Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory

Nuttapol Assarut[1], Piyabutr Bunaramrueang[2] & Patanaporn Kowpatanakit[3]
Chulalongkorn University, Thailand

Abstract

Space Transition Theory is one of the key theories that explain why people commit cyber crime. However, past research in the field has mainly used qualitative research methods. This is because there has been a lack of quantitative tools to measure the concept in a large-scale survey. This research proposes a measurement of attitudes towards cyberspace based on Space Transition Theory. The analysis results identify the three factors in attitudes towards cyberspace, namely anonymity, freedom and insecurity, which are then used to classify 487 Thai respondents into five groups. The socio-demographic profiles and the tendency to commit crime-related behaviours in cyberspace compared to physical space are explored for each group. We find that freedom and anonymity are key factors in the behavioural intention to commit cyber crime. The results help us identify people who have the greatest tendency to commit cyber crime. This allows us to make recommendations for law amendments and prosecution improvements.

Keywords: Cyber Crime, Cyberspace, Quantitative Approach, Space Transition Theory, Tendency to commit Cyber Crime.

Introduction

The emergence of the Internet has changed the way people connect to another. Along with advances in hardware communication technologies, people can connect to the Internet using several methods, such as desktop computers, laptop computers, mobile devices (i.e., smart phones and tablets), and smart devices (i.e., smart TVs and other household appliances). This helps people connect to the Internet from anywhere and anytime—and creates a ubiquitous society—which increases the frequency and time that people spend online on the Internet (Tan & Wang, 2010).

[1] Associate Professor, Marketing Department, Chulalongkorn Business School, Chulalongkorn University, Phyathai Road, Bangkok 10330, Thailand. Email: nuttapol@cbs.chula.ac.th
[2] Assistant Professor, Faculty of Law, Chulalongkorn University, Phyathai Road, Bangkok 10330, Thailand. Email: piyabutr.b@chula.ac.th
[3] Assistant Professor, Faculty of Law, Chulalongkorn University, Phyathai Road, Bangkok 10330, Thailand. Email: patanaporn.k@chula.ac.th

In the beginning, the Internet was used in the workplace. However, in the last decade, the rise of social networks has made people engage more on the Internet on various platform, e.g., web boards, blogs, MSN, Line, Facebook, Instagram, YouTube. The Internet is no longer a platform for work but has become a part of people's lifestyle (Antoci, Sabatini, & Sodini, 2014; Goldfarb & Prince, 2008; Kotler, Kartajaya, & Setiawan, 2016; Van Deursen, van Dijk, & Peter, 2015). It is a new world called the cyber world or cyberspace. We are now not able to deny that the Internet has become a necessity in our life, whether work life or private life. The population in cyberspace has dramatically increased in the past few years, especially on social network platforms, where the monthly number of Facebook active users has reached 2.07 billion in the third quarter of 2017. The number is more than the population of a small country (Statista, 2018)

When people connect to the Internet from any device almost all the time, their social identity, social interaction, and relationship formation may be different on the Internet than in real life (Mckenna & Bargh, 2000, p. 57). The impact of the Internet is so enormous that researchers have tried to investigate the many aspects of the phenomenon. In most fields of study, one key factor that is a concern is the attitude towards the Internet; in this study, this is called attitudes towards cyberspace.

Past research has found that people's attitude towards cyberspace influence their online behaviours. The attitude has been indicated to be a predictor of Internet usage (Chang, Tsai, & Chiu, 2015; Eastman & Iyer, 2004; Jackson et al., 2003; Porter & Donthu, 2006; Teo, Lee, & Chai, 2008). The attitude has an impact on the frequency, purpose, and usage of the Internet after adoption (Cheung & Huang, 2005; Duggan, Hess, Morgan, Kim, & Wilson, 2001), and on Internet addiction behaviour (Chou, Chou, & Chen 2016; Tsai & Lin 2001), and social and security behaviour (Chou et al., 2016). However, the studies have attempted to investigate the impact of attitudes towards cyberspace in the context of technology adoption, marketing or education research. The dimensions of attitudes examined in the studies were related to the ease of usage or the benefits that people derived from using the Internet.

For example, Tsai and Lin (2004) proposed a 4-T model, including technology as an improvement of life, tool for information acquisition and communication, a toy for pleasure, and a tour/travel to navigate and open up to the world. The model was later modified due to the rise of Web 2.0 and e-commerce platforms to include space for self-expression and trade (Chou et al., 2016; Chou, Wu, & Chen, 2011, 2013; Chou, Yu, Chen, & Wu, 2009). Another example is the attitude scale that was developed by Dutton and Blank (2013) in the Oxford Internet Survey (OxIS) project, which consisted of 14 questions that were classified into four dimensions, i.e., enjoyable escape, instrumental efficiency, problem generator, and social facilitator (Dutton & Blank, 2013, 2015). Moreover, Liaw (2002) developed a scale to measure attitudes towards computers and the World Wide Web based on a computer attitudes scale (Al-Khaldi & Al-Jabri, 1998; Nash & Moroz, 1997) and a technology acceptance model (Davis, Bagozzi, & Warshaw, 1989; Fenech, 1998; Moon & Kim, 2001). The scale was further validated by Bras and Miranda (2013), who confirmed that the scale is composed of three dimensions, i.e., confidence about information and communication technology (ICT, learning through ICT, and talking about ICT.

On the other hand, in criminological research, researchers have tried to investigate the reasons for why people conduct cyber crime. Jaishankar (2007, 2008) proposed space transition theory that explains the characteristics of cyberspace that affect people's

tendency to conduct cyber crime. It was found that people are varied in their attitudes towards cyberspace and online behaviours due to their socio-economic background and past experiences (Chou et al., 2016). Thus, the characteristics of cyberspace discussed in space transition theory would be perceived differently by people with different backgrounds and thus affect the tendency to conduct cyber crime. However, only a limited number of quantitative studies applying space transition theory in a large-scale survey exist. This is due to the lack of a quantitative scale to measure people's attitudes towards cyberspace in terms of cyberspace characteristics.

While existing measurements of attitudes towards cyberspace are related to the benefits of the Internet, this study aims to develop a measurement of attitudes towards cyberspace based on assumptions about the characteristics of cyberspace in space transition theory. Then, by applying the measurement in a large-scale survey, this study also investigates the impact of attitudes towards cyberspace on people's tendency to conduct several types of cyber crime.

This study is an interdisciplinary study in criminology and marketing research. We applied cluster analysis in the data analysis—a quantitative research technique widely used in marketing research (Dutton & Blank, 2015; Eiamkanchanalai & Assarut, 2016; Srisuphaolarn & Assarut, 2017). The respondents were classified into groups according to their attitudes towards cyberspace. Then, the socio-economic profiles and the tendency to conduct cyber crime of each group were analysed. The analysis results can identify people who have a high tendency to conduct cyber crime and guide policy makers to launch campaigns to protect people from conducting cyber crime.

Literature Review

In the field of criminology, there are several theories explaining why people conduct crime, namely, routine activities theory (Cohen & Felson, 1979), self-control theory (Gottfredson & Hirschi, 1990), social learning theory (Akers, 1998), and techniques of neutralization (Sykes & Matza, 1957). The growing number of cyber crimes has made researchers apply traditional criminology theory to explain the phenomenon (Morris, 2011; Ngo & Paternoster, 2011; Pratt, Holtfreter & Reisig, 2010). Holt and Bossler (2008) have explained the possibility of applying Cohen & Felson's (1979) routine activity theory to cyber crime victimization. However, Yar (2005) have suggested that the theory may not be applicable to all cyber cases.

Jaishankar (2007, 2008) has propounded the space transition theory—an essential theory that explains the antecedents of cyber crime behaviour. The theory suggests that people behave differently when they move from one space to another. In other words, according to the theory, people behave differently in physical space and cyberspace. The assumptions of the theory are as follows:

1. Persons with repressed criminal behaviour (in the physical space) have a propensity to commit crime in the cyberspace, which they could otherwise not commit in physical space due to their status and position.
2. Identity flexibility, dissociative anonymity and lack of deterrence factors in the cyberspace provide the offenders with the choice to commit cyber crime
3. The criminal behaviour of offenders in cyberspace is likely to be imported into physical space, which may then be exported to cyberspace as well.

4. The intermittent ventures of offenders into cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.
5. a. Strangers are likely to unite together in cyberspace to commit crime in the physical space.
   b. Associates in physical space are likely to unite to commit crime in cyberspace.
6. Persons from a closed society are more likely to commit crimes in cyberspace than persons from an open society.
7. The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cyber crimes.

According to the assumptions of the space transition theory, it can be concluded that the characteristics of cyberspace that affect cyber crime behaviour are status and position, identity flexibility and anonymity, spatio-temporal nature, conflict of norms, deterrence factors, open or closed society and physical or cyber world associates. The theory is a novel theory applied to explain cyber crime behaviour in various studies (Danqua & Longe, 2011; Diamond & Bachmann, 2015; Holt & Bossler, 2016; Holt, Bossler, & Spellar, 2015; Moore, 2012, Wada, Longe, & Danquah, 2012).

The theory is consistent with past research in criminology; for example, Arbak (2005) remarked that online users who commit crime are usually concerned about their social status in the physical world but are not bothered about their status in cyberspace because there is no one to watch and stigmatize them. Later studies have confirmed the assumptions of space transition theory. Danquah and Longe (2011) found that most cyber crimes in Ghana were cyber-deception crimes, with some positive and negative relationships between physical space and cyberspace. Wall (2011) explained that compared to traditional crimes, it is much more difficult to identify and apprehend cyber criminals because they can use technology to conceal their identities and physical locations.

However, the studies on space transition theory have been mostly qualitative (Akanle, Adesina, & Akarah, 2016; Danquah & Longe, 2011; Kethineni, Cao, & Dodge, 2018; Tade, 2013). The scope of these studies has been limited to cyber criminals, which may not represent the behaviour of the general public. The current study attempts to investigate the tendency to conduct cyber crime among the general public. In this case, a quantitative survey is needed. Thus, based on the assumptions of space transition theory, this study develops a measurement scale to quantitatively investigate attitudes towards cyberspace and to analyse the tendency to conduct cyber crime among people who perceive cyberspace in different ways.

Methodology

1. Sample

Thailand is the case study in this research. The country has enacted its Computer Crime Act (CCA) B.E.2550 (2007). The law includes all kinds of computer crimes and imposes strong punishments, with sentences of up to 20 years. However, the number of computer crimes has continued to increase. The wrongdoings have been developed with the latest technologies. The law is losing its grip on technological changes and social media.

This study conducted a survey on attitudes towards cyberspace among Thai citizens. The 487 respondents in this study were Thai people aged 15-60 years old. The entire

sample must have had experience using and accessing the Internet on a regular basis. The questionnaires were distributed among proper proportions of age groups (15-24, 25-34, 35-44, and more than 45 years old) and gender (male and female) to avoid the biasing of results that could occur based on the respondents' characteristics (see Table 1).

2. Data Collection

A self-administered questionnaire was used as the data collection method. The questionnaire consisted of four parts. First, the respondents answered questions regarding their Internet behaviour, including their frequency of usage and the access method (personal computer, tablet, or smartphone).

Then, in the second part, the respondents rated the frequency of doing 15 particular activities in online and offline situations using a four-point scale (1= never done, 2 = used to do it in the past, 3 = do it sometimes, 4 = usually do it). The activities covered the four types of crime behaviours (Wall, 2001; Yar, 2005), including the following:

1) Cyber-trespassing: This is a *violation and invasion behaviour* that involves crossing boundaries into other people's property and/or causing damage, e.g., hacking, defacement and viruses.
2) Cyber-deception and theft: This is a *deception and fraud behaviour* that involves stealing (money, property), e.g., credit card fraud, intellectual property violation, piracy.
3) Cyber-pornography: This is an *obscene behaviour*, including activities that breach laws on obscenity and indecency.
4) Cyber violence: This a *violent and defamation behaviour* that involves causing psychological harm to others or inciting physical harm against others, thereby breaching laws pertaining to the protection of persons, e.g., hate speech.

After that, the respondents rated their attitudes towards the online world on a five-point Likert scale. The 13 questions measuring respondents' attitudes towards the online world were extracted from the assumptions of the space transition theory by Jaishankar (2007, 2008) and the qualitative works of Danquah and Longe (2011). Finally, the respondents answered questions about their socio-demographic profiles (gender, age, occupation, income).

Results

Table 1 and Table 2 present the respondents' profiles and Internet usage behaviours. According to Table 1, the respondents were collected with a good proportion of gender and age groups, as indicated in the methodology. The majority of the respondents connected to the Internet using mobile phones, with a duration of usage of 4-6 hours per day (n = 190; 40%) or 1-3 hours per day (n = 120; 40%). It is clear that personal computers were not the major way that people connect to the Internet and that tablet usage was still in the introduction stage of the market.

Table 1. Respondents' Profiles

	Male	Female	Total
15-24 years old	62	61	123
25-34 years old	62	59	121
35-44 years old	61	59	120
>= 45 years old	49	74	123
Total	234	253	487

Table 2. Internet Connection Device and Usage

	Personal Computer	Mobile Phone	Tablet
Never or Rarely	110	25	351
1-3 hours / day	146	120	96
4-6 hours / day	119	190	23
7-9 hours / day	88	92	13
More than 10 hours / day	24	60	4
Total	487	487	487

1. Attitudes towards Cyberspace

The 13 questions measuring attitudes towards the cyber world were analysed using principal component analysis with varimax rotation to identify the construct of the measurement as well as the scale reliability and validity.

The analysis results suggested the three components of attitudes towards cyberspace. They were anonymity, freedom, and insecurity. The Kaiser-Meyer-Olkin (KMO) index of analysis was .878. The communality of all questions was greater than .400, and the factor loadings were above .500. Moreover, the Cronbach's alpha coefficients of the three components were .546-.849. All the indices suggested the acceptable validity and reliability of the measurement.

Considering the questions in the three components, the anonymity component means that people are not identified in cyberspace. They do not feel peer pressure, do not need to care about relationships and can easily control what happens. The freedom component means that people think that no one knows them in cyberspace, so that they can do anything that they cannot do in physical space; they do not need to concern themselves about their role and status. The last component is insecurity, which means that cyberspace is not secure. A person can easily find a friend but he or she may not be trustworthy.

Table 3. Principal Component Analysis of the Attitudes towards Cyberspace Measurement

	Mean	Factor Loadings			Communalities Extraction
		F1	F2	F3	
F1: Anonymity					
ST12 I do not need to think much about anything online.	2.99	**.783**	.217	.092	.669
ST13 It is easy to control things that could happen in cyberspace.	2.94	**.763**	.166	-.075	.615
ST10 I do not have to worry about relationships between people.	3.18	**.762**	.272	.070	.659
ST09 I am not able to identify people in cyberspace.	3.23	**.674**	.250	.236	.573
ST08 There is no pressure from people around in the cyberspace.	3.34	**.622**	.398	.081	.552
ST11 I do not need to know anyone in cyberspace.	3.35	**.594**	-.043	.479	.583
F2: Freedom					
ST01 There is more freedom and I am able to be myself in cyberspace.	3.53	.018	**.829**	.092	.695
ST02 There is no need to worry about acting according to social status.	3.24	.365	**.758**	-.012	.708
ST03 Nobody knows us very well.	3.20	.393	**.637**	.095	.569
ST05 I can do many things in cyberspace that I cannot do in physical space.	3.64	.314	**.514**	.352	.486
F3: Insecurity					
ST06 People you know in cyberspace are unfaithful.	3.73	.230	-.033	**.773**	.651
ST04 The online world is dangerous.	3.49	-.276	.169	**.735**	.645
ST07 It is easy to find friends online.	3.67	.294	.344	**.503**	.458
Rotation Sums of Squared Loadings		3.572	2.450	1.842	-
% of Variance		27.476	18.847	14.168	60.491
Cronbach's Alpha Coefficients		0.849	0.764	0.546	0.860

2. Clustering the Cyberspace Population

Though there were three components of attitudes towards cyberspace, the differences in people's backgrounds and experiences in cyberspace made them perceive cyberspace differently. This study performed a further analysis by clustering the respondents into several groups according to their attitudes towards cyberspace.

The average score of each attitude component was calculated into a standardized score and applied in K-mean cluster analysis. The results suggested classifying the respondents into five clusters (Table 4). Furthermore, the profiles and Internet usage behaviours of each cluster are shown in Table 5 and Table 6, respectively.

Table 4. Results of Cluster Analysis

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5
Anonymity	.394	-.841	.531	1.895	-.863
Freedom	-.587	-.789	.872	1.399	.548
Insecurity	-.318	1.270	.965	-1.578	-.580
Count (n = 487)	204	57	89	14	123
Proportion	42%	12%	18%	3%	25%

3. Tendency to Conduct Cybercrime of the Five Clusters

The last analysis was to investigate the tendency to conduct cybercrime of each cluster compared to the behaviour in physical space. The 15 questions in Table 7 represented the four types of crime behaviours, including violation and invasion behaviour, deception and fraud behaviour, obscene behaviour, and violent and defamation behaviour. The respondents rated the frequency with which they conducted the behaviours on a four-point Likert scale Thus, in this study, an average score that was higher than 3.0 implied that the respondents had a high frequency of doing the behaviour, while a 2.0-2.9 score implied moderate behaviour, and less than 2.0 indicated a low frequency of the behaviour.

Table 5. Gender, Age, and Education of the Five Clusters (Percentage within Cluster)

		Male				Female				Total
		15-24	25-34	35-44	>= 45	15-24	25-34	35-44	>= 45	
Cluster 1 (n= 204)	< Bachelor	1.00%	3.00%	2.50%	3.90%	4.90%	3.00%	3.40%	3.00%	24.70%
	Bachelor	3.00%	7.40%	6.40%	6.40%	6.40%	4.40%	6.90%	23.30%	64.20%
	> Bachelor	0.00%	3.00%	2.00%	0.50%	1.00%	2.00%	1.50%	1.50%	11.50%
	Total	**3.90%**	**13.30%**	**10.80%**	**10.80%**	**12.30%**	**9.40%**	**11.80%**	**27.70%**	100.00%
Cluster 2 (n= 57)	< Bachelor	1.80%	0.00%	0.00%	0.00%	5.30%	0.00%	0.00%	3.50%	10.60%
	Bachelor	15.80%	0.00%	7.00%	1.80%	22.90%	7.00%	7.00%	3.50%	65.00%
	> Bachelor	0.00%	3.50%	3.50%	7.00%	1.80%	0.00%	7.00%	1.80%	24.60%
	Total	**17.50%**	**3.50%**	**10.50%**	**8.80%**	**29.90%**	**7.00%**	**14.00%**	**8.80%**	100.00%
Cluster 3 (n= 89)	< Bachelor	4.50%	0.00%	6.80%	1.10%	2.30%	4.50%	9.10%	2.30%	30.60%
	Bachelor	9.10%	3.40%	11.50%	10.20%	2.30%	6.80%	5.70%	3.40%	52.40%
	> Bachelor	0.00%	9.10%	3.40%	1.10%	0.00%	0.00%	2.30%	1.10%	17.00%
	Total	**13.60%**	**12.50%**	**21.70%**	**12.50%**	**4.50%**	**11.40%**	**17.00%**	**6.80%**	100.00%
Cluster 4 (n= 14)	< Bachelor	21.40%	0.00%	0.00%	0.00%	14.30%	0.00%	0.00%	0.00%	35.70%
	Bachelor	0.00%	21.40%	7.10%	0.00%	0.00%	0.00%	14.30%	0.00%	42.80%
	> Bachelor	0.00%	14.30%	7.10%	0.00%	0.00%	0.00%	0.00%	0.00%	21.40%
	Total	**21.40%**	**35.70%**	**14.30%**	**0.00%**	**14.30%**	**0.00%**	**14.30%**	**0.00%**	100.00%
Cluster 5 (n= 123)	< Bachelor	2.40%	1.60%	0.80%	0.00%	0.80%	0.80%	0.80%	0.80%	8.00%
	Bachelor	21.10%	6.50%	8.10%	4.90%	7.30%	16.30%	7.30%	4.90%	76.40%
	> Bachelor	0.00%	5.70%	0.80%	2.40%	2.40%	4.10%	0.00%	0.00%	15.40%
	Total	**23.60%**	**13.80%**	**9.80%**	**7.30%**	**10.60%**	**21.10%**	**8.10%**	**5.70%**	100.00%

Table 6. The Internet Usage Behaviours of the Five Clusters

	Cluster 1		Cluster 2		Cluster 3		Cluster 4		Cluster 5		Total	
	n	%	n	%	n	%	N	%	n	%	n	%
Personal Computer												
Never or Rarely	58	28%	14	25%	17	19%	1	7%	20	16%	111	23%
1-3 hours / day	66	32%	18	32%	22	25%	1	7%	39	32%	147	30%
4-6 hours / day	46	23%	14	25%	19	21%	2	14%	38	31%	120	25%
7-9 hours / day	27	13%	9	16%	24	27%	8	57%	20	16%	89	18%
>=10 hours / day	7	3%	2	4%	7	8%	2	14%	6	5%	24	5%
Mobile Phone												
Never or Rarely	16	8%	2	4%	4	4%	1	7%	2	2%	25	5%
1-3 hours / day	52	25%	6	11%	26	29%	0	0%	36	29%	121	25%
4-6 hours / day	85	42%	26	46%	29	33%	1	7%	49	40%	191	39%
7-9 hours / day	36	18%	11	19%	17	19%	2	14%	26	21%	93	19%
>=10 hours / day	15	7%	12	21%	13	15%	10	71%	10	8%	61	13%
Tablet												
Never or Rarely	158	77%	41	72%	53	60%	5	36%	94	76%	353	73%
1-3 hours / day	36	18%	11	19%	23	26%	4	29%	22	18%	97	20%
4-6 hours / day	6	3%	1	2%	9	10%	1	7%	6	5%	23	5%
7-9 hours / day	3	1%	3	5%	4	4%	3	21%	0	0%	13	3%
>=10 hours / day	1	0%	1	2%	0	0%	1	7%	1	1%	4	1%

Table 7. Behaviour of the Five Clusters in Cyber Space and Physical Space

	Cyber Space Behaviour					Physical Space Behaviour					Difference Score (Cyberspace – Physical space)				
	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5					
Violation and Invasion Behaviour															
01 Purchasing or acquiring pirated software	2.162	2.474	2.404	3.500	2.276	2.078	1.895	2.213	3.643	2.008	0.1	0.6	0.2	-0.1	0.3
02 Purchasing or acquiring pirated music	2.431	2.877	2.663	3.500	2.732	2.270	2.228	2.506	3.643	2.341	0.2	0.6	0.2	-0.1	0.4
03 Purchasing or acquiring pirated films	2.412	2.667	2.640	3.714	2.626	2.309	2.228	2.528	3.786	2.293	0.1	0.4	0.1	-0.1	0.3
Deception and Fraud Behaviour															
04 Providing false personal information to others	2.172	2.351	2.584	3.714	2.146	1.887	1.789	2.112	2.286	1.756	0.3	0.6	0.5	1.4	0.4
05 Filling in false personal information on forms	2.093	2.088	2.303	3.500	1.878	1.794	1.596	1.820	1.857	1.423	0.3	0.5	0.5	1.6	0.5
06 Obtaining access to information, documents or letters of other people without them knowing	1.775	1.579	1.730	3.214	1.610	1.652	1.386	1.584	1.929	1.382	0.1	0.2	0.1	1.3	0.2
07 Using texts or content without reference to the source	1.784	2.123	1.944	3.429	1.951	1.632	2.018	1.640	2.786	1.553	0.2	0.1	0.3	0.6	0.4
Obscene behaviour															
08 Watching pornographic pictures or movies	1.985	2.351	2.483	3.643	2.285	1.877	1.544	2.169	3.357	1.967	0.1	0.8	0.3	0.3	0.3
09 Buying pornographic pictures or movies	1.407	1.211	1.798	3.143	1.390	1.338	1.175	1.730	2.786	1.333	0.1	0.0	0.1	0.4	0.1
10 Directing or guiding friends to porn sellers	1.343	1.158	1.899	3.286	1.276	1.348	1.193	1.854	3.286	1.285	0.0	0.0	0.0	0.0	0.0
Violent and Defamation Behaviour															
11 Embarrassing someone so that they are ashamed	1.402	1.474	1.618	3.500	1.301	1.397	1.456	1.562	3.143	1.333	0.0	0.0	0.1	0.4	0.0
12 Being embarrassed and feeling ashamed	1.377	1.579	1.697	3.357	1.325	1.485	1.596	1.573	3.214	1.382	-0.1	0.0	0.1	0.1	-0.1
13 Spreading personal negative narratives of others	1.407	1.614	1.674	3.286	1.309	1.544	1.930	1.730	3.000	1.520	-0.1	-0.3	-0.1	0.3	-0.2
14 Spreading personal negative narratives of the king	1.216	1.158	1.472	2.357	1.163	1.289	1.421	1.461	2.357	1.317	-0.1	-0.3	0.0	0.0	-0.2
15 Expressing political views through various media	1.559	1.912	2.056	3.000	1.610	1.569	1.877	1.910	3.214	1.553	0.0	0.0	0.1	-0.2	0.1

Discussion

1. Overall Behaviours in Cyberspace and Physical Space

Focusing on the difference score between cyberspace and physical space, overall, the respondents in all clusters have a higher tendency to conduct the behaviours in cyberspace than in physical space, except for violent and defamation behaviours, which the respondents tend to do more in physical space. The results support the assumption of space transition theory that people tend to conduct crime in cyberspace more than in physical space. This may be due to the nature of cyberspace, which is characterized by freedom and anonymity (Jaishankar, 2007, 2008).

Violation and invasion behaviour, which were related to consuming and purchasing pirated software, were the behaviours exhibited by all clusters. This implies that pirated software is still a major problem in Thailand, which most people are still not concerned about.

Similarly, two behaviours in deception and fraud behaviours, i.e., *Providing false personal information to others (04)* and *Filling in false personal information on forms (05),* were the behaviours that the clusters conducted the most. This also implies that people are still concerned about providing their private information in cyberspace.

Furthermore, *Watching pornographic pictures or movies (08)* is another behaviour that most clusters conducted, except for cluster 1, in which the majority of respondents were female and aged more than 45 years old. Though this behaviour is not a crime behaviour

according to Thai law, it is a risky behaviour that motivates the selling of pornographic pictures and movies, which violates the cyber law of Thailand.

With regard to violent and defamatory behaviours, it was found that the respondents engage in these behaviours more in physical space than in cyberspace. This may be because the evidence on these actions taking place is as clear as in cyberspace as it is in physical space.

2. Characteristics and Behaviours of the Five Clusters

According to Tables 4 to 7, the characteristics of the five clusters as well as their behaviours can be summarized as follows:

Cluster 1 is the largest cluster, consisting of 204 respondents (42%). They thought that there is no freedom in cyberspace (mean = -.587) but that it is anonymous (mean = .394) and secure (mean = -.318) (Table 4). The majority of them were females aged more than 45 years with a bachelor-degree education (23.2% of the group size) (Table 5). The respondents in this group were low to moderate users of the Internet. The majority of them connected to the Internet for less than three hours per day via a personal computer or tablet and for 1-3 hours to 4-6 hours per day via a mobile phone (Table 6). Though the respondents in this cluster thought that cyber space is anonymous and free, they still had a lower tendency to conduct behaviours related to cyber crimes compared to other clusters (Table 7). This may be because of their socio-demographic profile, which is female aged over 45 years old with high education.

Cluster 2 consisted of 57 respondents (12%) who were relatively conservative and risk averse in cyberspace. They thought that the cyberspace is insecure (mean = 1.270), that it is not anonymous (mean = -.841) and that there is no freedom (mean = -.789) (Table 4). Most of them were females and males aged 15-24 years old with bachelor's degree (female = 22.8%, male = 15.8%) (Table 5). They were moderate users of the Internet by connecting via a personal computer for 1-3 hours per day and for 4-6 hours per day via a mobile phone (Table 6). This cluster seems to have clear attitudes towards cyberspace, which is not anonymous, not free, and insecure. However, in addition to the basic behaviours that most of the clusters engaged in, the respondents in cluster 2 also tended to *copy another user's message without reference to the source (07)* and to *view pornographic pictures or movies (08)* (Table 7). This may be because they were of the younger generation and were not educated about copyrights and citation requirements.

Cluster 3 was the third largest group, with 89 respondents (18%). In their opinion, the cyberspace is insecure (mean = .965) but full of freedom (mean = .872) and anonymous (mean = .531) (Table 4). The respondents were relatively more mature than the other groups and were aged 35-44 years (male = 21.6%, female = 17.0%) (Table 5). They varied in their Internet usage behaviour (Table 6). Respondents in this cluster thought that cyberspace is insecure but still provides freedom and anonymity. Thus, they still *view pornographic pictures or movies (08)* and *post political opinions through various media (15)*. This may be because of the majority of this cluster is aged 35-44, which is the age range that is the most engaged in political issues.

Cluster 4 was the smallest group and consisted of 14 respondents (3%). They thought that the cyberspace is anonymous (mean = 1.895), secure (mean =-1.587) and full of freedom (mean = 1.399). They seemed unaware of the dangers in cyberspace (Table 4). The majority of the respondents in this group were males aged less than 35 years old with an education level lower than a bachelor's degree (57.1%) (Table 5). The group members

were heavy users of the Internet. They connected to the Internet via a personal computer for 7-9 hours per day and for more than 10 hours per day with a mobile phone (Table 6). Respondents in this cluster tended to engage in all of the behaviours related to crimes both in cyberspace and physical space (Table 7). This may be because the majority of the respondents were young males who had low education, which made them think that the cyberspace is anonymous, secure, and full of freedom.

Cluster 5 was the second largest group (n = 123; 25%), and the respondents thought that the cyberspace is not anonymous (mean = -.863) but that it is secure (mean = -.580) and full of freedom (mean = .548) (Table 4). The majority of the group were males aged less than 25 years old with a bachelor's degree (23.6%) and females aged 25-35 years old with a bachelor's degree (16.3%) (Table 5). They were rather high on their Internet usage, i.e., 1-3 hours or 4-6 hours per day with a personal computer and 4-6 hours per day with a mobile phone (Table 6). In addition to the basic behaviour that most clusters engaged in, such as violating software, providing untrue personal information, and viewing pornographic pictures and movies, the respondents in this cluster did not conduct any other crime-related behaviour.

Conclusion

This study, based on space transition theory (Jaishankar, 2007, 2008), developed a measurement scale to quantitatively gauge people's attitudes towards cyberspace. The scale provides a great opportunity to quantitatively conduct research related to cyberspace behaviour in a large-scale survey.

Using statistical techniques, the study was able to classify respondents into five clusters according to their attitudes towards cyberspace. The characteristics and crime behaviours of each cluster were also further investigated, and it was found that the key factors that lead people to conduct cyber crime are as follows:

1. *Social norms:* common behaviours that most people do make people overlook the fact that the behaviours are illegal. Even if they know this, they may think that the behaviour is not a severe violation: for example, infringing software copyrights, providing untrue information, or viewing pornographic pictures or movies.
2. *Demographic profiles:* females who are of higher age and who have higher education tend to conduct less crime-related behaviours than other groups, such as cluster 1.
3. *Attitudes towards cyberspace:* those who think that cyberspace is anonymous, free, and secure (Cluster 4) seem to conduct cyber crime-related behaviours more than other groups. The second riskiest group is Cluster 3, which thought that cyberspace is anonymous and free but insecure. This implies that the security of cyberspace is not the most important characteristic of cyberspace that leads people to conduct cyber crime. The key factors are anonymity and freedom.

The analysis results can help identify the groups of people who have a high tendency to conduct cyber crimes. It is shown statistically that attitudes towards cyberspace are major factors in cyber crimes, especially the attitudes regarding anonymity and freedom. Speaking of anonymity and freedom, it is not new to point them out as major attitudinal factors in people's commitment of cyber crimes. Recent developments such as fake news and real-name systems help emphasize that we need to counter the false attitudes of anonymity and freedom. However, many people are still unaware that anonymity is shrinking. Policy makers can then customize their strategy to prevent cyber crimes,

especially by addressing anonymity and freedom to fit each cluster, which will be a more effective way to prevent cyber crime. Cyberspace should be a communication channel for all, not the other space for us to live parallel lives in.

Acknowledgements

This study was supported by Rabi Bhadanasak Research and Development Institute, Office of Judiciary, Thailand. We sincerely thank the Editor-in-Chief of IJCC and the anonymous reviewers for their valuable comments and feedback.

References

Akanle, O., Adesina, J. O., & Akarah, E. P. (2016). Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria. *African Journal of Science, Technology, Innovation and Development*, *8*(2), 213-220.

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.

Al-Khaldi, M. A., & Al-Jabri, I. M. (1998). The relationship of attitudes to computer utilization: New evidence from a developing nation. *Computers in Human Behavior*, *14*(1), 23-42.

Antoci, A., Sabatini, F., & Sodini, M. (2014). Bowling alone but tweeting together: the evolution of human interaction in the social networking era. *Quality & Quantity, 48*(4), 1911-1927.

Arbak, E. (2005) Social Status and Crime. *GATE Working Paper No. W.P.05-10*. Available at SSRN: https://ssrn.com/abstract=906771

Bras, P., & Miranda, G. L. (2013). Validation of Liaw's attitude questionnaire: A study with Portuguese teachers. In *Information Systems and Technologies (CISTI), 2013 8th Iberian Conference on* (pp. 1-6). IEEE.

Chang, Y. C., Tsai, C. L., & Chiu, W. Y. (2015). The influence of life satisfaction and well-being on attitude toward the internet, motivation for internet usage and internet usage behavior. *Journal of Interdisciplinary Mathematics*, *18*(6), 927-946.

Cheung, W., & Huang, W. (2005). Proposing a framework to assess Internet usage in university education: an empirical investigation from a student's perspective. *British Journal of Educational Technology*, *36*(2), 237-253.

Chou, H. L., Chou, C., & Chen, C. H. (2016). The moderating effects of parenting styles on the relation between the internet attitudes and internet behaviors of high-school students in Taiwan. *Computers & Education*, *94*, 204-214.

Chou, C., Wu, H. C., & Chen, C. H. (2011). Re-visiting college students' attitudes toward the Internet-based on a 6-T model: Gender and grade level difference. *Computers & Education*, *56*(4), 939-947.

Chou, C., Wu, H. C., & Chen, C. H. (2013). Tool, toy, telephone, territory, trade, or treasure of information: a cross-sectional study of Taiwanese students' attitudes toward the Internet. *Chinese Journal of Communication*, *6*(2), 202-220.

Chou, C., Yu, S. C., Chen, C. H., & Wu, H. C. (2009). Tool, toy, telephone, territory, or treasure of information: Elementary school students' attitudes toward the Internet. *Computers & Education*, *53*(2), 308-316.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608.

Danquah, P., & Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. *African Journal of Computing & ICTs, 4*(2), 37-48.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, *35*(8), 982-1003.

Duggan, A., Hess, B., Morgan, D., Kim, S., & Wilson, K. (2001). Measuring students' attitudes toward educational use of the Internet. *Journal of Educational Computing Research, 25*(3), 267-281.

Dutton, W. H., & Blank, G. (2013), *Cultures of the Internet: The Internet in Britain*, Oxford Internet survey 2013 Report. Oxford: Oxford Internet Institute.

Dutton, W. H., & Blank, G. (2015), Cultures on the Internet, *InterMedia, Winter 2014/15, 42*(4/5), 55-57.

Eastman, J. K., & Iyer, R. (2004). The elderly's uses and attitudes towards the Internet. *Journal of Consumer Marketing, 21*(3), 208-220.

Eiamkanchanalai, S., & Assarut, N. (2016). Consumer innovativeness and opinion leadership: revisiting consumer characteristics in new product diffusion model. *Global Business and Economics Review, 18*(1), 15-27.

Fenech, T. (1998). Using perceived ease of use and perceived usefulness to predict acceptance of the World Wide Web. *Computer Networks and ISDN Systems*, *30*(1-7), 629-630.

Goldfarb, A., & Prince, J. (2008). Internet adoption and usage patterns are different: Implications for the digital divide. *Information Economics and Policy, 20*(1), 2-15.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25.

Holt, T., & Bossler, A. M. (2016). *Cyber crime in progress: theory and prevention of technology-enabled offenses*. Abingdon, Oxon: Routledge.

Holt, T., Bossler, A. M., & Spellar, S. K. (2015). *Cyber crime and Digital Forensics*. Abingdon, Oxon: Routledge.

Jackson, L. A., Von Eye, A., Barbatsis, G., Biocca, F., Zhao, Y., & Fitzgerald, H. E. (2003). Internet attitudes and Internet use: Some surprising findings from the HomeNetToo project. *International Journal of Human-Computer Studies*, *59*(3), 355-382.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology, 1*(2), 7-9.

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. *American Journal of Criminal Justice, 43*(2), 141-157.

Kotler, P., Kartajaya, H., & Setiawan, I. (2016). *Marketing 4.0: moving from traditional to digital*. John Wiley & Sons.

Liaw, S. S. (2002). An Internet survey for perceptions of computers and the World Wide Web: relationship, prediction, and difference. *Computers in Human Behavior*, *18*(1), 17-35.

McKenna, K. Y., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. *Personality and Social Psychology Review*, *4*(1), 57-75.

Moon, J. W., & Kim, Y. G. (2001). Extending the TAM for a World-Wide-Web context. *Information & Management*, *38*(4), 217-230.

Moore, R. (2012). *Cyber crime: investigating high-technology computer crime*. Abingdon, Oxon: Routledge.

Morris, R. G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T. J. Holt and B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and Implications* (pp. 1-17). IGI Global: Hershey, PA.

Nash, J. B., & Moroz, P. A. (1997). An examination of the factor structures of the computer attitude scale. *Journal of Educational Computing Research*, *17*(4), 341-356.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*, 773-793.

Porter, C. E., & Donthu, N. (2006). Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of business research*, *59*(9), 999-1007.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*, 267-296.

Srisuphaolarn, P., & Assarut, N. (2017). The Influence of Corporate Social Responsibility on Work Engagement and Organizational Commitment. *Chulalongkorn Business Review, 38*(4), 68-92.

Statista (2018) *Number of monthly active Facebook users worldwide as of 4th quarter 2017* (in millions) Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*, 664-670.

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, *23*(4), 689-705.

Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In 2010 *3rd international conference on advanced computer theory and engineering (ICACTE)*, *5*, V5-376.

Teo, T., Lee, C. B., & Chai, C. S. (2008). Understanding pre - service teachers' computer attitudes: applying and extending the technology acceptance model. *Journal of Computer Assisted Learning*, *24*(2), 128-143.

Tsai, C. C., & Lin, S. S. (2001). Analysis of attitudes toward computer networks and Internet addiction of Taiwanese adolescents. *CyberPsychology & Behavior*, *4*(3), 373-376.

Van Deursen, A. J., van Dijk, J. A., & Peter, M. (2015). Increasing inequalities in what we do online: A longitudinal cross sectional analysis of Internet activities among the

Dutch population (2010 to 2013) over gender, age, education, and income. *Telematics and Informatics, 32*(2), 259-272.

Wada, F., Longe, & O. Danquah (2012). Action Speaks Louder than Words: Understanding Cyber Criminal Behavior Using Criminological Theories. *Journal of Internet Banking and Commerce, 17*(1), 1.

Wall, D. S. (2001). Cyber crimes and the internet. In D. Wall (ed.) *Crime and the Internet* (pp. 1-17). London: Routledge.

Wall, D. S. (2011). Policing Cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research: An International Journal, 8*, 183-205.

Yar, M. (2005). The Novelty of "Cybercrime" An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427.