.

Kshetri, N. (2010b), “Diffusion and Effects of Cybercrime in Developing Economies,” *Third World Quarterly*, 31 (7), 1057-1079.

Kshetri, N. (2010c), *The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives*, Springer-Verlag: New York, Berlin and Heidelberg.

Kshetri, N. (2010d), "Cloud Computing in Developing Economies”, *IEEE Computer*, 43 (10), 47-55.

Kshetri, N. (2013a), *Cybercrime and Cybersecurity in the Global South: Structure, Processes and Characteristics*. Palgrave Macmillan: Houndmills, Basingstoke, U.K.

Kshetri, N. (2013b), “Cyber-victimization and Cybersecurity in China," *Communications of the ACM*, 56 (4), 35-37.

Kshetri, N. (2013c), “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.

Kshetri, N. (2013d), “Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations," *Electronic Commerce Research*, 13 (1), 41-69.

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

Kshetri, N. (2016b), *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, Springer-Verlag: New York, Berlin and Heidelberg.

Mazzitelli, A. L. (2007), “Transnational Organized Crime in West Africa: the Additional Challenge,” *International Affairs*, 83 (6), 1071-1090.

Mintzberg, H. 1993, *Structure in Fives: Designing Effective Organizations*. Prentice-Hall, Englewood Cliffs, NJ.

Niosi, J. (2008), “Technology, Development and Innovation Systems: An Introduction,” *Journal of Development Studies*. 44 (5), 613-621.

Nolen, S. (2012), “India's IT revolution doesn't touch a government that runs on paper,” *The Globe and Mail, Canada*, June 13, A1.

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

North, D. C. (1996), “Epilogue: Economic Performance through Time,” In L. J. Alston, T. Eggertsson and D. C. North (Eds.). *Empirical Studies In Institutional Change*. 342-355. Cambridge University Press, Cambridge, MA.

Nye, J. S. Jr. (2011, January/February), “China's rise doesn't mean war,” *Foreign Policy*, 184, 66-66.

Otis, C. and Evans, P. (2003), “The Internet and Asia-Pacific Security: Old Conflicts And New Behavior,” *Pacific Review*, 16 (4), 549-550.

Pandya, Dhwani. 2009. CISO reporting to board of directors: Myth or for real?, November 23, (accessed October 12, 2016), [available at http://www.computerweekly.com/news/1375176/CISO-reporting-toboard-of-directors-Myth-or-for-real].

Parto, S. (2005), “Economic activity and institutions: Taking stock,” *Journal of Economic Issues*, 39 (1), 21-52.

Reilly, M. (2007), “Beware, Botnets Have Your PC in Their Sights” *New Scientist*, 196 (2634), 22-23.

Roland, G. (2004), “Understanding Institutional Change: Fast-Moving and Slow-Moving Institutions”, *Studies in Comparative International Development*, 28 (4), 109-131.

Rowan, Brian. (1982), “Organizational Structure and the Institutional Environment: The Case of Public Schools”, *Administrative Science Quarterly*, 27 (2), 259-279

Seo, M.G., Creed, WED. (2002), “Institutional contradictions, praxis, and institutional change: a dialectical perspective,” *Academy of Management Review*, 27 (2), 222-247.

Sweeney, B. (2016), “Cybersecurity Is Every Executive’s Job,” *Harvard Business Review*, September 13, (accessed October 12, 2016), [available at https://hbr.org/2016/09/cybersecurity-is-everyexecutives-job].

tmcnet.com (2010), “Banks Upgrade Systems to Stop Cyber Criminals,” Business Daily/All Africa Global Media via COMTEX, (accessed October 12, 2016), [available at http://www.tmcnet.com/usubmit/2010/08/18/4963795.htm].

UNDP, (2006), “Country Evaluation: Assessment Of Development Results Honduras,” New York: United Nations Development Programme Evaluation Office, (accessed on October 12, 2016), [available at http://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf].

Veiseh, N. (2010), “Reconciling Acemoglu and Sachs: Geography, Institutions and Technology,” *Journal of International Affairs*, 64 (1), 205-220.

Wade, R. H. (2008), “How can Middle-Income Countries Escape 'Gravity' and Catch up with High-Income Countries? The Case for Open Economy Industrial Policy,” *Halduskultuur*. 9, 12-29.

Wylie, I. (2007), “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*, C.1.

Zorzini, C. (2016), “The Ultimate, Epic Guide to Create a Successful Online Business,” October 2016, ecommerce platforms, October 4, (accessed October 12, 2016), [available at http://ecommerceplatforms.com/ecommerce-selling-advice/ultimate-epic-guidesuccessful-online-shop].