Differences in cyber crime awareness between Korea and the UK

Woo SeongWook
(University of Portsmouth, MSC Economic Crime)

Lee SangHak
(중앙대학교 융합보안학과 연구원)

Differences in cybercrime perceptions between Korea and the UK: Based on a survey

Woo SeongWook[1]
Lee SangHak[2]

< Summarize >

This paper investigates perceptions and actual experience with cyber fraud in the United Kingdom and South Korea and perceptions of viewers on cyber theft broken down by age. The study found out how cyber risk is of a dynamic and ephemeral structure, whose experience varies across different cultures.

This was a mixed-method design cross-sectional study, from respondents who ranged in age from 18 to 54. This study thus finds that not only is there a lack of clinical literature dealing with these issues, but further, that one must carefully consider the cultural context within which the studies must be considered relevant to an issue, in this case to experiences of cybercrime.

The findings also form a foundation for related recommendations to ensure that cybercrime prevention and response measures targeted at specific populations are reinforced within the global movement to promote a more all-inclusive global strategy in the fight against illegal online based activities; Strengthening the Cybersecurity Posture of Responsible Institutions Intended population: Other than the principles, a national cybersecurity strategy provides the various legal and policy

1 University of Portsmouth, Msc Economic Crime
2 중앙대학교 보안대학원 융합보안학과

instruments.

Overall, this work brings out the point that proper strategies regarding cybersecurity are sensitive to the culture. The challenge involved is to make the set of regulations not only resilient but adaptive in the face of a kaleidoscopic variety of local and international cyber threats. The global relevance of these findings and their implications cannot be underestimated, with their authors asserting that their study needs replication in a variety of countries worldwide in order to factor into global debates on cybercrime and its prevention.

: United Kingdom, South Korea, Fraud, Cyber Crime, Cyber perception

목 차

I. Introduction

The Internet has significantly impacted the economies of countries around the world. In developed nations, the Internet has been a key driver of GDP growth, accounting for 21% over the past 25 years and 10% in the last 5 years. In emerging economies like China, India, and Brazil, it has contributed to growth rates of over 7% in the past decade. Countries with mid-level economies, such as Turkey, Malaysia, and Mexico, are also reaping economic benefits. The Internet of Things (IoT) optimizes industrial processes, reduces operational costs, and plays a vital role in various other sectors, including healthcare and logistics. The combination of IoT and blockchain fosters data monetization and security while creating new business models. Additionally, the Internet offers social benefits such as improving health, promoting social connections, and providing online job opportunities.

However, there are negative aspects as well. Cybercrime poses a severe threat to adolescents, small businesses, consumers, and individuals. Small businesses, in particular, are at higher risk due to limited resources to defend against cyberattacks. Cybercrime can disrupt e-commerce systems, causing financial losses. Children are especially vulnerable to mental health risks from cyberbullying, and attacks like denial-of-service and data breaches can result in

significant costs.

This paper analyzes and compares public perceptions of cybercrime in the UK and South Korea. The study aims to understand the current state of affairs and suggests that both countries face unique challenges. By learning from and citing best practices through mutually exclusive approaches, they can improve policies. The analysis seeks to assist society in enabling effective responses to cybercrime.

II. Cyber crime definition and Law

1. Definition of cyber crime

1) Definition of cyber crime

In the modern world, cybercrime is growing increasingly important. The rapid development of the Internet and digital technologies has led to the emergence of new sources of profit for criminal groups. Although experts cannot agree on the definition of cybercrime, it is generally understood to be any activity for personal gain or damage to others that uses a computer or the Internet. The forms of such crimes are extremely diverse and can be limited to the hacking of the simplest television or create a computer virus so complex that it causes financial collapse. There are four main forms of such crimes, namely: cyber intrusion, cyber fraud and theft, cyber pornography, and cyber violence. Researchers generally argue that while cybercrime causes no physical harm to victims, its psychological harm makes it an effective tool for criminals. Real examples demonstrate this more clearly. So, “Mary” lost a lot of money after a registered fake auction site. “Tom” even faced fraud alongside malware on his computer. He paid unnecessary penalties for many dangers in the form of warnings. There are countless varieties of threats in the digital space. Therefore, one should always be on the lookout and reasonably assess the situation.

Preventive work to protect personal information is also necessary. Collaboration between law enforcement and technology companies and the media can be the key to effective cybercrime prevention. Recognizing the potential dangers and taking appropriate corrective action will ensure the safe use of the digital space.

2) Rise of Cyber Crime

Attack of Cybercrime is growing Day by day. The evolution of cybercrime were detected going back as far as the 1820s through attacks against tele-communication networks in the 1960's. 1980s - malware (90s spent in financial crime and terrorism) Spam emails and phishing attacks exploded in the 2000s. 2017 saw 600% rise in IoT attacks, and around the globe there were some 300 data breach incidents last year 2019: Worst ransomware attack- Public and healthcare sectors During the COVID-19 pandemic, social engineering attacks increased since early 2020. The first is from the side of society after incidents : The COVID-19 pandemic and social transition to digitalizing daily transactions naturally results in vast cyber frauds. The increase in the use of electronic services (remote work, online schools and universities, shopping) led to an increase in Internet traffic - which was immediately noticed by cybercriminals. This was especially made use of by a lack-luster attention around new technologies, over-staking on automated systems and phishing scams. Moreover, the surge in telemedicine - which is particularly true for psychiatric services due to COVID-19- has broadened its attackable area by cybercriminals. In summary, the history of cybercrime is a story that developed parallel to technological innovation; as we have seen with so many aspects in our lives during the COVID-19 crisis, and digital transformation which has tended only to expedite such advancements. Most importantly, everyone has to equip their own cybersecurity awareness and security measures against those threats.

2. South Korea and The UK Law

1) South Korea

Internet fraud is not one, whole law: it covers a variety of laws depending on the nature of the offense. Nevertheless, according to the general understanding of what fraud is, an internet scam falls within the wide range of pogroms deriving from simple deception and therefore underlies this basic law against deceiving straightforwardly. The laws in question depend on the form of damage caused by internet fraud. In the Law Prohibiting Unfair Acquisition of Property by Deceit in Electronic Commerce, if a person uses deceit to acquire property or financial gains from others, he/she will face up to 10 years imprisonment and be fined up to 20 million KRW, respectively. In the case of forming, using false information or issuing illegal commands by a computer to seek own profit and gain undue advantage for someone else in connection with the above crimes related to multiple official certificates (Article 135 of the Additional Criminal Act), up to ten years imprisonment or a 20 million won fine can be imposed. Theft which refers to stealing somebody else's property, its punishment is imprisonment for not more than 6 years or a fine of up to KRW 10 million. Penalties of up to 5 years of imprisonment or a fine of up to fifteen million KRW for using computer tampering with the work performed by another person. Cases of reported credit cards, such as advertising and using lost or stolen debit cards since it was established Crime to punish maximum 7 years in prison (maximum fine 50 million KRW). In the case of laws that prohibit acts obstructing information and communication networks, those who send a large number of signals or data, process illegal commands to interfere with stable operation in an emergency situation may be punishable by imprisonment for up to 5 years or a fine not exceeding 50 million KRW. The penalties imposed for breaching the rules on advertising information transmission are fixed using different schemes. In a lawsuit involving electronic financial

transactions between banks and customers on January 15, the Seoul Central District Court ruled in favor of national banks and regional agricultural cooperatives. According to the court, the bank had a duty to provide relief for damage arising from digital certificate forgery and wrongful transfer transaction. In the event that a customer is not thought to be grossly negligent, banks must refund customers' losses. "Pharming" is a form of internet address redirecting that directs bank customers trying to homepage access their bank's internet site over and electronic banking fraudulent loading fake webpage onto their computer or mobile phone device for the purpose of stealing personal information. This meant that the victim was exposed to the theft of his digital certificate and transfer transactions were performed, causing damage. The Electronic Financial Transactions Act provides that these were what was responsible. Resulting in different compensation amounts for the damages suffered by various plaintiffs. Plaintiffs 1, 9, and 24 paid for legal proceedings against Shinhan Bank, NongHyup Bank, Jangseungpo Agricultural Cooperative, and Nambu An Agricultural Cooperative. The share in the costs incurred by Seongyeon Agricultural Cooperative and Sangdong Agricultural Cooperative should be paid to Plaintiffs 8, 25, and 29.

2) The United Kingdom

Under the UK's "Cyber (Sanctions) (EU Exit) Regulations 2020", one could, on conviction, either for an offense under Part 3—Offences Relating to Financial Matters—or for a license violation under Regulation 21—Financial, be sent to imprisonment, fined, or both, which is discretionary, according to the general limits of the magistrates' courts in England and Wales. Similar penalties exist in Scotland and Northern Ireland, with slight variations concerning maximum imprisonment terms and fines. On conviction, breaches of Regulation 9(6), 2005, may result in up to 7 years' imprisonment or a fine or both. Moreover, on conviction, an offense under Regulations 23(6) or 27,

2005, in connection with Part 3 information, is liable to a maximum imprisonment of 6 months or a fine. According to the Crown Prosecution Service, 2019, cyber fraud entails imprisonment of up to 10 years and fines as stipulated under sections 1-3ZA and 6-7 of the Fraud Act 2006. Besides, legal considerations in respect of the proceeds of crime are dealt with under Part 7 of the Proceeds of Crime Act 2002, POCA 2002. Cyber fraud is directed towards individuals and businesses. It may be committed through online transactions or financial information.

Consequently, the "International Comparative Legal Guides" of 2020 revealed that a student from London was jailed for 22 months in August 2021 for sending fake text messages while purporting to be from Royal Mail, HM Revenue and Customs, banks, and mobile phone companies in an attempt to collect personal account information from people.

III. Related Research

1. Related Research

Although the growth rate of cybercrime is rapid, people are still less aware about cybercrime. Much research into this topic has already been conducted, and these studies play a vital role in understanding the impact and severity of cybercrime.

1) Dimc & Dobovšek (2010)

In Slovenia, most people and law enforcement agencies lack awareness and understanding of cybercrime. The research carried out with regard to perceptions of various kinds of cybercrime caused perceptions that were far from similar to activities carried out in the real world. For example, whereas theft is considered inappropriate in the real world, it is easily condoned in the virtual world, like in the case of illegal copying. It is further found that there is a process of desensitization that occurs when conventional crimes are committed on

the internet, and most people are uninformed about various cybercrimes and laws regulating them. All these findings point to the need for creation of awareness in the population and enforcement agencies regarding the dangers of cybercrime and its reality.

2) Bernik et al. (2011)

Research on perceptions of cybercrime suggests that information technology and Internet users are only relatively well aware of the issues, and their knowledge is driven by media exposure. While users are more aware of highly publicized cyber threats like computer viruses and hacking attacks, awareness of other threats is very low. Such risks also prove to be relevant for responsible behavior in cyberspace. The paper has overstressed broad and continuous education to raise awareness of the risks of cybercrime and reduce fears. It supports the idea that there is a positive relationship between the level of fear from cybercrime and the level of knowledge of cyber threats existing in cyberspace. It suggests that the risks and fears can be reduced by making users aware of various cyber threats and protective measures.

3) Methmali (2016)

One fact that was researched looked into cybercrime awareness. It has been found that information technology and Internet users are fairly aware of cybercrime, though their knowledge greatly channels through media exposure. As such, there is relatively more awareness among users on those cyber threats that are more frequently reported in news media, like computer viruses and hacking incidents. Meanwhile, fewer responses are those represented by other threats that have not received the same level of reporting, although these are equally important in guiding responsible behavior in cyberspace. This paper highlights that awareness about cybercrime risks should always be made at the user's end to minimize the level of fear. This paper also points out that knowledge of the users regarding the threats in

cyberspace has a clear relationship with the fear of cybercrime. The research will show that educating users about various cyber threats and protective measures is very important in terms of risk and fear minimization.

4) Narahari1 & Shah2 (2016)

Most young Internet users seem to be uninformed about cybersecurity and cybercrime in India. While they claim to know about these crimes, the user misinterprets that cybercrime is political attacks on big corporations and not upon all those who work with the Internet. The survey also showed that most users are not even aware of the bulk of cybercrimes, which include identity theft, phishing, distribution of inappropriate pornography, cyberstalking, mobile hacking, crimes on TOR and the dark web, copyright infringement, and cyberbullying. In addition, quite a number of internet users do not know where to report cybercrime or whom to contact.

5) Kamruzzaman et al (2016)

In 2016, a study investigated the experiences of young Bangladeshis aged 16-24 who were affected by cybercrime. The results showed that 60.16% of respondents were vulnerable to cybercrime through internet scams, and 78.81% agreed that social media exacerbates the damage by spreading false information. The most common type of damage was extensive attacks, accounting for 82.20% of the cases. Additionally, the study revealed that 56.78% of participants had been victims of additional crimes. Furthermore, 72.03% of respondents believed that more information about the internet could reduce harm, and 61.86% felt uncomfortable in cyberspace. This research contributes to the literature on cybercriminals and emphasizes the need for public education and security measures to protect young people from cybercrime. Overall, the study enhances the understanding of the challenges and consequences faced by young people in South Asian

countries.

6) Du Toit et al (2018)

While a large proportion of South Africans reported having fallen victim to cybercrime, the general willingness to report these cases was low. This included reasons such as people lacking understanding of how to report cybercrime or the reporting process as futile. Research also reveals that only very few strongly believed in South African law's capability to deal effectively with cybercriminals.

7) Odey & Ana (2021)

There were three general areas that evinced some general near-total lack of interest and understanding from the Nigerian respondents: general knowledge, industry knowledge, and personal views of Nigerians about cybersecurity. Many people, including executives, appear not to be well-informed about existing cyber laws and penalties in their country. This lack of awareness is one major reason why cybercrime is so rampant in Nigeria, as some offenders believe they can get away with their wrong deeds. Some of the cybercriminals do not even know that what they are doing is criminal and punishable under the law. Further responses also showed a lack of awareness regarding whom to report to or how to go about involving the appropriate authorities.

IV. Findings

1. Demographic characteristics

Division	category	amount	frequency (%)
Country	Korea	280	84.6
	UK	51	15.4
Age	Under 30s	241	72.8
	30s	32	9.7
	40s	24	7.3
	Above 50s	34	10.3
Sex	Male	224	67.7
	female	107	32.3
Graduation	High school diploma or less	203	61.3
	Bachelor's degree	71	21.5
	master's degree	37	11.2
	PhD	20	6
working place	school	319	96.4
	outside of school	12	3.6
total		331	100

<Table 1> Frequency analysis of demographic information

The frequency analysis of demographic information presented in <Table 1> shows that a total of 331 complete data sets were used for the final analysis. Among the participants, 84.6% were from South Korea, and 15.4% were from the United Kingdom. Most of the study participants were young individuals under the age of 30, and they had diverse educational backgrounds.

2. Difference between South Korea and The UK

		A few hours per day (<8)	Many hours per day (8+)	A few hours per week	A few hours per month	Hardly ever	Never
use the telephone	UK	38 (50.6%)	23 (30.6%)	8 (10.6%)	4 (5.3%)	2 (2.6%)	0 (0%)
	Korea	177 (59%)	102 (34%)	17 (5.6%)	1 (0.3%)	2 (0.6%)	1 (0.3%)
use the internet	UK	28 (37.3%)	46 (61.3%)	1 (1.3%)	0 (0%)	0 (0%)	0 (0%)
	Korea	154 (51.3%)	100 (33.3%)	34 (11.3%)	8 (2.6%)	2 (0.6%)	2 (0.6%)
reading and sending emails	UK	21 (28%)	4 (5.3%)	42 (56%)	7 (9.3%)	1 (1.3%)	0 (0%)
	Korea	69 (23%)	23 (7.6%)	97 (32.3%)	83 (27.6%)	21 (7%)	7 (2.3%)
read and send text/SMS messages	UK	44 (58.6%)	6 (8%)	17 (22.6%)	5 (6.6%)	3 (4%)	0 (0%)
	Korea	128 (42.6%)	53 (17.6%)	83 (27.6%)	23 (7.6%)	10 (3.3%)	3 (1%)
buy things online	UK	9 (12%)	1 (1.3%)	23 (30.6%)	37 (49.3%)	5 (6.6%)	0 (0%)
	Korea	54 (18%)	16 (5.3%)	111 (37%)	97 (32.3%)	19 (6.3%)	3 (1%)
bank online	UK	10 (13.3%)	1 (1.3%)	21 (28%)	40 (53.3%)	3 (4%)	0 (0%)
	Korea	90 (30%)	27 (9%)	107 (35.6%)	60 (20%)	14 (4.6%)	2 (0.6%)
Meet friends/family online via Zoom, Skype, etc	UK	12 (16%)	0 (0%)	27 (36%)	18 (24%)	13 (17,3%)	5 (6.6%)
	Korea	24 (8%)	10 (3.3%)	65 (21.6%)	109 (36.3%)	60 (20%)	32 (10.6%)

<Table 2> Frequency of Digital Activities by Participants from the UK and Korea

<Table 2> shows the frequency of digital activities among participants from the UK and South Korea. According to the study, UK participants had a higher rate of using their phones for several hours daily, with this rate being even higher among South Korean participants. The frequency of internet use among UK participants was high, with 28 participants using the internet for several hours daily and 46 participants using it for a few hours daily. Email usage varied, with 23 participants using email for several hours daily and 69 using it for a few hours daily. Text messaging was more common among South Korean participants, with 128 participants using it for a few hours daily and 53 using it for several hours daily. UK participants had a lower frequency of online shopping, with 9 participants shopping online for a few hours daily and 1 participant for several hours daily. South Korean participants spent more time online, with 90 participants shopping online for a few hours daily and 27 for several hours daily. UK participants used Zoom and Skype daily for meetings, but South Korean participants had more frequent meetings, with 24 meetings daily and 10 meetings lasting several hours. Both groups had weekly, monthly, and occasional meetings. This information shows that UK and South Korean participants have significantly different digital activity habits. South Korean participants engage more extensively in digital activities, particularly in text messaging, online shopping, online banking, and everyday internet use. UK participants have a higher frequency of weekly and monthly activities but show overall more moderate levels of engagement. These results highlight cultural and infra structural differences in digital behavior between the two groups.

3. Comprehensive case analysis and response strategy

In recent years, there has been a noticeable increase in internet fraud and hacking, requiring greater attention. Additionally, the types

of internet fraud and hacking occurring in South Korea and the UK have become more diverse. In South Korea, there were 19 cases out of 300 individuals, while in the UK, there were 18 cases out of 75 individuals. In summary, there are 5 types of cases in the UK and 7 types in South Korea. This chapter will evaluate various fraud and hacking cases through real-world examples and propose appropriate response strategies.

1) South Korea

The first case involves a phishing email impersonating Apple. The user received an email confirming a transaction they did not make. Clicking on a button within the email led them to a fake Apple website designed to steal account and financial information. As a result, the user's account was hacked and deactivated, necessitating the creation of a new account. These phishing emails often impersonate well-known companies to gain users' trust.

The second case concerns transaction fraud related to gaming. The victim printed out documents to submit to the police after recognizing the fraud but took no further action and ignored the situation. Additionally, there was an attempted scam through an internet promotion promising significant discounts from a reputable company. The victim was able to avoid the scam by verifying the offer through internet searches.

The third case involves unauthorized transactions amounting to 100,000 won due to a hacked Google payment system. The victim reported this to the authorities, changed their password, activated two-factor authentication, and logged out of all active sessions to prevent further account abuse.

The fourth case is an online scam using a second-hand trading market. The victim sent money but did not receive the goods and reported the incident to the police's cybercrime unit. Although the case was considered a failed attempt rather than a completed crime, the

victim received a full refund through Toss Pay. Toss Pay is a mobile financial service app based in South Korea, connecting users to local bank accounts, with 22 million registered users and 14 million monthly active users.

The fifth case involves extortion via email. Scammers used the victim's email address to threaten to expose their viewing of pornographic films unless money was paid. The victim did not respond, as the claims were not true.

Another case is a high-return cryptocurrency investment scam. The victim did not take further action and later learned that the investment company had gone out of business. Additionally, the victim was subjected to a voice phishing scam where the scammer claimed a new phone number had been registered. The victim did not provide personal information and terminated the contract.

Finally, there was a parcel scam using a text message with a malicious URL disguised as a delivery notification. The victim ignored the message and thus avoided falling for the scam.

2) The United Kingdom

The first involves email, text message, phone call, and WhatsApp-based phishing attacks. The victim having reported the successful phishing attempts to the relevant company, as a precautionary measure, requested monitoring and blocking. There are other online credit accounts that have been found to be opened in the victim's name and address. Action Fraud was contacted by the victim, but due to lack of evidence, help couldn't be obtained. The victim then notified ID Mobile, Vodafone, Argos, and O2 concerning the fake accounts. Given the nature of the victim's work, they made a report to their manager and was transferred to desk duties pending complete verification relating to the fake accounts.

The next incident was a case of bank impersonation. The victim did receive the phishing e-mails and text messages, but he did not click the

links nor reply to them. Despite this, hackers still managed to steal his details of his internet card and went on to buy Apple products worth £1,000. He did not report to authorities.

The third was about a friend whose Instagram account had been compromised. An email was sent which appeared to be from Royal Mail demanding tax payment. The victim recognized that this was a phishing email and did not open the link but had already clicked a Royal Mail delivery-related scam text link.

The fourth case is related to Facebook hacking. A perpetrator has used the victim's information to create a fake Instagram account, after which the gaming account has been stolen. Moreover, the victim's Instagram account was hacked; subsequently, ads for cryptocurrencies and other virtual currencies started appearing. At last, the victim had to delete their account.

The fifth case involves an email scam in the name of Booking.com. The e-mail which was received by the victim seemed to be from booking.com but was further proved not to be so. As a result of this mail scam, the victim had their email account deactivated.

3) Conclusion

The cases of the UK and South Korea underline the severe risks involved with online fraud and hacking. These, therefore, serve as a warning to all users to act carefully. It is in the nature of phishing attacks to imitate some reputable companies to take advantage of the user's trust. Users must not click suspicious links or attachments and must independently verify whether the contact is credible. Setting and changing passwords regularly based on government-recommended guidelines will help prevent account theft. In case of an incident, one should report it immediately to the necessary authorities and preserve the evidence well. Steps for enhancing security measures and learning new strategies against scams will minimize the risk of going victim to online frauds and hacking.

V. Discussion

1) Differences and Similarities

Comparative analysis between the mitigation strategies of cybercrime in South Korea and the UK shows a number of marked differences and similarities. The two countries agree on one fact, that cybercrime is bound to pose a threat to national security and economic stability. However, the most common types of cybercrime and their targets vary according to cultural perspectives, regulatory frameworks, and technological infrastructure. South Korea is a perfect case of misinformation and online digital harassment because the internet penetration rate is 95 percent, with correspondingly large social media usage. On the other hand, the UK has more identity theft, online fraud, and financial crimes because of high usage of online banking and e-commerce activities.

2) Cyber perceive

The view of cybercrime presents a massive problem that threatens national security, economic stability, and personal privacy. The awareness of cybercrime differs demographically, regionally, and contextually. It is also influenced by perception, experience, and exposure to media. The perceptions about cybercrime are preconditioned by the advances in technology, connectivity to the internet, and glottalization.

Due to connectivity on the internet, these new cyber activities principally focus on phishing and virus attacks in the banking and financial sectors. The early cyber-attacks were untargeted and disruptive, though have now turned into complex and malign forms done by organized crime groups or state actors aiming at financial gain or theft of intellectual property.

UK participants were much more aware of the proper channels for reporting cyber fraud. Whereas only 48.6% of South Korean

participants knew about the right procedures, 52.9% of those in the UK did. This could be because some South Korean participants had safety training on protection from frauds: 44.6% versus 17.6% in the UK. There are also differences in terms of the incidence of specific crimes related to cybercrime across countries, because cultural attitudes differ, as do regulative settings and levels of technological adoption. Such educational programs are therefore of high relevance in both countries for raising awareness among the population regarding cyber threats and the need for cybersecurity measures.

In both countries, awareness about cybercrime underlines the specially tailored need in policies and education concerning cybersecurity. Both nations can improve their cyber defenses against criminal activity if they address the specific challenges and barriers among their populations. Such perceptions of cybercrime are driven by a mix of factors, including technological progress, the deliberateness of cyber-attacks, exposure through the media, and demographic traits that characterize the segments. Addressing such perceptions is quite important in improving the level of resilience against cybercrimes and consequently reducing their occurrence through education and proper awareness.

3) Future Research

Future research should expand its focus to include additional countries with diverse technological environments and regulatory frameworks. This would enhance the understanding of global cybercrime dynamics and the effectiveness of various legislative measures. Additionally, conducting surveys and interviews with cybercrime victims, law enforcement officials, and policymakers could provide insights into the real impacts and practical response challenges.

Moreover, longitudinal studies can offer a deeper understanding of

how attitudes and behaviors towards cybercrime evolve over time amid changes in technology and legal environments. Longitudinal surveys collect data on the same subjects over a period, providing more reliable information through short-term memory and allowing for the analysis of changes to distinguish various aspects of change over time. These studies are crucial for understanding causality and identifying factors related to changes, making them essential for research and policy-making.

VI. Conclusion

The effect of the internet on the global economy and industrial revolution has been very great. It brought new, influential innovations in several industries by bringing transparency to the industrial process and making new business models and streams of revenue possible. As technological progress was fast, so were the new challenges brought about, to be met by careful analysis and proper responses.

Advanced infrastructure of the Internet enhances connectivity, communication, and collaboration. It drives economic growth and innovation, supports commerce, healthcare, education, and other industries by allowing entrepreneurs to break into new markets, improve operational efficiencies, and create new products and services. Secondly, it opens up more opportunities for education and access to information for the populace. In addition, this enhanced and heightened convenience and efficiency in daily life also helps provide an advanced line of defense for cybersecurity and improved digital security.

However, the invention of the internet increased cybercrime. This paper analyzes perceptions about cybercrime in South Korea and the UK, describing major differences and similarities between them. According to the analysis, both countries share conceptions that cybercrime is an increasing threat, but people's perception about the crime differs due to the cultural, social, and economic background.

The general public in South Korea tends to feel that most cyber activities are safer, while that of the UK is relatively more cautious. For instance, on issues to do with the security of using phones, the internet, or reading/sending emails, the South Korean public feels more secure, which might be an indication of the level of trust in

the security measures put in place in South Korea.

The perception of threats from cyber-attacks is higher among the UK public. They have been proven to be more aware of risks such as phishing, malware, ransomware, social engineering, and identity theft, hence the level of education and information provision about these risks within the UK is more profound compared to those in South Korea. On the contrary, the perception of the risks of these threats by the South Korean public stands relatively lower, hence requiring more effective cybersecurity education.

It is thus clearly the case that while the UK public has higher threat awareness and protective measures, it further highlights the need for education in cybersecurity and dissemination of information toward that end. On the other hand, with an extremely active digital participation, the South Korean public showed lower threat awareness and preventive measures, placing the need for systematic cybersecurity education.

참 고 문 헌

국내문헌

고려대학교 지식기반 포털시스템 https://portal.korea.ac.kr/front/Security.kpd

국가법령정보센터 (2015, January 15)
https://www.law.go.kr/precInfoP.do?mode=0&precSeq=177819&vSct=%EC%95%85%EC%84%B1%20%EC%9D%B4%EB%A9%94%EC%9D%BC

국외문헌

Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: why and how of it? Indian Journal of Medical Specialities, 4(2).

Avital, M., Dennis, A. R., Rossi, M., Sørensen, C., & French, A. (2019). The Transformative Effect of the Internet of Things on Business and Society. Communications of the Association for Information Systems, 44(1), 129–140.

Arakelyan, A. M. (2023). THE INFLUENCE OF SOCIO-ECONOMIC FACTORS ON THE PROCESSES OF PROFESSIONAL ORIENTATION AND EMPLOYMENT OF THE POPULATION. Èkonomika I Upravlenie: Problemy, Rešeniâ, 3/4(139), 124–127.

Bayard, E. E. (2019). The rise of cybercrime and the need for state cybersecurity regulations. Rutgers Computer and Technology Law Journal, 45(2), 69-96.

Bernik, I., Mesko, G., & Faculty of Criminal Justice and Security, University of Maribor, Ljubljana, Slovenia. (2011). Study of the perception of cyber threats and the fear of cybercrime.

Blank, G., & Lutz, C. (2016). Benefits and harms from Internet use: A differentiated analysis of Great Britain. New Media & Society, 20(2), 618–640.

Button, M., Hock, B., & Shepherd, D. (2022). Economic Crime. Routledge.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391–408.

Crown Prosecution Service. (2019, April 12). Cybercrime - Prosecution Guidance. Cps.gov.uk; Crown Prosecution Service.

Das, S., & Nayak, T. (2013). IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. International Journal of Engineering Sciences & Emerging Technologies, 6(2), 142–153.

Dashora, K., & Patel, P. (2011). Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, 3(1), 240–259.

Dimc, M., & Dobovšek, B. (2010). Perception of Cyber Crime in Slovenia. Journal of Criminal Justice and Security Year, 12(4), 378–396.

Donaldson, S., & Grant-Vallone, E. (2002). UNDERSTANDING SELF-REPORT BIAS IN ORGANIZATIONAL BEHAVIOR RESEARCH. Journal of Business and Psychology, 17(2).

Du Toit, R., Hadebe, P., & Mphatheni, M. (2018). PUBLIC PERCEPTIONS OF CYBERSECURITY: A SOUTH AFRICAN CONTEXT. Southern African Journal of Criminology, 31(3).

Evans, J. R., & Mathur, A. (2005). The value of online surveys. Internet Research, 15(2), 195–219.

Greenland, S., Schwartzbaum, J. A., & Finkle, W. D. (2000). Problems due to Small Samples and Sparse Data in Conditional Logistic Regression Analysis. American Journal of Epidemiology, 151(5), 531–539.

Gryszczyńska, A. (2021). The impact of the COVID-19 pandemic on cybercrime. Bulletin of the Polish Academy of Sciences Technical Sciences, 137933–137933.

Harwood, D., Rollins, J., & Dahl, E. (2014). NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA BARRIERS TO CYBER INFORMATION SHARING.

International Comparative Legal Guides. (2020, November 14). International Comparative Legal Guides International Business Reports.

Ivankova, N., & Wingo, N. (2018). Applying Mixed Methods in Action Research: Methodological Potentials and Advantages. American Behavioral Scientist, 62(7), 978–997.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014, July 25). Cybercrime classification and characteristics. University of Northampton's Research Explorer; Elsevier Inc.

Kamruzzaman, M., Islam, A., Hakim, M., Islam, M., Shahidul Islam, M., Hossain, & Hakim, A. (2016). Plight of Youth Perception on Cyber Crime in South Asia Plight of Youth Perception on Cyber Crime in South Asia. American Journal of Information Science and Computer Engineering, 2(4), 22–28.

Kanyuk, P. Á., Song, D., Wahdani, F., Gogokhia, G., Moe, T., & Bordás, P. (2018). Public Goods & Governance.

Karagiannopoulos, Dr. V., Kirby, Dr. A., Oftadeh-Moghadam, S., & Sugiura, Dr. L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. Computer Law & Security Review, 43, 105615.

Lapuh Bele, J., Dimc, M., Rozman, D., & Sladoje, A. (2014). RAISING AWARENESS OF CYBERCRIME -THE USE OF EDUCATION AS A MEANS OF PREVENTION AND PROTECTION.

국외문헌

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.
Lynn, P. (2009). Methods for Longitudinal Surveys.
Mabrouk, F., Abdalla, F., & Khiralla, M. (2020). Statistics of Cybercrime from 2016 to the First Half of 2020 Statistics of Cybercrime from 2016 to the First Half of 2020. IJCSN -International Journal of Computer Science and Network, 9(5).
Malina, M. A., Nørreklit, H. S. O., & Selto, F. H. (2011). Lessons learned: advantages and disadvantages of mixed method research. Qualitative Research in Accounting & Management, 8(1), 59–71.
Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the Internet on economic growth and prosperity.
Methmali, S. (2016). Perception of internet usage and its impact on cyber-crime in Sri Lanka internet usage and relationship with cyber-crime | IEEE Conference Publication | IEEE Xplore. Ieeexplore.ieee.org.
Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4).
Nabe, C. (2020). Impact of COVID-19 on Cybersecurity. Deloitte Switzerland; Deloitte.
Nabie, Y., Conteh, & Royer, M. (2016). The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. In International Journal of Computer.
Narahari1, A. C., & Shah2, V. (2016). Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India).
Nature of fraud and computer misuse in England and Wales: Appendix tables - Office for National Statistics. (n.d.). Www.ons.gov.uk.
Oates, B. (2001). Cyber Crime: How Technology Makes It Easy and What to Do About It. Information Systems Security, 9(6), 1–6.
O'Byrne, P. (2007). The Advantages and Disadvantages of Mixing Methods: An Analysis of Combining Traditional and Autoethnographic Approaches. Qualitative Health Research, 17(10), 1381–1391.
Odey, J., & Ana, P. (2021). A SURVEY ON THE PERCEPTIONS AND AWARENESS OF CYBER SECURITY IN NIGERIA.
Rahman, A., & Muktadir, Md. Golam. (2021). SPSS: An Imperative Quantitative Data Analysis Tool for Social Science Research. International Journal of Research and Innovation in Social Science, 05(10), 300–302.
Rayhan, R. U., Zheng, Y., Uddin, E., Timbol, C., Adewuyi, O., & Baraniuk, J. N. (2013). Administer and collect medical questionnaires with Google documents: a simple, safe, and free system. Applied Medical Informatics, 33(3), 12–21.
Rebman, C., Booker, Q., Wimmer, H., Levkoff, S., Mcmurtrey, M., & Powell, L. (2023). An Industry Survey of Analytics Spreadsheet Tools Adoption: Microsoft Excel vs Google Sheets. Information Systems Education Journal (ISEDJ), 21(5).
Rezk, A., Barakat, S., & Saleh, H. (2017). THE IMPACT OF CYBER CRIME ON E-COMMERCE. International Journal of Intelligent Computing and Information Sciences, 17(3), 85–96.
Rutter, M. (1994). Beyond longitudinal data: Causes, consequences, changes, and continuity. Journal of Consulting and Clinical Psychology, 62(5), 928–940.
Salmon, K. (2024). UK hailed as Europe's most advanced digital economy. ChannelLife UK.
The Cyber (Sanctions) (EU Exit) Regulations 2020. (2020). Legislation.gov.uk.
The impact of scams and fraud on isolated older people The unseen price of a scam. (2023).
Toss Pay | Checkout Payment | Alipay Docs. (2024). Global.alipay.com.
Van Selm, M., & Jankowski, N. W. (2006). Conducting Online Surveys. Quality and Quantity, 40(3), 435–456.
Viano Editor, E. (2016). Cybercrime, Organized Crime, and Societal Responses International Approaches.
White, K. (2013). The rise of cybercrime 1970 through 2010. A tour of the conditions that gave rise to cybercrime and the crimes themselves.
Yang, S. (2017). Networking South Korea: Internet, nation, and new subjects. Media, Culture & Society, 39(5), 740–749.

[Abstract]

Cybercrime perception between the UK and South Korea

University of Portsmouth, Woo[1]
Chung-ang University, Lee[2]

There are lively debates on cyber crime and how different cultures perceive digital threats, which this dissertation aims to expand. It explores the ways that cyberfraud is perceived and experienced by people in the UK and South Korea. The paper also showed results for different age groups, exploring how the public perceives cyber theft. The social implications of this research are articulated in collected data which alludes to the ephemeral and protean nature of cyber threats; a heterogeneous experience amongst victims residing within differing cultural arenas; whilst enunciating mounting challenges concerning efficacious prevention and response. The research took on a mixed-methods technique and used both closed-ended and open-ended questions in an online survey. This method provided a comprehensive investigation of how the public perceive and experience cyber fraud among individuals aged 18 to 54.

The thesis also shows how understudied cyber fraud is and to what extent cultural context plays a role in shaping such an understanding. It also highlights the importance of targeting cyber crime prevention and response efforts for specific demographic groups. Dealing with these issues adds to the broader global effort against cyber crime, he says. It provides good practices enshrined in law and policy tools intended to further enhance the Cyber security posture of Responsible Entities, improving alertness. The findings of this study underscore the need for a subtle and culturally sensitive cyber security

---

1 1st author, University of Portsmouth
2 2nd author, Chung-ang University

approach. It raises the broader implications of its findings for developing robust regulations that can adapt to the dynamic and international nature of cyber threats. The authors state that further research should effort to replicate these findings thereby informing the global discussion with respect to cyber crime and its prevention.

Key words: South Korea, The United Kingdom, cyber crime, perception, cyber fraud