Cybercrime and Cybersecurity Issues in the BRICS Economies

By: Nir Kshetri

Kshetri, Nir (2015). "Cybercrime and Cybersecurity Issues in the BRICS Economies," Editorial, *Journal of Global Information Technology Management* (JGITM), 18(4), 1-5.

Abstract:

Cybercrime and cybersecurity issues in the BRICS countries have important global implications, both politically and economically. All of the fast-growing BRICS economies are members of the Group of Twenty. These economies' cybersecurity frameworks have strong similarities and striking differences. This editorial provides a comparison of BRICS economies' approaches to cybersecurity.

Keywords: BRICS Economies | Cybercrime | Cybersecurity | PRISM Internet Surveillance Program

Article:

INTRODUCTION

Cybercrime and cybersecurity issues in the so-called BRICS countries (Brazil, Russia, India, China, and South Africa) have important global implications, both politically and economically. This is because these fast-growing economies, all of which are members of the Group of Twenty (also known as the G-20 or G20), represent about 3 billion people or 40% of the world population and 18% of the world economy. A key point from our perspective is that these economies have exhibited both strong similarities as well as striking differences in their approaches to cybersecurity.

A *China Daily* article published in July 2014 describes the common concerns that these economies share. The article noted that "further cooperation in improving cybersecurity will be a major focus of all BRICS states, all of which are inclined to alleviate dependence on Western technologies" (Yao, 2014, para. 10) All the BRICS countries have been concerned about the West's cyberspace dominance and are seeking to change the status quo by engaging in and fostering new international alliances. They are also making efforts to reformulate norms and standards. However, China's and Russia's emphasis on information security is an important

dimension on which these two economies deviate significantly from Brazil, India, and South Africa. China and Russia view information security as much broader than cybersecurity issue. A real purpose is arguably to increase the state's capacity and legitimacy for cyber-control and censorship. Observers have noted that important differences between India-Brazil-South Africa (IBSA) and BRICS meetings. For instance, it is noted that "issues related to human rights and civil society are not mentioned when the BRICS meet" (Stuenkel, 2012).

A comparison of cybercrimes in these economies and their approaches to cybersecurity could thus provide an interesting opportunity to explore contexts, mechanisms, and processes associated with the cybersecurity frameworks in economies with diverse political, cultural, and economic backgrounds. The goal of this editorial is to provide such a comparison in order to better understand emerging cybersecurity frameworks.

CYBERCRIMES IN BRICS ECONOMIES

The BRICS countries are originators of significant cybercrime activities and are also characterized by high cybercrime victimization rates. According to the 2013 Norton Report, Russia, China, and South Africa ranked the world's top three countries in terms of number of cybercrime victims (Symantec Corporation, 2013). As early as 2004, losses from online financial fraud in Brazil were estimated to exceed losses through bank robberies. A study of PricewaterhouseCoopers (PwC) revealed that hackers stole US$1 billion from Brazilian companies in 2011. According to the Brazilian Federation of Banks (Febraban), cybercrime accounts for 95% of losses incurred by Brazilian banks. Febraban estimated that US$1.4 billion was lost to electronic fraud in 2012.

A 2012 *China Daily* piece titled "Personal Data Protection" provided a succinct and valuable update on China's data privacy breaches' increasing prevalence and consequences. According to the editorial, illegal firms in the country specialize in collecting and selling personal information, acquiring information from subsidiaries of major telecommunication firms, and sending text messages for profit. Some bank and telecommunications company employees have been arrested for selling personal information to such firms. A China Internet Network Information Center report indicated that, in the first half of 2011, 121 million Chinese had their online account information stolen (Kshetri, 2014).

According to the Norton Cybercrime Report 2011 (Symantec Corporation, 2011), 30 million Indians had become cybercrime victims, which cost the Indian economy $7.6 billion a year. India also generates significant amount of cybercrimes that affect Internet users worldwide. For instance, India was the top origin country for spam in 2011 and 2012. Likewise, a phishing survey released by the Anti-Phishing Working Group (APWG) in April 2012 found that India had the highest phishing TLDs by domain score (calculated as phish per 10,000 domains) in the second half (H2) of 2011.

Likewise, cybercrime in Russia has grown into a substantial industry, which according to some estimates employs 10,000–20,000 people in "dark side" activities such as engaging in bank frauds, selling scareware, and sending fake pharmacy spam (Leyden, 2010). Most economic and financial crimes in Russia and other former Soviet Union economies are associated with

organized crime groups. Russian hacking rings and organized crime networks have reportedly collaborated with criminals groups with Australia, Japan, Malaysia, and other countries.

In the same vein, cybercrime is the fastest-growing white-collar crime in South Africa. PwC biennial Global Economic Crime Survey conducted in 2007 indicated that 72% of South African companies had become cybercrime victims in the previous 2 years. A consultant to the biometric security industry estimated that South African organizations lose about US$20 billion a year in cybercrimes. According to the perpetrators, based on complaints made to the U.S. agency Internet Crime Complaint Center (I3C), South Africa ranked among the top 10 countries.

BRICS ECONOMIES' APPROACHES TO CYBERSECURITY

Due to the rapidly growing cybercrimes and various other forces, the BRICS economies have introduced a number of cybersecurity measures. Indeed, some of these economies have been among global leaders in the enactment of new cybersecurity-related legislations. The Internet Bill of Rights known as "Marco Civil da Internet," which was proposed in the Brazilian Congress in 2011, received new significance following the revelation of the U.S. National Security Agency's (NSA) PRISM (Personal Record Information System Methodology) Internet surveillance program. Brazil's president Dilma Rousseff postponed her planned state visit to the United States because of anger at the revelations that the NSA had allegedly intercepted her private communications. In a speech to the U.N. General Assembly in September 2013, Rousseff condemned the NSA's spying as a breach of international law. Rousseff also called for a global multilateral Internet governance meeting. It led to the NETmundial held in April 2014 in Sao Paulo, Brazil. Marco Civil da Internet was passed by the Brazilian Senate in April 2014 and signed by the president in the same month. It intends to provide privacy protections for Internet users, and limit the amount of metadata that can be gathered on Brazilians. Disclosure of personal data to third parties requires the user's informed consent. Companies collecting personal data from residents of Brazil are subject to Brazil's laws and courts in cases involving information on Brazilians irrespective of the location of data storage (Stankey, 2014). In order to get opposition support, the government agreed to withdraw a provision in the proposed Internet law, which would have required foreign Internet companies to host data of Brazilians in the country.

China has enacted a number of key legislations governing data privacy and security most recent of which include The Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data, issued December 28, 2012, and Information Technology Security—Guideline for Personal Information Protection Within Information Systems for Public and Commercial Services, issued February 1, 2013 (Kshetri, 2014). A national body formed in February 2014 to coordinate cybersecurity is headed by President Xi Jinping. Analysts have interpreted this as a signal of the importance he placed on cyber-control.

India has been relatively quick in following the global trend in enacting cybersecurity related laws and regulations. For instance, the Information Technology Act was passed in 2000, which was amended in 2008 to address a number of issues (e.g., adoption of electronic signatures and a more detailed and careful approach to child pornography). The Information Technology Amendment Act of 2008 has made it an offence to facilitate the abuse of children online. A goal

has also been to bring Indian data protection laws to the same level as the European and the U.S. standards (Kshetri, 2015).

Russian cybersecurity-related legal framework is comparable to most European countries (Kshetri, 2013). To discourage spammers, in April 2010, Russia introduced regulations to tighten up domain registrations. The new regulations require copies of passports or legal registration papers for businesses to register a .ru domain. Before this regulation came into effect, domains were set up without any checks (Leyden, 2010).

In the same vein, South Africa's Cabinet passed the National Cyber Security Policy Framework in March 2012. The Department of Communications appointed the National Cyber Security Advisory Council in October 2013. South Africa is one of the four non-member states of the Council of Europe (CoE) which has signed the International Treaty on Cybercrime. The CoE's Cybercrime Convention asks signatory countries to enact legislation criminalizing the Convention-specified cybercrime categories.

The issue is not one of the existence of cybercrime laws, but of enforcement mechanisms. In Brazil, only 5–8% of crimes are solved due to the scarcity of law enforcement resources. A prevailing culture of violence in cities such as São Paulo, Rio de Janeiro, and Brasília have taken most of the available resources, and left little law enforcement resources to enforce cybercrimes. In China, the relatively selective enforcement of existing regulations and intensification of cybercontrol measures have led to the arrest of several democracy organizers, human rights activists, members of the spiritual organization Falun Gong, scholars, and other dissidents for alleged involvement in cybercrimes. On the other hand, the Chinese government has devoted relatively few resources to enforce data privacy measures.

Looking at the situation in India, in 2004 for instance, of the 4,400 police officers in India's Mumbai city, only five worked in the cybercrime division. As of November 2011, the Delhi Police cybercrime cell had only two inspectors (Kshetri, 2013). In June 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, A1) This has led to a widespread lack of confidence in law enforcement agencies. According to a survey cited by indiatimes.com, while most business process outsourcing (BPO) organizations in Gurgaon had been cybercrime victims, about 70% of the respondents did not report to the police. Most organizations expressed concerns about competence, professionalism and integrity of the police in handling cybercrimes. About 50% of the respondents not reporting thought that the cases are not dealt with professionally and 30% noted that they had no faith in the police. Likewise, prosecutions related to cybercrime are vanishingly low at five to six people per year in Russia (cited in Kshetri, 2013).

CONCLUDING COMMENTS

Various elements of formal institutions such as orientation toward democratic power structures and the nature of relationship with the West are tightly linked to the approaches to cybersecurity. For instance, compared to Brazil, India, and South Africa, China and Russia have shown stronger disagreements with the West in issues related to cybersecurity.

Cybercrime and cybersecurity issues in the BRICS economies are representative of the situations that exist in many other emerging and developing countries. As in BRICS economies, there is an enormous gap between laws in the book and enforcement capability in most emerging and developing countries. They can enact all the rules and regulations they want, but they are meaningless if they do not have resources to enforce them. In fact, in most other developing countries the situation is even worse than in BRICS economies. This is because most of the smaller developing economies are not subject to the same level of pressure to strengthen cybersecurity-related regulatory measures. They are also often under conditions of more severe resource constraints. Due to the global and trans-border nature of cybersecurity issues, industrialized economies need to be prepared to offer appropriate help and support to smaller and poorer developing nations in order to help them develop appropriate regulatory framework and enforcement mechanisms.

REFERENCES

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

Kshetri, N. (2014). China's data privacy regulations: A tricky trade-off between ICT's productive utilization and cyber-control. *IEEE Security & Privacy*, *12*(4), 38–45. doi:10.1109/MSP.2013.105

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

Leyden, J. (2010). *Russian trade body aims to fight cybercrime: Russia no safe haven for spammers and cybercriminals*. Retrieved from http://www.theregister.co.uk/2010/04/12/russia_cybercrime_feature/

Nolen, S. (2012, June 13). India's IT revolution doesn't touch a government that runs on paper. *The Globe and Mail* (Canada), A1, para. 5.

Personal Data Protection. (2012, April 6). [Editorial]. *China Daily*. Retrieved from http://www.chinadaily.com.cn/opinion/2012-04/06/content_14987674.htm//website/

Symantec Corporation. (2011). *Norton Cybercrime Report 2011: The Shocking Scale of Cybercrime*. Mountain View, CA: Author. Retrieved from http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

Symantec Corporation. (2013). *2013 Norton Report*. Mountain View, CA: Author. Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Stankey, R. (2014). *Brazil enacts "Internet Bill of Rights," including net neutrality and privacy protections.*Retrieved from http://www.jdsupra.com/legalnews/brazil-enacts-internet-bill-of-rights-36906/

Stuenkel, O. (2012, August 12). Keep BRICS and IBSA separate. *The Diplomat*. Retrieved from http://thediplomat.com/the-editor/2012/08/13/keep-the-brics-and-ibsa-seperate/

Yao, Z. Z. (2014, April 7). Role of emerging economies. *China Daily*. Retrieved from http://usa.chinadaily.com.cn/opinion/2014-07/14/content_17756717.htm

Author information

Nir Kshetri is a professor at Bryan School of Business and Economics, The University of North Carolina at Greensboro, and a research fellow at Kobe University. He is the author of four books and 85 journal articles. He has been interviewed and/or quoted in over 60 TV channels, magazines, and newspapers.