Available online at www.rsu.ac.th/rjsh
ISSN 2286-976X / Online: ISSN 2539-5513
RJSH Vol. 4, No. 2, July - December 2017, pp.23-33

The Cyber-Attacks and Digital Economy in India during 2004 - 2015

Srirath Gohwong

Faculty of Social Sciences, Kasetsart University, Bangkok 10900 Thailand
E-mail: srirathg3@yahoo.com

Submitted 19 June 2017; accepted in final form 7 August 2017

Abstract

This article focuses on the study of the cyber-attacks and digital economy in India during 2004 – 2015 in order to 1) to find out the types and patterns of all cyber-attacks in India during 2004 – 2015, 2) to investigate the relationship between GDP of India and the cyber-attacks in India during 2004 – 2015, and 3) to compare the cyber-attacks between India and Thailand during 2012 – 2015 due to the availability of data. Frequency, percentage, mean, standard deviation, and Pearson's Product-Moment Correlation are the statistics employed for data analysis. The level of significance was set at .05.

The results were as follows: 1) There were 310,146 attacks, or approximately 25,846 attacks per year during 2004 to 2015 in India, 2) In aspect of techniques of the attacks, there were big four in India during 2004 – 2015: abusive content, information security, intrusions, malicious code, 3) In overall, there has been an upward trend of cyber-attacks in India since 2004 – 2014, except in 2015 due to the implementation of "Digital India" program. In categorical level, two absolute different trends – upward and downward trends occurred in India. The upward trend focuses on all crowd – oriented cyber-attacks of information gathering, information security, malicious code, and others whereas the downward trend focused on individual-oriented cyber-attacks such as abusive content, intrusions, and fraud, 4) there were quite high positive relationship between GDP of India and the cyber-attacks in India during 2004 – 2015 in the overall level at the .01, and categorical level, fraud, information gathering, and malicious code had high positive relationships with GDP of India at the .01, and with intrusions and other at .05; and 5) In overall, the amount of cyber-attacks of Thailand (Z score = 6.47) was higher than India (Z score = 5.18). In categorical level, Thailand had more serious cyber-attacks than India with approximately 1.48 S.D. in malicious code and approximately 0.76 S.D. in intrusions.

Keywords: *Cyber-attacks, digital economy, India, 2004 2015*

1. Introduction

According to her long plan, India Vision 2020, India has changed herself to be a developed country in the year of 2020 by transforming from product-based economy to digital economy since 1993, in which her Vision about Technology in India Vision 2020 was set by Technology Information, Forecasting and Assessment Council (TIFAC). In addition, the emerging of "Digital India" program since 2014 in order to prepare India's readiness for digital economy will accelerate the growth of Indian digital economy in India for supporting 462,124,989 Internet Users, 34.83% of total population, on July 2016. (Kalam & Rajan, 1998; CMAI, 2014; Blasi et al., 2015; Department of Electronics and Information Technology, Ministry of Electronics and Information Technology, Government of India, 2015; Internet Live Stats, 2016.) However, the transformation towards new economy has a big cost of more innovative and sophisticated cyber-attacks which directly compromises CIA triangle of information security of India and Confidentiality-Integrity-Availability. These attacks decelerates the growth of digital economy (Whitman & Mattord, 2003; Whitman & Mattord, 2008; Whitman & Mattord, 2012; Gnanasambandam et. al., 2012; Durand & Vergne, 2013; Boyle & Panko, 2015; Tapscott, 2015; Deloitte, 2015; Nedeltchev, Gopalratnam, & Tirumala, 2015) For India, according to data since 2004 of Indian Computer Emergency Response Team (CERT-In, 2016), there are 310,146 attacks, or approximately 25,846 attacks per years.

According to the above-mentioned concern, this article has three focuses on India in order to get the basic information about cyber-attacks in India and the lessons for the implementation of digital economy of Thailand as follows: 1) to find out the types and patterns of all cyber-attacks in India during 2004-2015, 2) to investigate the relationship between GDP of India and the cyber-attacks in India during 2004-2015, and 3) compare the cyber-attacks between India and Thailand during 2012-2015 due to the availability of Thai data.

2. Digital India

The Digital India has been adopted by Prime Minister Narendra Modi since 2014. It is an umbrella program, run by Department of Electronics and Information Technology (DeitY) for many government Ministries and Departments under a single vision of the Government of India in order to prepare and promote "citizen empowerment and inclusion" and "digital economy / knowledge economy" in India. It has lots of consultations from many entities such as government, industry, civil society and citizens. It also employs the "myGov" (http://mygov.in/) – a digital platform by DeitY – for facilitating, collaborating and participating the program. In general, the program centered on 3 key areas – info-structure for every citizen, public services on demand, promotion of digital literacy and IT access of every citizen. In addition, there are nine strategies / pillars in this program: broadband highways, universal access to mobile connectivity, public internet access program, e-Governance reforming government through technology, e-Kranti or electronic delivery of services, information for all, electronics manufacturing, IT for jobs and early harvest programs. Each of these strategies is run across multiple ministries and departments (Department of Electronics and Information Technology, Ministry of Electronics and Information Technology, Government of India, 2015; Deloitte, 2015).

3. Type of Information Attacks

Cyber-attacks are any acts by threat agents for compromising the security of victims' devices for the interest of attackers (Whitman & Mattord, 2003; Whitman & Mattord, 2008; Whitman & Mattord, 2012). There are various classification of information attacks (Whitman & Mattord, 2003; Whitman & Mattord, 2008; Whitman & Mattord, 2012; Oz, 2009; Brown, C.V. et al., 2014; Marakas & O'Brien, 2014; Valacich & Schneider, 2014; Boyle & Panko, 2015; Laudon & Laudon, 2016; European Computer Security Incident Response Team Network, 2003).

In this paper, eCSIRT's taxonomy will be employed for data analysis because it is the standardized framework which covers all above-mentioned classifications. In addition, it is very convenient for comparing with cyber-attacks in Thailand, which employs this classification for national cyber-security (Gohwong, 2016a).

European Computer Security Incident Response Team Network (eCSIRT) employs the WP4 Clearinghouse Policy - Release 1.2, the common framework for information security – classified by Jimmy Arvidsson in 2003, as follows: abusive content (spam, harassment, child/sexual/ciolence), malicious code (virus, worm, Trojan, spyware, Dialer), information gathering (scanning, sniffing, social engineering), intrusion attempts (exploiting of known vulnerabilities, login attempts, new attack signature), intrusions (privileged account compromise, unprivileged account compromise, application compromise), availability (DoS, DDoS, Sabotage), information security (unauthorized access to information, unauthorized modification of information), fraud (unauthorized use of resources, copyright, masquerade), and otherall incidents which don't fit in one of the previous categories (European Computer Security Incident Response Team Network, 2003).

4. Methodology

This study is a quantitative research. The data for analysis were 1) the cyber-attacks data during 2004 – 2015 from Indian Computer Emergency Response Team (CERT-In, 2016) for analyzing the types and patterns of all cyber-attacks in India during 2004 – 2015, 2) the cyber-attacks data during 2012 – 2015 from MICT of Thailand (MICT of Thailand, 2016) for comparing India and Thailand, and 3) GDP data from World Bank (World Bank, 2016) for finding out the relationship between GDP of India and the cyber-attacks in India during 2004-2015. The statistics employed in this study are frequency, percentage, mean, standard deviation, Pearson's Product-Moment Correlation. The level of significance is set at .05.

5. Findings

5.1 Types and patterns of all cyber-attacks in India during 2004 – 2015

All cyber-attacks in India during 2004 – 2015 are shown in Table 1 and Figure1.

Table 1 Types and patterns of all cyber-attacks in India during 2004-2015
(N = 12)

eCSIRT's classification	India	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	Total
Abusive content	1	0	0	0	0	305	285	981	2480	8150	54677	85659	0	152537
Information security	2	0	0	0	0	0	0	0	0	0	0	25037	26244	51281
Intrusions	3	0	0	0	0	835	6548	6344	4394	4591	5265	7286	961	36224
Malicious code	4	5	95	19	358	408	596	1817	2765	3149	4160	4307	9830	27509
Other	5	4	18	17	264	148	160	188	1240	2417	3484	3610	8213	19763
Information	6	11	40	177	223	265	303	477	1748	2866	3239	3317	3673	16339
Fraud	7	3	101	339	392	604	374	508	674	887	955	1122	534	6493
Availability	N/A	0	0	0	0	0	0	0	0	0	0	0	0	0
Intrusion Attempts	N/A	0	0	0	0	0	0	0	0	0	0	0	0	0
Total		**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**	**71780**	**130338**	**49455**	**310146**

Note. 1 = Spam, 2 = Website Defacements, 3 = Website Compromise (Website Intrusion) and Malware Propagation, 4 = Virus / Malicious Code, 5 = Others, 6 = Network Scanning/Probing, 7 = Phishing

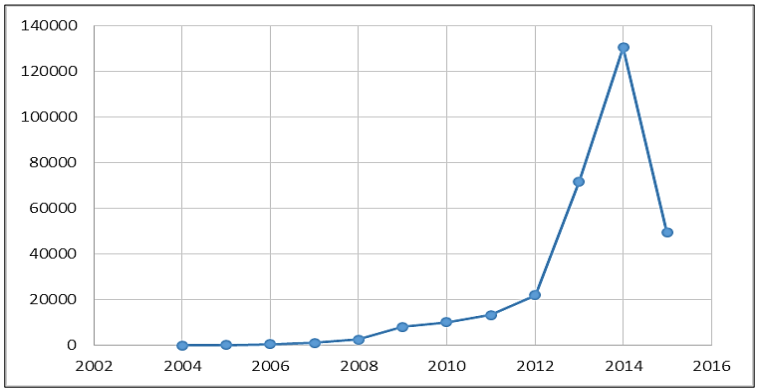

Figure 1 Amount of overall cyber-attacks in India during 2004-2015

The findings were found as follows:

1) There are 310,146 attacks, or approximately 25,846 attacks per year in India during 2004 – 2015.

2) According to Figure 1, in overall, there has been an upward trend of cyber-attacks in India since 2004 – 2014. After that, due to the implementation of "Digital India" program on info-structure, online governmental services, and IT literacy since 2014, it becomes the downward trend in which 62.1% deceased from 2014.

3) In categorical level, there are two absolute different trends according to techniques of cyber-attacks – upward and downward trends. The upward trend in pattern I, shown in figures 5 – 8, comprises all crowd – oriented cyber-attacks as follows: information gathering (network scanning / probing), information security (website defacements), malicious code (virus), and other attacks such as email spoofing (2004-2006) whereas the downward trend in pattern II, shown in figures 1 – 4, focuses on individual-oriented cyber-attacks such as sbusive content (spam), intrusions (website compromise / website intrusion and malware propagation) and fraud (phishing).

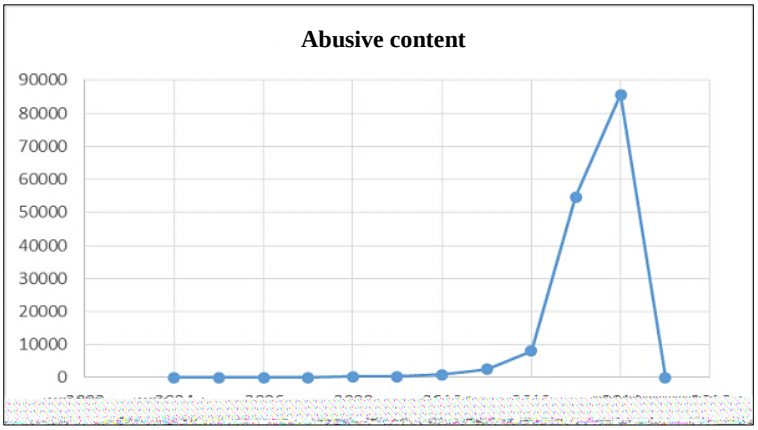

Figure 2 Abusive content in India during 2004-2015

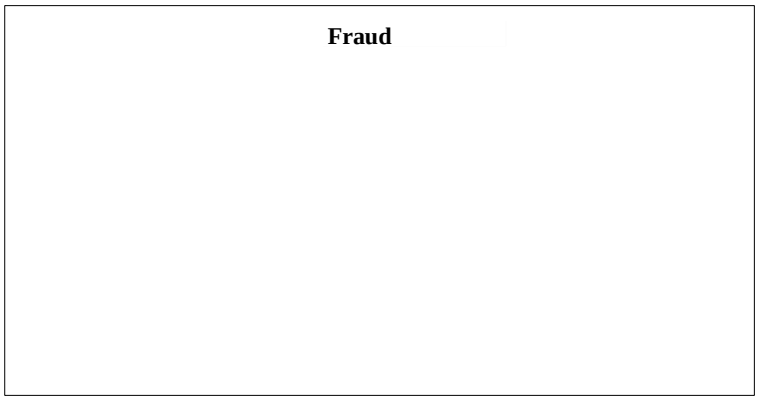

Figure 3 Fraud in India during 2004-2015

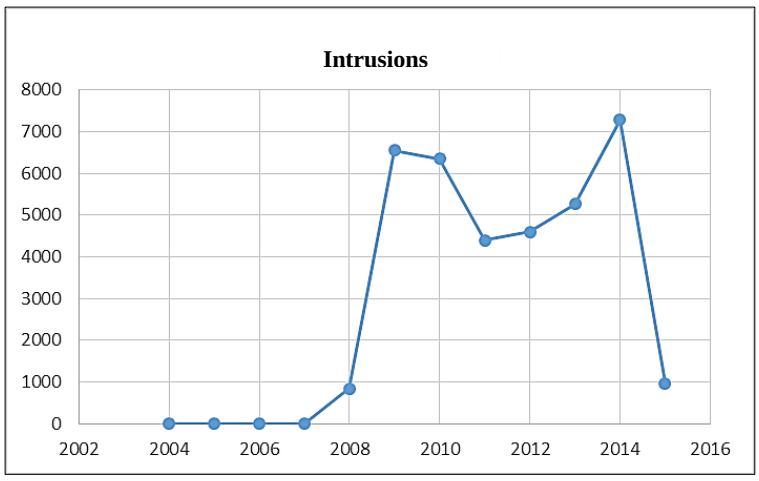

Figure 4 Intrusions in India during 2004-2015

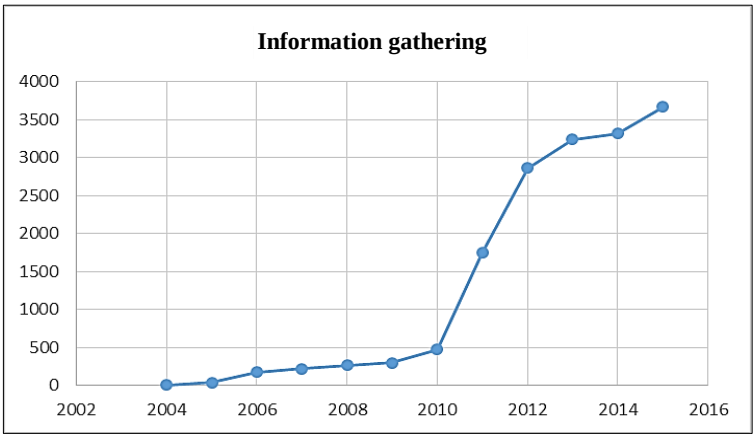

Figure 5 Information gathering in India during 2004-2015

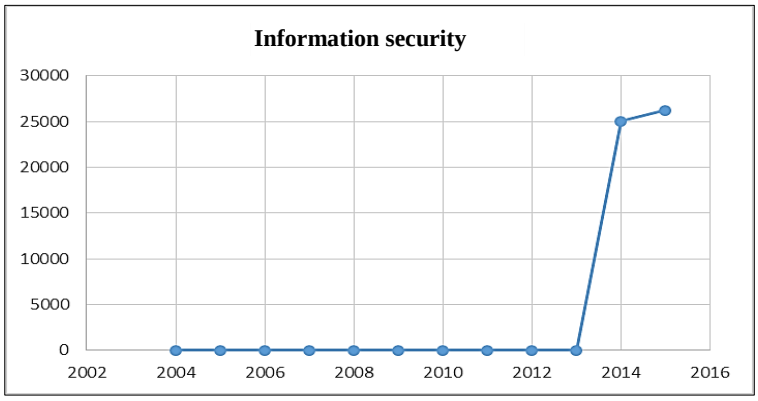

Figure 6 Information security in India during 2004-2015

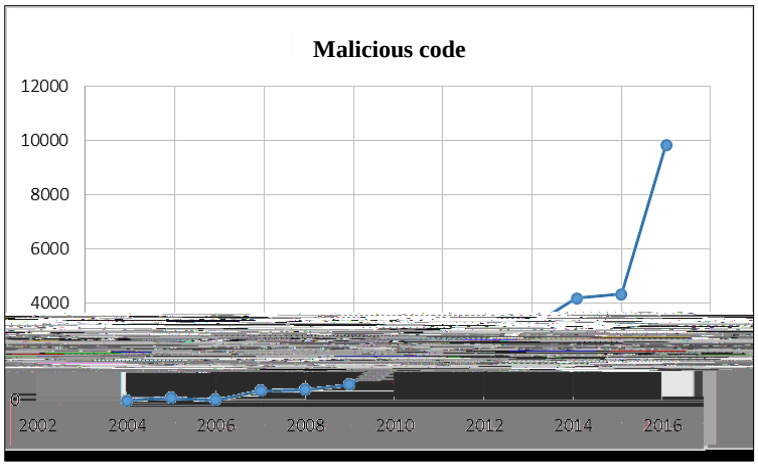

Figure 7 Malicious code in India during 2004-2015

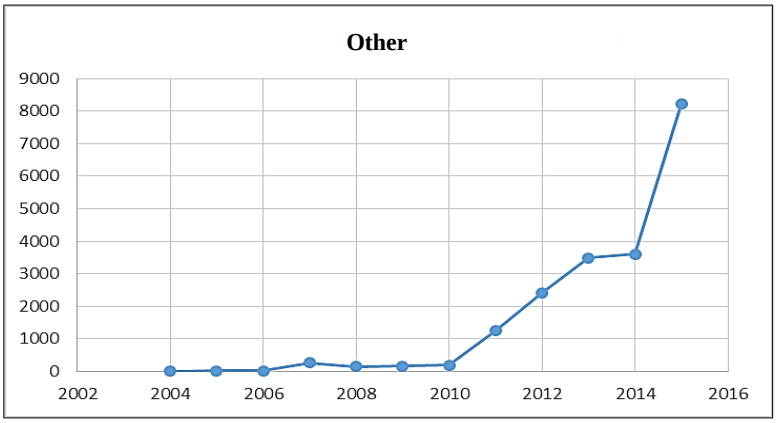

Figure 8 Other attacks in India during 2004-2015

4) In aspect of techniques of the attacks, there are big four in India during 2004-2015 (see Table 2): abusive content, information security, intrusions, and malicious code. The big four cyber-attacks can be categorized into two groups: crowd-oriented cyber-attacks (information security and malicious code) and individual-oriented cyber-attacks (abusive content and intrusions). The first group has in the upward trend though its number of attacks is less than the latter group. In contrast to the first one, the latter one has downward trend though abusive content which is the highest and intrusions is in the third place. However, spam as one technique in abusive content is the highest cyber-attacks with almost 50% in India.

Table 2 Overall of cyber-attacks in India during 2004-2015
(N= 12)

eCSIRT's classification	India	Total	Mean
Abusive content	Spam	152537 (49.18)	12711.42
Information security	Website Defacements	51281 (16.53)	4273.42
Intrusions	Website Compromise (Website Intrusion) and Malware Propagation	36224 (11.68)	3018.67
Malicious code	Virus / Malicious Code	27509 (8.87)	2292.42
Other	Others	19763 (6.37)	1646.92
Information gathering	Network Scanning/Probing	16339 (5.27)	1361.58
Fraud	Phishing	6493 (2.09)	541.08
Availability	N/A	0 (0.00)	0
Intrusion Attempts	N/A	0 (0.00)	0
Total		**310146 (100.00)**	**25845.50**

The association between GDP of India and the cyber-attacks in India during 2004-2015 is shown in Table 3.

Table 3 The association between GDP of India and the cyber-attacks in India during 2004-2015 (N = 12)

Cyber-attacks in India During 2004 – 2015	GDP (current US$)	
	r	P
Abusive content	.490	.11
Fraud	.842	.00**
Information gathering	.844	.00**
Information security	.538	.07
Intrusions	.691	.01*
Malicious code	.777	.00**
Other	.698	.01*
Total	**.666**	**.02***

* Significant at the .05 level, ** Significant at the .01 level

There are quite high positive relationship between GDP of India and the cyber-attacks in India during 2004-2015 in the overall level at the .01, and categorical level, fraud, information gathering, and malicious code have high positive relationships with GDP of India at the .01, and with intrusions and other at .05.

5.2 Comparison between India and Thailand

The key purpose of this paper is to give an important lesson for Thailand; therefore, comparison of cyber-attacks between India and Thailand is a must. However, due to the availability of data, comparison of cyber-attacks between India and Thailand was conducted only during 2012-2015. In addition, Z-score, shown in Table 4, was employed in this study for standardizing cyber-attacks data from two different sources, which had different amount, data collection methods and mean (Rowntree, 2000; Rumsey, 2011).

Table 4 Z-score of cyber-attacks between India and Thailand during 2012-2015

Z-score of cyber-attacks during 2012 - 2015	India	Thailand
Abusive content	2.51	-0.79
Availability	-0.65	-0.79
Fraud	-0.57	1.44
Information gathering	-0.37	-0.74
Information security	0.44	-0.80
Intrusions	-0.26	0.76
Intrusion Attempts	-0.65	0.23
Malicious code	-0.19	1.48
Other	-0.27	-0.80
Total	**5.18**	**6.47**

Table 5 Types and patterns of all cyber-attacks in Thailand during 2012-2015 (N= 4)

eCSIRT's classification	Thailand
Malicious code	3439 (31.51)
Fraud	3376 (30.93)
Intrusions	2358 (21.60)
Intrusion Attempts	1559 (14.28)
Information gathering	99 (0.91)
Abusive content	32 (0.29)
Availability	26 (0.24)
Other	19 (0.17)
Information security	7 (0.06)
Total	**10915 (100.00)**

Table 6 GDP between India and Thailand during 2012-2015

Year	India	Thailand
2012	$1,444.27	$5,859.92
2013	$1,456.20	$6,171.26
2014	$1,576.82	$5,941.84
2015	$1,581.59	$5,814.86

Note. GDP per capita (current US$)
Source: World Bank, 2016a, 2016b

According to the data from Tables 4, 5 and 6, in overall, the amount of cyber-attacks in Thailand (Z score = 6.47), with greater GDP per capita than India, was higher than India (Z score = 5.18). In categorical level, Thailand had more serious malicious code and intrusions – two top cyber-attacks of both countries –than India with approximately 1.48 S.D. in malicious code and approximately 0.76 S.D. in intrusions.

6. Discussion

Findings about cyber-attacks in India during 2004-2015

1) The finding about 310,146 attacks, or approximately 25,846 attacks per year in India during 2004-2015 reveals one fact that the more access to Internet under digital economy since 1996, the less information security (Whitman & Mattord, 2012).

2) In overall, there has been an upward trend of cyber-attacks in India since 2004-2014, except in 2015 due to the implementation of "Digital India" program, especially the third area – promotion of digital literacy and IT access of every citizen (universal digital literacy) by universal access to

digital resources, all documents such as certificates and entitlements on cloud, digital resources / services in Indian languages, "myGov" as a key collaborative digital platform for participating the program. People with good 1IT knowledge do not easily become the victims of cyber-criminals.

3) In categorical level, two absolute different trends – upward and downward trends occur in India. The upward trend focuses on all crowd – oriented cyber-attacks as follows: information gathering, information security, malicious code, and other whereas the downward trend focuses on individual-oriented cyber-attacks such as abusive content, intrusions, and fraud. These attacks of the upward trend focuses on property rights and intellectual property, online anonymity, network security (Himma & Tavani, 2008; Quinn, 2012; Quinn, 2015; Laudon & Laudon, 2016).

4) For the investigation of association between GDP of India and the cyber-attacks in India during 2004-2015, there are quite high positive relationship between GDP of India and the cyber-attacks in India during 2004-2015 in the overall level at the .01, and categorical level, fraud, information gathering, and malicious code have high positive relationships with GDP of India at the .01, and with intrusions and other at .05. This findings support the previous findings in 6.1.1 that the more access to Internet under digital economy, the less information security, and in 6.1.2 that almost of cyber-attacks are attacks towards masses of people with high positive relationship such as information gathering (r = .844), malicious code (r = 0.777), other (r = 0.698), except fraud (r = 0.842) and intrusions (r = 0.691). It shows an interesting trend in India that the state of the art and trend of cyber destruction in India focuses on mass deterioration.

In overall, an important lesson for Thailand from the previous findings is that India (Z score = 5.18) with lower value of GDP per capita faced cyber-attacks less than Thailand (Z score = 6.47) because she had higher gap of digital "haves" and digital "have-nots" than Thailand. This kind of problem about access to ICT equipment with Internet is digital divide, measured by ICT Development Index (IDI). This standard tool, which full score is 10, has 11 indicators in three groups – access, use and skills. For instance, in 2015, her IDI score 2.69 whereas Thailand was 5.36 (ITU, 2015). If IT is considered as a language, people in the country with good IT literacy who can both use, read and write or code the programs do not easily become the victims in digital setting. In addition, some people often have opportunistic behaviors by committing cyber-crimes from their good knowledge on digital language. In other words, the more IDI score, the more people with high IT literacy. That is why India with low IDI score mostly had cyber-attacks in information gathering (network scanning / probing), information security (website defacements), malicious code (virus), and other attacks such as email spoofing (2004-2006) – which are the crowd–oriented cyber-attacks – because it is quite convenient for attackers to do this kind of cyber-attacks against their victims who have low IT literacy about network security. On the other hand, Thailand with medium IDI score mostly faced the problems from individual-oriented cyber-attacks such as intrusions (website compromise / website intrusion, malware propagation), intrusion attempts, and fraud (phishing) because the attackers must employ more sophisticated techniques against the networks of their victims who have fair IT literacy.

In categorical level, Thailand had more serious malicious code and intrusions – two top cyber-attacks of both countries –than India with approximately 1.48 S.D. in malicious code and approximately 0.76 S.D. in intrusions. The possible reason is that most of top Thai universities according to the top-100 Asia-Pacific universities of Webometrics, the leading E-university ranking, put great emphasis on infrastructure / IT infrastructure in their undergraduate-level curriculum of management information systems such as coding which is necessary for malicious code and intrusions. It is noteworthy that there was not any university of India in the list (Webometrics, 2015; Gohwong, 2016b).

7. Conclusion

This article focuses on the study of the cyber-attacks and digital economy in India during 2004-2015, by using data from Indian Computer Emergency Response Team (CERT-In) in order to (1) find out the types and patterns of all cyber-attacks in India during 2004-2015, (2) investigate relationship between GDP of India and the cyber-attacks in India during 2004-2015, and (3) compare the cyber-attacks between

India and Thailand during 2012-2015. The findings give an important lesson for Thailand, which just fully join the digital economy in 2014 that the more access to Internet under digital economy, the less information security. In addition, it is not easy to find the balance between access and information security, especially in digital economy (Whitman & Mattord, 2012; Tapscott, 2015; Gohwong, 2016).

8. References

Abigail, B. (2015). *India. Singapore*. Lonely Planet Publications: Pty.

Boyle, R. J., & Panko, R. R. (2015). *Corporate Computer Security*. Essex: Pearson Education Limited.

Brown, C. V., DeHaes, D.W., Slater, J., Martin, W.E., & Perkins, W.C. (2014). *Management Information Technology*. Essex: Pearson Education Limited.

Gnanasambandam, C., Madgavkar, A., Kaka, N., Manyika, J., Chui, M., Bughim, J., & Gomes, M. (2012). *Online and upcoming: The Internet's impact on India McKinsey*. Retrieved June 6, 2016, from http://www.mckinsey.com/~/media/mckinsey%20offices/india/pdfs/online_ and_upcoming_the_internets_impact_on_india.ashx

CMAI. Digital India. (2014). Retrieved June 6, 2016, from http://www.cmai.asia/digitalindia/

Department of Electronics and Information Technology (DeitY), Ministry of Electronics & Information Technology, Government of India. (2015). Digital India: Power to empower (2015). Retrieved June 6 from http://www.nio.org/nio/uploads/digital-india-ebook.pdf

Deloitte.(2015). Digital India: Unleashing Prosperity. Retrieved June 6, 2016, from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology- media-telecommunications /in-tmt-tele-tech-2015-noexp.pdf

Durand, R., & Vergne, J. P. (2013). The Pirate Organization: Lessons from the Fringes of Capitalism. Boston: Harvard Business Review Press.

European Computer Security Incident Response Team Network (eCSIRT). (2003). WP4 Clearinghouse Policy - Release 1.2. Retrieved January 1, 2016, from http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html

EY & FICCI. (2015). Speeding ahead on the telecom and digital economy highway: Key priorities for realizing a "Digital Bharat". Retrieved June 6, 2016, from http://www.ey.com/Publication/vwLUAssets/ey-speeding-ahead-on-the-telecom-and-digital-economy-highway/$FILE/ey-speeding-ahead-on-the-telecom-and-digital-economy-highway.pdf

Gohwong, S. (2016a). The Cyber-attacks and digital economy in Thailand during 2012 – 2016. 1st International Conference (IRC1/2016) at Hong Kong on August 25-27, 2016.

Gohwong, S. (2016b). The investigation of the study of Management Information Systems in undergraduate level of ASEAN in 2015. The 4th ASEAN Conference on Humanities and Social Sciences at Sokha Angkor Resort, Siem Reap, Cambodia on February 12, 2016.

Himma, K. E., & Tavani, H.T. (Eds.). (2008). The Handbook of Information and Computer Ethics. NJ: John Wiley and Sons. Indian Computer Emergency Response Team (CERT-In). Annual Report. Retrieved June 6, 2016, from http://www.cert-in.org.in/Internet Live Stats.

India Internet Users. (2016). Retrieved December 12, 2016, from http://www.internetlivestats.com/internet-users/india/

ITU. (2015). ICT Development Index (IDI). Retrieved December 24, 2015, from http://www.itu.int/net4/ITU-D/idi/2015/

Kalam, A., & Rajan, Y. S. (1998). *INDIA 2020: A Vision for the New Millennium*. New Delhi, India: Penguin Books India Pvt Ltd.

Laudon, K. C., & Laudon, J.P. (2016). Management Information Systems: Managing the Digital Firm. Essex: Pearson Education.

Marakas, G. M., & O'Brien, J.A. (2014). Introduction to Information Systems Singapore. McGraw-Hill Education.

MICT of Thailand Statistics. (2016). Retrieved June 6, 2016, from https://www.thaicert.or.th/statistics/statistics-en.html

Nedeltchev, P., Gopalratnam, V. C, & Tirumala, S. (2015). Opportunities for India in the Digital Economy: Strategic Internet of Everything-based opportunities abound in the public and private sectors. Retrieved June 6, 2016, from http://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/t-en-06032015-opportunities-india-digital.pdf

Oz, E. (2009). Management Information Systems. Boston: Course Technology.

Quinn, M. J. (2012). Ethics for the Information Age. NJ: Pearson Education.

_____ (2015). Ethics for the Information Age. NJ: Pearson Education.

Richmond, S., Bonetto, C., Brash, C., Brown, J.S., Bush, A., Karlin, A., & Robinson, D. (2013). Discover Malaysia & Singapore: Experience the best of Malaysia & Singapore. China: Lonely Planet Publications Pty Ltd.

Rowntree, D. (2000). Statistics without tears. London: Penguin Books.

Rumsey, D. (2011). Statistics for dummies. Indianapolis, IN: John Wiley and Sons.

Tapscott, D. (2015). The Digital Economy: Rethinking Promise and Peril in the Age of Networked Intelligence. New York, N.Y.: McGraw-Hill.

Valacich, J., & Schneider, C. (2014). Information Systems Today: Managing in the Digital World. Essex: Pearson Education.

Webometrics. (2016). Ranking of Asia/Pacifico 2015. Retrieved January 1, 2016, from http://www.webometrics.info/en/asia_pacificoWhitman, M. E. & Mattord, H.J. (2003). Principles of Information Security. MA: Thomson Course Technology.

Whitman, M. E., & Mattord, H. J. (2008). Management of Information Security. MA: Thomson Course Technology.

Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security. CHINA: Course Technology.

World Bank. India (2016a). Retrieved June 6, 2016, from http://data.worldbank.org/country/india

World Bank. Thailand (2016b). Retrieved June 6, 2016, from https://data.worldbank.org/country/thailand