Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator

Noura Al-Suwaidi[1], **Haitham Nobanee**[2], **& Fauzia Jabeen**[3]
Abu Dhabi University, Abu Dhabi - United Arab Emirates

Abstract

This paper explores cyber crime from different perspectives, providing a deeper analysis of the phenomena itself as more sophisticated technical tools have emerged. Making detection of such methods quite difficult for law enforcement authorities around the globe, since the rise of the deep-web has made the prevention of such crimes is difficult if not impossible. However, the main objective of this paper is to examine the effect of unemployment rates and GDP growth per capita on the level of cyber-attacks in 10 countries (USA, Belgium, the Netherlands, Japan, China, Italy, Spain, India, and Canada) during the period of 2005-2017. In addition, this study seeks to provide insight into what might be the reason behind the fluctuating levels of attacks in these countries. This paper provides different authorities as well as the government with insight into how to take steps forward in preventing and combating these crimes.

Keywords: Cyber crime, Unemployment, GDP growth.

Introduction

Technology has become a powerful and remarkable tool for criminals to use to engage in illicit transnational activities. Criminals have realized the possibilities offered by the cyber landscape and have outpaced expectations, giving rise to a large number of threats by exploiting digital technology to promote their objectives (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014). International and domestic Internet economies are attractive targets for a range of cyber-dependent crimes that are committed through the use of computers or forms of information communication technology; these cyber-enabled crimes include financial fraud, information theft and illicit drug purchases (Cyber Crime Assessment, 2016).

This paper explores cyber crime from different perspectives, moving away from the usual stereotypes revolving around the more typical images of cyber hacking and extortion. Smith (2015) stated "There has been a change in the people who attack computer networks away from the "bragging hacker" towards those driven by monetary motives" (P. 104). A deeper analysis of

[1] Doctoral candidate, College of Business Administration, Abu Dhabi University, Abu Dhabi - United Arab Emirates. Email: 1048112@students.adu.ac.ae
[2] Associate Professor of Finance, College of Business Administration, Abu Dhabi University, Abu Dhabi - United Arab Emirates. Email: haitham.nobanee@adu.ac.ae
[3] Associate Professor of Management, College of Business Administration, Abu Dhabi University, Abu Dhabi - United Arab Emirates. Email: fauzia.jabeen@adu.ac.ae

the phenomena itself has taken place as more sophisticated technical tools have emerged, making the detection of such methods quite difficult for law enforcement authorities around the globe since the rise of the deep web has made the prevention of such crimes difficult if not impossible.

Today, criminals require no special skills to initiate a cyber-attack. Information and communication technology tools are becoming more sophisticated and easier to use, releasing a continuous onslaught of enhanced Trojans, malwares and spywares. What makes this situation more serious is the shadow of the deep web shedding its darkness onto the surface and gaining more popularity among the common population, giving criminals the possibility of "setting things right" with a low probability of being detected.

Interestingly, Broadhurst et al. (2014) argued that the government can use cyberspace to indirectly do what is required by engaging in organized illicit activities, such as the claims about Russia's encouragement of the denial distribution of service attacks, the engagement of the Chinese authorities in widespread economic and industrial espionage, and what Edward Snowden revealed about the US government engaging in massive cyber surveillance programmes, not to mention the cyber operations against Iranian nuclear enrichment facilities (Sanger, 2012). Despite this interesting illumination, the focus of this article is on the criminal groups and the individuals involved in massive cyber illicit activities.

The objective of the current paper is to examine the effect of the unemployment rate and GDP growth per capita on the amount of cyber attacks in 8 countries (UAE, USA, Spain, Italy, Japan, the Netherlands, China, Belgium, India and Canada) during the period of 2000-2017. To achieve this objective, the following research question was addressed:

1. To what degree is the number of cyber attacks affected by a country's unemployment rate and GDP growth per capita?

The main focus of this paper is to provide evidence on how the number of cyber crimes might increase depending on the size of the unemployed population in different countries. In addition, this paper provides insight into what might be the reason behind the fluctuating levels of attacks in these countries. Nevertheless, a short review of cyber crime, its forms and preferred cyberspace is also provided.

Literature Review

Organized Cyber Crime

Literature compiled prior to the recession of 2008 identifies some debate concerning the type of crime existing within the cyber landscape. Questions such as the following: is it actually traditional organized crime online or an online crime that is organized, or both (McCusker, 2006). Furthermore, McCusker (2006) illustrated that the synergy between the Internet and organized crime is a natural tendency and is likely to develop further in the future. The previous focus was on conventional organized crime groups using the Internet as a mediator to commit crimes. The Internet has been used for several years as a primary facilitator for crimes, which does not necessarily make it an inherent part of the illicit act (Lavorgna, 2015). Various forms of cyber crimes require high levels of coordination and organization, and empirical evidence to ascertain whether cyber crime has been taken over by organized crime groups is insufficient (Lusthaus, 2013). There are few studies focusing on the existence of both traditional organized crimes and newly established criminal groups in the cyber landscape (to name a few, Hutchings, 2014; Lavorgna, 2015; Leukfeldt et al., 2016; Lusthaus, 2013), and the existing literature based on criminology has not addressed the nature and the rate of criminal adaptability to a sufficient

degree yet (Lavorgna & Sergi, 2016). Nevertheless, the number of studies and reports from cyber security entities are growing, and these studies show that different organizational structures are involved in cyber crimes, which have expanded the concept of organized cyber crime to cover profit-driven criminal activities occurring fully or partially in the cyber landscape (Broadhurst et al., 2014; Leukfeldt et al., 2016).

McGuire (2012) identified three main types (type I, II, and III) and six subtypes (swarm, hubs, extended hybrids, clustered hybrids, aggregates, and hierarchies) of cyber-organized crime groups and concluded that up to 80% of cyber crime is organized crime. According to McGuire's report, certain key characteristics of traditional organized crime groups need to be reconsidered when groups are operating online. For instance, in cyberspace, the size of a group does not correlate with the impact and scope of their offenses, and many associations are highly transitory. The interpretation offered in the report is that cyberspace has augmented, rather than replaced, existing varieties of organized criminal organizations. To decide whether a certain network of offenders should be labelled organized crime, however, the report examined recurring offending patterns and the scale of activity, they examined the debates around the definitions of organized crime, and they adopted the organized crime umbrella term to include a broad range of groups exhibiting some degree of organization.

Whether a cyber-attack is conducted by an individual or by criminal groups using the Internet as a mediator, new trends have emerged with the increased usage of social media applications. For example, with regard to the current events in the Middle East and the Gulf region, social media has been flooded with fake accounts used mainly by individuals who support terrorism and extremist thoughts. Such applications have been used to air crimes by the criminals themselves with no fear of being known or detected.

Cyber crime and the Deep Web

Cyber criminals are continuously searching for new means to ensure their anonymity while surfing through the cyber landscape. One of the major tools for ensuring such levels of obscurity is by surfing through the deep web. However, what is the deep web? How can it be accessed? What threats and opportunities does it hold for its users? Can it be accessed easily?

The deep web is an underground cyber-culture, unreachable through regular search engines, which contains valuable information that can be widely used for both legitimate and illegitimate purposes. It is characterized by its unknown breadth, depth, content, and users. Within the deep web reside layers of routes and URLs, deeper than one can imagine which are harder to reach and contain more than 80% of what the surface Internet can offer. This platform, called the dark web, contains content that has been intentionally concealed by unknown users. The most dangerous criminals reside here whose crimes are committed online. Online, drugs are being sold, and human trafficking is taking place. Most of the illicit activities of criminal groups and cults are committed without the fear of detection. Thousands of illicit goods and services are being traded through an underground market, and money is being exchanged through an underground banking system in which money cannot be traced. Money usually takes the form of cryptocurrency like Bitcoin, Dark-coin, Peer-coin (Sui, Caverlee, & Rudesill, 2015) and Lite-coins (Ciancaglini, Balduzzi, Goncharov, & McArdle, 2013). One of the widespread anonymous marketplaces in the deep web was the Silk-Road, which was confiscated by the FBI in 2013 (Sui et al., 2015).

Several networks are available for use that support anonymity and ensure safe connections between peers. However, the only network that has gained traction and popularity in the

underground marketplace is The Onion Router (TOR), which, probably because of its maturity, has been accepted as the best choice for anti-censorship tools, and the level of development it has reached is superior compared to the rest of the available systems, such as the Invisible Internet Project (I2P), Freenet and rogue TLDs (Ciancaglini et al., 2013).

Beyond the spreading beliefs of what the deep web is actually offering in the eye of the regular population, we found Ciancaglini et al. (2013) crawling into that unreachable area and explaining things in a more realistic light. Ciancaglini et al. (2013) identified the deep web as any online content that cannot be indexed by search engines, including dynamic web pages, blocked sites, unlinked sites, private sites with login credentials, non- HTML/-contextual/-scripted content, and limited-access networks. This content also includes anything that is below the searchable Internet that is inherently hidden, harder to get to, or not readily visible. Thus, Ciancaglini et al. (2013) compared this content to mining through subterranean layers of the earth in terms of scale, volatility, and accessibility. Ciancaglini et al. (2013) then reported the various activities conducted in the deep web, such as:

- Trading Malwares that host command-and-control (C&C) infrastructure, for example, VAWTRAK malware; the banking Trojans that spread via phishing emails and CryptoLocker, which is a ransomware variant that encrypts victims' personal documents before redirecting them to a site where they have to pay in order to regain access to their files once again.
- The use of Bitcoin for laundering money and purchasing illegal goods and services, since all Bitcoin transactions are anonymous as long as the real identity is not linked. A major fact that has to be highlighted and that is of major importance to legal personnel is the fact that Bitcoin trading is fully public. Every transaction is publicly available, making users vulnerable to investigations and examination. Thus, tracking money as it moves through the system is practical but is not without difficulties because of services that add further anonymity to the system.
- Buying and selling stolen accounts for instant details of credit card numbers, bank account numbers, and online auction and gaming site credentials.
- Selling Passports, IDs, legal documents and even their fake counterparts.
- Leaking confidential information.
- Assassination services.

Both the deep and the dark web are considered to be major tools for cyber criminals, making the tackling of cyber crime very difficult to achieve and requiring more and more association among law enforcement agencies to survey and counter them. Leukfeldt et al. (2016) believe that to better counter these types of illicit activities, more knowledge on the actors involved, their characteristics, and their modes of operation needs to be identified.

Cyber crime Cost

With the increase in cyber-attacks, the security of digital space has become a highly demanding topic. Nevertheless, statistics related to cyber crimes reported to law enforcement and governments are limited (Holt, Blevins, & Burkert, 2010). Evidence has been collected from different sources that have supported the increase in the attack ratio at a national level. According to the Cyber Crime Report (2016), 122 million attacks were detected and prevented, indicating a 35% increase in the number of attacks from 2015 to 2016. The American Institute of CPAs identified the major cyber crimes according to their costs and losses, as described in the Table below:

Table 1. Top Types of Cyber Crimes

Types	Definition	Losses
Corporate Account Takeover	▪ An emerging type was first identified in 2008, usually involving the act of obtaining an entity's financial banking credentials through the use of social engineering and malware to hijack the entity's computers for the purpose of stealing funds. ▪ Example: Electronic fund transfer fraud, such as: Automated Clearing House or wire transfer.	▪ Was projected to reach 800 million dollars by the end of 2016.
Theft of Identity	▪ The act of stealing personal identification information for the purpose of committing illegal acts, such as: opening a line of credit, renting a house, purchasing goods or services, auction- and wage-related fraud or extortion.	▪ 112 billion dollars in the past six years (prior to 2016).
Data Theft	▪ The act of illegal possession of sensitive data, which includes unencrypted credit card information stored in businesses, trade secrets, intellectual property, source code, customers' information and employee records.	▪ The act has affected 21.5 million people and 4.2 million current and former federal employees.
Ransomware	▪ A type of malware used to restrict access to important files or the entire system in which access is not granted until extortion payment is received and granted.	▪ Cost varies based on the cyber criminal demand.

Source: AICPA (2013, 2017)

The Table 1 indicates the cost of certain types of cyber crimes conducted in the United States of America. Cyber crime reports identify identity theft and data theft as separate trends. However, the Anti-Phishing Working Group (APWG) identifies these two types as one attack called phishing activity, in which social engineering methods and technical subterfuge are employed to steal both identity and financial account credentials (APWG, 2014). According to Kigerl (2016), the United States is the first target of phishing attacks, "suffering 60% of the worldwide phishing volume, with an average amount of 1,800 dollars lost per individual and 20,070 dollars lost per business" (P. 149). Moreover, China ranks at the top of malware-infected countries, followed by Taiwan and Turkey, whereas Scandinavian countries have the lowest infection rate (APWG, 2016). However, a survey conducted by PWC (2016) illustrated that companies residing in the Middle East suffered greater losses than other regions worldwide, resulting in 56% of businesses losing more than 500,000 dollars, compared to 33% globally. Additionally, the Anti-Phishing Working Group (APWG) found that the most attacked and targeted business sectors are retail and services, suffering from 43% of the attacks, followed by the financial sector with 21%, the Internet

service providers with 12%, and then payment services, multi-media and social networking, with government, surprisingly, having just 1% of the total attacks.

This cost explicitly impacts businesses by completely perturbing their marketing activities, damaging their reputation, causing a loss of consumers' confidence and, consequently, killing the business (Smith, Smith, & Smith, 2011) if action is not taken to strengthen cyber security measures. Interestingly, Smith et al. (2011) found, upon examining whether cyber crime news negatively affects shareholder value, that "cyber crime and resulting news stories do affect shareholder value, at least in the short term, via significant decreases in stock price" (P. 6). Moreover, according to Kshetri (2010), people in developing countries are attracted to cyber crimes because of high unemployment rate and low wages; there are reports indicating that traditional organized crime groups in these countries have been involved in such attacks after diverting their operations to cyberspace to expand their illicit activity globally.

Theoretical Background

How is this explained? Cyber-attacks can be better explained through the rational activity theory. This theory focuses on the characteristics of the illicit cyber activity (rather than the perpetrator) in which different components can be explained through different elements such as motivated offender, target and absence of physical or software-based corporate protection (Rivard, 2014). Moreover, Compeau and Higgins (1995) suggested the social cognition theory, in which environmental influences, personal factors and behaviour are determined to explain the capabilities of any user to use the digital platform to commit or to attempt an attack. These theories may go beyond just explaining the activity to expose what the actual motives are and who is behind an attack that may be classified as e-terrorism, cyber organized crime or simply that of an individual offender. Tade (2013) argues that multiple theories, such as the routine activity theory and the social learning theory, have been employed to understand cyber crime with limited explanatory value with regard to the phenomenon itself, emphasizing the superiority of the space transition theory in explaining aspects such as criminal behaviour and anonymity as well as a lack of deterrence factors, a chance of going un-detected and a unity of strangers to commit a crime in physical space.

Space Transition Theory argues that, people behave differently when they move from one space to another" (Jaishankar, 2008, pp. 292-296; Jaishankar, 2018). It also indicates what might be emerging in cyberspace. Cyber crime has become more organized and more frequently committed by groups rather than lone offenders. Organized criminal groups started to use Internet means not only for the purpose of communication but also to commit fraudulent activities, extortion, theft or money laundering (Tade, 2013). Moreover, cyber offenders may operate as a loose network in close geographic proximity, even if the conducted attacks are characterized as transnational (Broadhurst et al., 2014). A recent study of Baek, H. (2018) aimed to study the deviant behaviors on the Internet has strongly supported the Gottfredson and Hirschi's self-control theory.

Drawing from the above review and theoretical background. It has been noticed that most research found to focus on which countries are high in cyber attacks, with no further illustration of why these countries are at such high level of security risk (Kigerl, 2012). With few inferential theoretical explanations, this study is intended to fill these gaps.

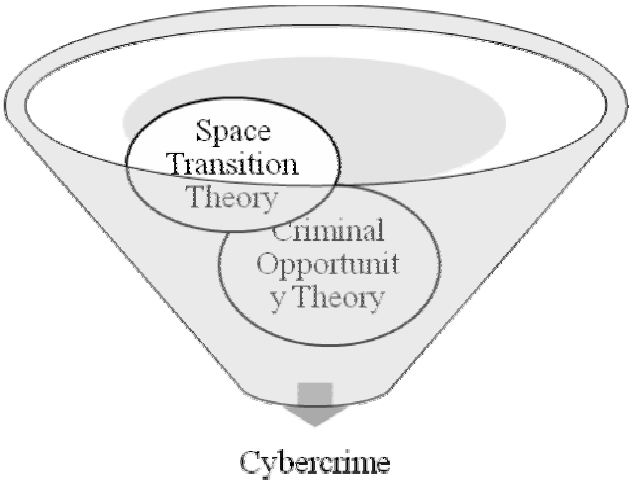
The Current Study

The current study aims to examine the effect of unemployment on the number of cyber crime cases in several countries (UAE, USA, Belgium, the Netherlands, Japan, China, Italy, Spain, India, Canada). A previous study by Song, Lynch, and Cochran (2016) found that structural conditions such as unemployment and non-urban populations are associated with the locations in which users access the Internet and may act as offenders. It was found that unemployment interacts with Internet usage; for example, the effect of the magnitude of Internet users on spam was strongest in nations with higher unemployment rates (Kigerl, 2012). Using cross-country data, Kigerl (2012) found that the unemployment rate and gross domestic product (GDP) per capita measured by the number of Internet users per capita and demographical/geographical factors such as each country's population and location had significant direct and indirect effects on both spamming and phishing rates (Song, 2017). Song (2017) specifically illustrated that the Kigerl study reported the following results: "GDP per capita had direct effects on both spamming and phishing rates. The number of Internet users per capita had a direct effect only on the cross-national rate of 26 spamming, while unemployment rates had a direct effect on phishing rates" (26-27). Davis (2012) held an interview with Misha Glenny, author of McMafia: Journal through the Global Criminal Underworld, who demonstrated that one of the reasons for engaging in cyber crime is the high level of unemployment, along with the presence of young people who are gifted in computer skills.

As explained earlier, routine activity theory and social learning theory have been applied to cyber crime with limited explanatory value for the phenomenon itself, emphasizing the superiority of space transition theory in explaining aspects like criminal behaviour, anonymity, lack of deterrence factors, chance of going un-detected and unity of strangers to commit a crime in the physical space (Tade, 2013). However, to explain the relationship that exists between the unemployed population and cyber crime, criminal opportunity theory is best. This theory examines how "situational opportunity and motivations explain criminal behaviour and criminal victimization" (Birkbeck & LaFree, 1993, p. 123-124). Criminal opportunity theory assumes the existence of a motivated offender while focusing on the effects of the characteristics of the individual himself (such as age, race, gender) and on the contextual target variables (such, unemployment rate, neighbourhood housing density, urban or rural location) (Song et al., 2016). Song et al. (2016) elaborate further that "prior research has indirectly measured these risk factors using multiple target variables" (p.584). Jaishankar (2018) illustrated that many researchers who attempted to address the causation of cyber crimes with traditional theories (such as social learning theory, routine activities theory and drift and neutralization theory) were not fully successful in their explanation of cyber attacks. For that reason, the space transition theory was propounded by Jaishankar himself.

In this study, we argue on the need for synergetic theoretical level to properly explain the opportunistic perspective of cyber crime in different cyberspace levels, as cyberspace incorporates different factors depending on the level of the space used by different population. Population itself varies not only in terms of size but also in terms of its geographical distribution, which also includes different variables (such as nationalities, generation, educational level, motives, economic status, geopolitical reasons). Figure 1 illustrates the overarching theoretical background used to explain the relationships between the listed hypothesis.

Figure 1. Overarching Theory

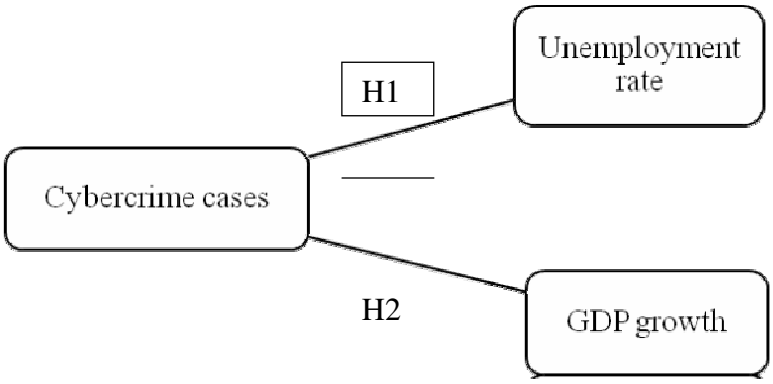


Thus, the first research hypothesis posited.

- H1: An increase in cyber crime cases is associated with an increase in unemployment rate.
- Since the Internet is increasingly integrated into every single aspect of society, the most meaningful effect of this increased integration is the Internet's share of global GDP (Ryder, 2014). Therefore, the hypothesis below can be drawn.
- H2: An increase in cyber crime cases is associated with an increased growth of GDP.

Figure 2 illustrates graphically the above hypothesis.

Figure 2. Research Model



Methodology

Data

The data related to cyber crime were collected from the online database source provided by Statista. A number of key words were used to obtain the data (such as number of cyber security incidents among firms, number of cyber crime related reports, number of cases of internet banking fraud, number of cyber crime offenses, number of identity theft incidents, number of reported cyber crime incidents committed, incoming complaints about internet crime on the IC3 website, annual number of data breaches and exposed records). The search yield a finding of cyber crime number for multiple countries (such as Singapore, Canada, USA, Belgium, the Netherlands, Japan, China, Italy, Spain, India, South Korea, Russian Federation, Colombia, Ukraine, Vietnam, Belarus, Kazakhstan, Philippines). However, we were faced with some limitations related to the number of the yearly available records of cyber crime cases in these countries. Since our initial target was to gather the data for the past 15 years, we were forced to limit our data duration to 2005 -2017 because of the unavailability of any full previous records. This limitation resulted in exclusion of some countries and inclusion of only (USA, Belgium, the Netherlands, Japan, China, Italy, Spain, India, Canada). Furthermore, we thought of adding UAE to the analysis and no data were available online that matches the previously found data. For that reason, the UAE related data were collected from government agency. We should illustrate that UAE data are confidential and cannot be described or provided in any means. On the other hand, the GDP and GDP per capita of the targeted countries were collected from the World Data Bank, where unemployment rate data were gathered from Federal Reserve Bank of St. Louis\Economic Research. No limitations were faced while gathering these data.

Since the purpose of the collected data was to measure the extent to which cyber crime is affected by GDP growth rate and the level of unemployment and the fact that the data for the selected countries were limited to the period of 2000-2017; the data were constructed as cross sectional time series data. Which resulted to a total sample size was 180 including some missing data related to the number of cyber crime cases.

For the purpose of preparing the data for analysis, the data on cyber crimes were transformed to their natural log, where GDP per capita and GDP were transformed to their growth rate.

Analytic Strategy and Experiment

The data were constructed as time-series cross-sectional data, which are characterized by having repeated observations over fixed units, such as in our case countries, to easily analyse them through the use of Stata commands. Models for the time-series cross-sectional data (temporal & spatial) make use of an ordinary least squares (OLS) problem (error of correlation & heteroscedasticity). To address these problems, Parks proposed the use of generalized least squares (GLS) (Beck & Katz, 1995). The panel data GLS estimator that uses model xtgls allows for a more flexible covariance structure for disturbances and random effects (Erik, 2010). This method fits cross-sectional time-series linear models using feasible generalized least squares and allows estimation in the presence of autocorrelation within panels and cross-sectional correlation and/or heteroscedasticity across panels (Erik, 2010). However, since Parks's method might lead to a dramatic underestimation of parameter variability (Beck & Katz, 1995), the feasible generalized least squares (FGLS) was used in this paper since it assumes that the error is known rather than estimated. Moreover, many linear models with serially correlated errors (such AR(1) errors) and

many linear mixed models can be fit with FGLS (Olive, 2017). For that reason, remedial and diagnostic test is not required to test the model since FGLS is used as solution.

We estimated the relationship between the number of cyber crimes and the level of unemployment in different countries, including economic growth. To get more accurate results, each country was measured and analysed separately.

The choice of *xtgls* was based on Figure 3. *Xtgls* allowed us to estimate the majority of the pooled model (Podestà, 2002):

Figure 3. Stata Commands Choice

Command	Option	SE estimates are robust to disturbances being	Notes
reg, xtreg	robust	heteroscedastic	
reg, xtreg	cluster()	heteroscedastic and autocorrelated	
xtregar		autocorrelated with AR(1)[1]	
newey		heteroscedastic and autocorrelated of type MA(*q*)[2]	
xtgls	panels(), corr()	heteroscedastic, contemporaneously cross-sectionally correlated, and autocorrelated of type AR(1)	*N* < *T* required for feasibility; tends to produce optimistic SE estimates
xtpcse	correlation()	heteroscedastic, contemporaneously cross-sectionally correlated, and autocorrelated of type AR(1)	large-scale panel regressions with xtpcse take a lot of time
xtscc		heteroscedastic, autocorrelated with MA(*q*), and cross-sectionally dependent	

[1] AR(1) refers to first-order autoregression
[2] MA(*q*) denotes autocorrelation of the moving average type with lag length *q*.

Source: (Hoechle, 2007)

Giving the assumption of the pooled TSCS, all the units are then characterized by the same regression equation at all points in time and can be written as (Beck & Katz, 1995):

$$y_{i,t} = x_{i,t}\beta + \epsilon_{i,t}; i = 1, \ldots, N; t = 1, \ldots, T \quad (1)$$

Where $x_{i,t}$ is a vector of one or more (κ) exogenous variables and observations are indexed by both unit (i), time (t) and ϵ is the error term. According to Beck and Katz (1995), Equation 1 can be estimated by generalized least squares regardless of any error complexities as long as the covariance of the error (Ω) is known. Given that assumption, GLS is completely efficient and yields consistent estimates of the standard error. GLS works by transforming equation 1 with a general error covariance matrix to another linear equation where the error covariance matrix is suitable for OLS estimation, such that the GLS estimates of Ω is given by:

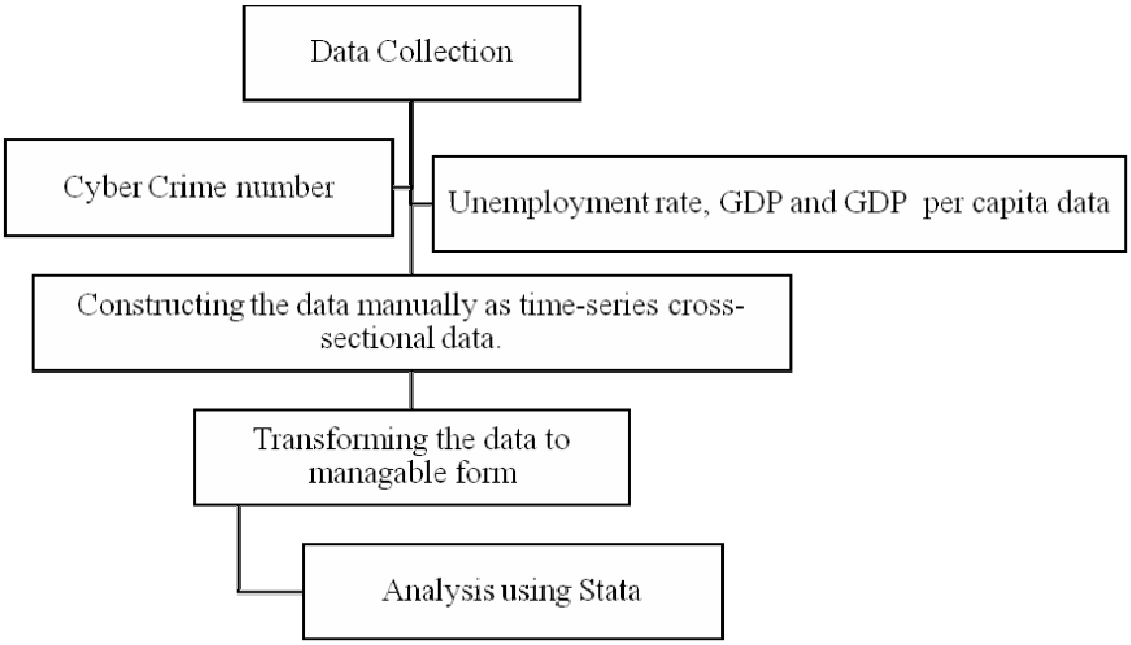
$$(X)'\Omega^{-1}(X)^{-1}X'\Omega^{-1}Y \quad (2)$$

With the estimated covariance matrix:

$$(X)'\Omega^{-1}(X)^{-1} \quad (3)$$

The experiment process is described in the figure 4.

Figure 4. Experiment Process



Results

The results below describe the estimated P value after running xtgls regression, which is measured by:

$$y_{it} = \beta_1 + \sum_{k=2}^{k} \beta_k x_{kit} + e_{it} \quad (4)$$

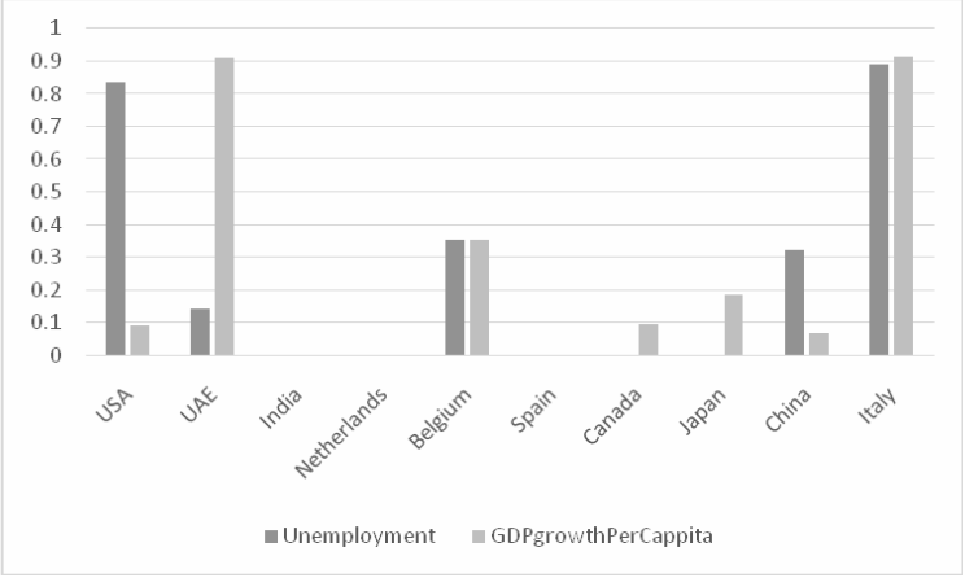
Where y_{it} is the dependent variable (natural logarithm of cyber crime number for each country),β is a parameter estimates, $x_{i,t}$ is a vector of the two exogenous variables (unemployment and GDP growth rate per capita) that are indexed by both unit (i) and time (t). Upon experimenting it was found that GDP growth rate per capita yields better results. So, for the purpose of this study GDP growth rate was excluded.

As shown in Table a, which illustrates the results of the overall hypothesis testing, it was found that the USA, UAE, Belgium, China and Italy are not significant, with a p-value greater than 0.05 with a statistical significant p (0.836, 0.141, 0.353, 0.323 and 0.892 respectively) for unemployment and p value of (0.092, 0.911, 0.354, 0.065 and 0.915 respectively) for GDP growth per capita, indicating that the reasons behind committing such crimes are completely non-dependable on both variables. However, India, Netherlands and Spain were of highly significant with a p-value of (0, 0.002 and 0 respectively) for unemployment and a value of significant of NULL for GDP growth per capita. Additionally, Canada and Japan were found to be highly significant in regard to unemployment rate with significant p-value (0) but not significant in terms of GDP growth per capita with a p-value of (0.094 and 0.186 respectively). Figure 5 demonstrates the distribution of level of significance for the 10 countries.

Table 1. Results of p Values

	P>|z|	
Country	**Unemployment**	**GDP growth Per Capita**
USA	0.836	0.092
UAE	0.141	0.911
India	0.000	0.000
Netherlands	0.002	0.000
Belgium	0.353	0.354
Spain	0.000	0.000
Canada	0.000	0.094
Japan	0.000	0.186
China	0.323	0.065
Italy	0.892	0.915

Figure 5. Distribution of level of significance for the 8 countries



The above results somewhat vary from the results obtained by study of Kigerl (2012). Upon his attempt to answer whether internet users per capita, unemployment rate, and participation in the Convention on Cyber crime international treaty could impact the spam or phishing output on a sample size of 132 countries. Kigerl found that"unemployment is no longer related to spam after controlling for spurious factors. However, the interaction between Internet users and unemployment is significant ($p < .001$). The effect of Internet users on spam is conditional on a nation's unemployment rate. The interaction suggests that the relationship between Internet users

and spam is strongest in countries with high unemployment. Moreover, it may be that unemployment motivates offenders to commit crime, but it could also mean that the unemployed spend more time online. On the other hand, countries with higher GDP per capita are also associated with more spam. A 1 SD unit increase in GDP per capita predicts a 1.9 increase in the expected count of spam sent ($p < .05$). Moreover, Wealthier countries send more spam, even when Internet users per capita are held constant" (p. 479). Kigerl (2012) finding are varied and came with an overall conclusion indicating that interaction involving unemployment was not significant.

Discussion and Conclusion

The present study aimed to empirically test the relationship between the commitment of cyber crimes and the unemployment level in different countries with various proportional levels of populations. The method employed provides a clear overview of how the GDP growth per capita in a certain unemployed population can affect the amount of cyber attacks in the studied countries.

The results of this paper serve as a good starting point when analysing the real results behind the increased number of cyber attacks in some countries and how much this number depends on the unemployment rates. Our results showed that the amount of cyber crime in the USA, UAE, Belgium, China and Italy does not depend on the unemployment level, with a statistical significant p (0.836, 0.141, 0.353, 0.323 and 0.892 respectively). Reasons behind this outcome might vary depending on the country's social and cultural diversity as well as its levels of economic and legitimate security. One surprising result is that of Italy with 0.892 level of significance, which is well-known to be controlled socially if not economically by the Mafia. This might indicate the following: first, the high level of knowledge today's malefactors have in different areas of technology; second, the gaps in safeguarding mechanisms; and third, the social fear of reporting any incident that might be controlled by the Mafia. As a matter of fact, these reasons might be shared among most of the countries included in the previous analysis with existing trends of cyber terrorism. However, China is different with a value of 0.323. Despite its large population, the rapid growth in advanced technologies merging with the slow growth in cyber security measures has left China vulnerable to an increased amount of cyber crimes (Ivezic, 2017).

However, the Netherlands, India and Spain were found to be of higher significance with a p-value of (0.002, 0 and 0 respectively).According to figures published by the security company Symantec, the Netherlands is the number one country in Europe and is fourth in the world for cyber criminals (DutchNews.nl, 2015). The Dutch news indicate the reason behind this increased level of cyber crime to be the fact that they have fast and reliable Internet connections, making the Netherlands one of the main countries targeted by criminals to start an anonymous cyber attack. According to Kshetri (2016), the reason behind such a high significance level with high unemployment rates in India is directly related to key economic and social characteristics, which include dual economy and low levels of income and education, which lead to low levels of human development, higher degrees of income inequality and weak democratic institutions. According to the Financial Action Task Force Mutual Evaluation Report (2014) on Spain, the recession period has put pressure on Spain's fiscal position, leading to increased taxation and a high unemployment rate relative to the other members of the European Union. Spain's black-market economy represents a significant share of economic activity and is usually making use of the Internet as an intermediary to move illicit cash associated with drug trafficking, tax and

customs fraud and human trafficking (Financial Action Task Force Mutual Evaluation Report, 2014).

Moreover, as previously shown in Table 1, the USA, UAE, Belgium, China and Italy had a p value of (0.092, 0.911, 0.354, 0.065 and 0.915 respectively) for GDP growth per capita. Where, India, Netherlands and Spain had a NULL significant value for GDP growth per capita. Additionally, Canada and Japan had a p-value of (0.094 and 0.186 respectively) in terms of GDP growth per capita.

Upon comparing the statistical significance obtained for both unemployment rate and GDP growth per capita, we can conclude that the level of cyber attacks do vary and obviously there are more factors involve. Probably, this study may be useful to academics, governments and regulators seeking to improve safeguarding mechanisms through better legislation and detection methods by classifying the population in terms of education and the number of nationalities residing in one country and, accordingly, finding the gaps behind the increase in cyber attacks. This method is especially beneficial in the detection stage. Moreover, this study is useful for FATF (Financial Action Task Force) as it can be used to re-evaluate its' recommendations related to cyber attacks and to allow more country customization accordingly.

The results in this study indicate that cyber crime level varies based on unemployment rate and GDP growth per capita. Moreover, the reasons behind the changing risk levels of cybercrime in different countries are still to be investigated further. In this study we argued the need for collaboration of space tradition theory and criminal opportunity theory to explain cyber crime since they incorporate not only cyber space but also population characteristics in different countries.

The study should be read in the context of its limitations of the data available, as the findings are not subject to information available elsewhere. Future research may be designed to compare and evaluate the findings of this study with those related to money laundering and terrorist financing involved with financial institutions. A more punctual research direction that might serve intelligence government agencies is through analyzing the three levels of cyber space (surface, deep and dark) web and to properly address their vulnerabilities. Addressing vulnerabilities will open a wider range of research areas for scholars working in computer security, digital forensic science and AI (Artificial Intelligence).

Acknowledgements

We sincerely thank the Editor-in-Chief of IJCC and anonymous reviewers for their valuable comments and feedback. We also thank Mr. Hamid Al-Zaabi, for helping us through collecting data of the United Arab Emirates and for his support.

References

AICPA. (2013). *The top five cybercrimes*. Durham, NC: AICPA.

AICPA. (2017). *Top cybercrimes white paper. How CPAS can protect themselves and their clients*. Durham, NC: AICPA.

APWG. (2014). Phishing activity trends report, APWG, 2nd quarter 2014. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf.

Baek, H. (2018). Computer-Specific Parental Management and Online Deviance across Gender in South Korea: A Test of Self-Control Theory. *International Journal of Cyber Criminology*, *12*(1), 68-83.

Beck, N., & Katz, J. N. (1995). What to do (and not to do) with time-series cross-section data. *American Political Science Review, 89*(3), 634-647. doi: 10.2307/2082979.

Birkbeck, C., & LaFree, G. (1993). The situational analysis of crime and deviance. *Annual Review of Sociology, 19*(1), 113-137. doi: 10.1146/annurev.so.19.080193.000553.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1-20.

Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). *Deepweb and Cybercrime. Trend micro report*. Retrieved from https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf.

Compeau, D. R., & Higgins, C. A. (1995). Application of social cognitive theory to training for computer skills. *Information Systems Research, 6*(2), 118-143.

Congressional Research Service. (2015). Dark web. CRS report (Pub. No 7-5700).

Cyber Crime Assessment. (2016). *Need for a stronger law enforcement and business partnership to fight cyber crime*. NCA Strategic Cyber Industry Group.

Davis, R. (2012). Organized crime in a network society. *Journal of International Affairs, 66*(1), 145-149.

DutchNews.nl. (2015). The Netherlands is popular with cyber criminals. Retrieved from http://www.dutchnews.nl/news/archives/2015/04/the-netherlands-is-popular-with-cyber-criminals/

Erik, B. (2010). *A tutorial for panel data analysis with stata*. Oslo, Norway: University of Oslo, January 04, 2010, Econ 5103 – Advanced econometrics – Panel data.

Financial Action Task Force Mutual Evaluation Report. (2014). Anti-money laundering and counter-terrorist financing measures - Spain, Fourth round mutual evaluation report. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Spain-2014.pdf.

Hoechle, D. (2007). Robust standard errors for panel regressions with cross-sectional dependence. *Stata Journal, 7*(3), 281.

Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse: A Journal of Research and Treatment, 22*(1), 3-24.

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 62*(1), 1-20.

Ivezic, M. (2017). Cybercrime in China – A growing threat for the Chinese economy. Retrieved April 2, 2018, from https://www.linkedin.com/pulse/cybercrime-china-growing-threat-chinese-economy-marin-ivezic

Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. *International Journal of Cyber Criminology*, *12*(1), 1-8.

Jaishankar K., (2008). Space transition theory of cyber crimes. In F. Schmallager and M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470-486. doi: /10.1177/0894439311422689.

Kigerl, A. (2016). Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates. *International Journal of Cyber Criminology, 10*(2), 147.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7), 1057-1079. doi: 10.1080/01436597.2010.518752.

Kshetri, N. (2016). Cybercrime and cybersecurity in India: Causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

Lavorgna, A. (2015). Organised crime goes online: Realities and challenges. *Journal of Money Laundering Control, 18*(2), 153-168. doi: 10.1108/jmlc-10-2014-0035.

Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging" cyber-organised crime" rhetoric in the United Kingdom. *International Journal of Cyber Criminology, 10*(2), 170.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2016). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287-300.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*(1), 52-60.

McCusker, R. (2006). Transnational organised cyber crime: Distinguishing threat from reality. *Crime, Law and Social Change, 46*(4-5), 257-273.

McGuire, M. (2012). *Organised crime in the digital age*. London, UK: John Grieve Centre for Policing and Security.

Olive, D. J. (2017). *WLS and Generalized Least Squares. In Linear Regression* (pp. 163-173). Springer, Cham.

Podestà, F. (2002). Recent developments in quantitative comparative methodology: The case of pooled time series cross-section analysis. *DSS Papers SOC, 3*(2), 5-44.

PWC. (2016). A false sense of security? Cybersecurity in the Middle East. Retrieved from https://www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf.

Rivard, J. P. (2014). *Cybercrime: The creation and exploration of a model* (Order No. 3691452). Available from ProQuest dissertations and theses global: The humanities and social sciences collection. (1671728162).

Ryder, N. (2014). Cyber crime, security and financial crime-what SMEs need to know and how to protect yourself. In *Partners in procurement - supplying the public sector*. Bristol, UK: University of the West of England.

Sanger, D. E. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power*. New York, NY: Crown Publishers.

Smith, G. S. (2015). Management models for international cybercrime. *Journal of Financial Crime, 22*(1), 104-125. doi: 10.1108/jfc-09-2013-0051.

Smith, K. T., Smith, L. M., & Smith, J. L. (2011). Case studies of cybercrime and their impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal, 15*(2), 64.

Song, H. (2017). *An exploratory study of macro-social correlates of online property crime* (Order No. 10604219). Available from ProQuest dissertations & theses global: The humanities and social sciences collection. (1949396347). Retrieved from http://adezproxy.adu.ac.ae/docview/1949396347?accountid=26149.

Song, H., Lynch, M. J., & Cochran, J. K. (2016). A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice, 41*(3), 583-601.

Sui, D., Caverlee, J., & Rudesill, D. S. (2015). *The deep web and the darknet: A look inside the internet's massive black box*. Washington Wilson Center.

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs, 23*(4), 689-705. doi: 10.2478/s13374-013-0158-9.