Child Pornography Websites on the Darknet

Julak Lee

Abstract: ***Cybercrime has been moving to the darknet which provides privacy and anonymity to users. Despite international efforts to eradicate child pornography, websites to distribute lurid materials are found to be resilient. Due to the significance of the criminality, law enforcement authorities have taken covert measures to dismantle the leadership of these websites, focusing on arresting the organizers and core members. In this paper, two cases involving child pornography websites were examined to disclose how these websites were structured and managed as well as investigation strategies and tactics employed by investigation agencies. Some similarities were identified during pre-arrest and after-arrest stages for an investigation goal and evidence verification, respectively. However, during a deanonymisation stage the two agencies used different investigation strategies to approach and arrest the target criminals. It is very likely that darknet websites will be managed in diverse manners, or that more anonymity and encryption will make pornography circulation structure invisible and unreachable. In this study, it was argued that perfect anonymity is not provided to the darknet users and that investigation agencies should make technical and social engineering efforts to deanonymise identities of criminals.***

Keywords: Child Pornography, Darknet, Criminal Investigation, Cryptocurrency, Management Style.

I. INTRODUCTION

In cyber security, darknet is a term that has been mentioned a lot in recent years. The darknet is a type of cyberspace which provides privacy and freedom to users. This allowed for some people to engage in constructive social and political activities, while for others to expose and realise their criminogenic desires. In general, the public and media perceived that darknet was a venue for criminals[1, 2, 3]. This negative perception on the darknet is also substantiated by academic research. Some academic papers[4, 5] found that the darknet is a hotbed for all sorts of illegal transactions. In particular, drug transactions via cryptocurrencies were the representative illegal activities, taking the vast majority of all transactions on marketplaces[6, 7]. Besides drugs, users can buy any products or services such as arsenal, pornography, counterfeit, exotic animals, credit card and personal information, and hacking software which cannot be normally sold and bought offline or on the normal Internet[8, 9, 10].

In recent years, many law enforcement agencies around the world had to face cybercrime on the darknet, and they tried to cooperate with other domestic and international counterparts. For example, FBI launched Operation Pacifier from January 2015. It was an unprecedentedly large investigative campaign against a child pornography website, *Playpen*. Cooperation among dozens of law enforcement agencies resulted in arresting about 1,000 paedophiles and rescuing around 350 children[11]. However, international operations highlighted some challenges pertaining to legal, jurisdictional, and technical issues. Cybercriminals and investigators are competing in a cat and mouse race in that the darknet itself evolves constantly following technological developments.

It is well known that the Internet has become the principal tool for sharing and distributing child pornography[12]. Likewise, one of the most vicious cybercrime on the darknet is child pornography[13]. Using the topic-model based text mining technique[14] found that child pornography has a relatively heavy weights in terms of the degree of presence on the darknet. The fact that child pornographic images and videos are circulated and sold online indicates that there are demands and supplies for those images and videos. The problem lies in the fact that continuous production of child pornography accompanies child victimisation. Victimised children in horrific footages suffer long-term physical and psychological damages.

Based on the understanding of the "dark" cyberspace, this paper will review and analyse two cases involving different darknet websites on child pornography. The first case is on *Gift Box Exchange* which was run by two operators (i.e., one American and one Canadian). It was successfully taken down by the US Homeland Security Investigations (HIS) in December 2016. The second case is on a website run by a Korean. He was arrested by the South Korean police in May 2017. The case studies were based on data from two sources. Documents from the media, government publications, and academic research were used. In addition, I have interviewed two law enforcement officers who were involved in the investigation of those cases. One interviewee was an investigator from the HIS involving the first case and the other interviewee was an inspector from the Korean police concerning the second case.

Drawing on documentary research and interview analysis, firstly, I will investigate how the child pornography websites operate. As a child pornography website is a venue for social interactions of paedophiles, it is of great importance to have a close look at the structure and management style of these websites. This examination will shed light on perceptions and behaviours of child sexual predators. After the examination of child pornography websites, secondly, I will analyse investigative techniques and the course of investigations ranging from approaching, identifying and arresting criminals to shutting down those websites. It is expected to illustrate the process of deanonymising criminals' identities and legal and technical challenges that law enforcement officers encounter. An investigation on the darknet requires a different set of investigative skills,

Revised Manuscript Received on July 22, 2019.

Julak Lee, Department of Security Management, Kyonggi University, 154-42 Gwanggyosan-Ro, Suwon-Si, 16227, Korea. Email: julaklee@kyonggi.ac.kr

which is a great challenge to law enforcement agencies.

II. LITERATURE REVIEW

A. Understanding the darknet

The darknet as a hidden space in the Internet keeps users anonymous, and law enforcement agencies have recently begun to understand what the darknet is. Because of anonymity it provides, it is considered as an appropriate space for people who need online anonymity: not only for many legitimate uses, but also for criminal activities[15]. Its technical complexity almost guaranteed that it is difficult to identify the user than the open online space. Like technical 'cat and mouse' games, law enforcement agencies had to develop investigative tools and tactics that corresponded to the technical developments on the darknet[7].

First of all, for future discussion, I need to define and distinguish surface web (or clear web), deep web, and darknet. The surface web is a collective term for public websites that people can often search through Google or Yahoo[16]. Deep Web is a collective term for all web pages that search engines cannot find, such as user databases, internal corporate networks, webmail pages, payment pages, and pages requiring login. The amount of data in the deep web is allegedly about 450 to 550 times larger than that of the surface web[17]. Finally, darknet is part of the deep web, which refers to a specific class of websites that exist on an encrypted network and that cannot be found or visited using a common search engine or common browser. To access the darknet users need to use particular web-browsers such as Tor (The Onion Router) or I2P (Invisible Internet Project) which make IP tracking almost impossible[18].

The Tor uses a network of volunteer computers to route web traffic and the communication at each relay server is encrypted, which indicates that the traffic cannot be traced to the original user[16]. When accessing a regular website via the Tor browser, the IP address is changed through at least three relay servers (i.e., entry, middle, and exit nodes). Hence, even if one of the relay servers is looked into, the message can hardly be seen[19]. It is known that about 6,000 of these relay servers are currently operating in the world.

The purpose of the Tor browser can be broadly divided into two. The first is to hide their IP address for privacy while accessing regular websites. Figure 1 shows the path after logging on to www.daum.net through the Tor browser. You can see that it is connected to the Internet via Tor browser (user) -> USA -> Netherlands -> Swiss relay servers.

Fig. 1. Accessing a normal website via the Tor browser

The second is to access websites on the darknet (i.e., .onion sites). In particular, the darknet has provided hidden services, making it harder to track sites and users. Among five characteristics of encryption (i.e., privacy, authentication, anonymity, virtual currency, and hidden exchanges) the Tor has two characteristics which allow for anonymous browsing and hosting of anonymous information exchanges[5].

B. Associated criminality

As offline crimes migrated to online, now cybercrimes are migrating from the surface web to the darknet[20]. In fact, some law enforcement agencies recently realised that an offline case is in fact related to the darknet as their investigation progresses. In July 2017, FBI and Europol launched successful campaigns against AlphaBay and Hansa[21]. They shut down these two major darknet marketplaces which traded various drugs and other illegal products and services. In the case of AlphaBay, tens of thousands of users have traded $600,000 to $800,000 daily earlier in 2017 and was notorious as the largest marketplace by far[22]. Despite this high criminogenic criminality, it took some time for the US authorities to notice this marketplace. However, there was a warning sign for the authorities. It was revealed that some people in the US who died of drug overdose bought large amount of fatal drugs from AlphaBay[20, 22]. If the authorities have not found the linkage of their deaths to this darknet marketplace, there might not have been the successful shutdown of the website.

Among many types of cybercrimes on the darknet, child pornography offenders could be riskier than other types of offenders[23]. argued that child pornography offenders are more likely to offend again either general crimes or sexual crimes. Therefore, many western countries such as the US, Canada, the UK heavily penalise production, dissemination, and possession of sexually explicit images of a minor based upon the UN's Convention on the Rights of the Child. The South Korean law(the Act on the Protection of Children and Juveniles from Sexual Abuse) also proscribes these activities to protect children and juveniles from sexual abuse. However, there is a lack of awareness of this prohibition. For example, although possessing child pornography is illegal in Korea, which could face imprisonment up to 1 year or a penalty up to 20 million won, this illegality is not well known to the general public[2, 24].

Child pornography users are proactive and interactive beyond sharing illegal materials. Many of them are actively engaged in discussions of related topics. Under the shadow of anonymity, users have a consensus that their sexual attraction to children is unreasonably discriminated in society, assuming that their propensity to child sexuality is one of normal sexual inclinations. They feel psychological support and mental peace based on the feeling of unity with other users[25, 26]. They are willing to share their personal stories in a comfortable manner, unlike other crime types[5].

Although criminal activities on the darknet evolved fast, law enforcement agencies were not aware of the risk that the darknet poses to society. Still law enforcement agencies relied on traditional methods of arresting and prosecuting cybercriminals on the darknet, having a limited extent of technical capacity and international cooperation[6].

On the darknet, investigation agencies frequently conduct a sting operation in the way that an undercover agent penetrates into the target website as a normal user[27]. Organizers and users of child pornography websites know this. Therefore, the organizers and users are concerned about security of their website to prevent their website from being caught by the agencies, and for this reason they have used darknet space[28].

It cannot be argued that simply closing a website has a significant effect on restraining online criminal activities. In fact, there are many alternative websites which can take its place[28]. As a representative example, since Silk Road, which was the top spot for drugs and illegal goods on the darknet, was shut down in October 2013, dozens of other trading markets appeared and existing users and suppliers moved to these sites[4, 29]. The displacement effects are also applied to child pornography websites. As darknet users are generally suspicious of law enforcement activities against them, an abrupt closure of a website is likely to lead to a stampede of the users. A crime suppression effect is lowered because the users are aware of the situation and move to other similar websites. Investigators are also aware of the balloon effect of darknet trading markets. Therefore, rather than closing the market prematurely, they are trying to arrest key players of the website on the target as well as to curb potential displacement of users.

Online distribution of child pornography can be systematically organized by criminal groups, but in most cases, this is done through communications and transactions among interested individuals[28]. Online pornography transactions can be uploaded on a specified website, or exchanged via email, messages, bulletin boards, group chat, and interpersonal networks. As pornography distribution methods increase and diversify, identifying users involved in child pornography became a challenge for criminal investigators. Illegal activities perpetrated by a criminal group can be stamped out relatively easily if the authorities identify the structure of the group. However, individual users on the darknet do not have any affiliation with a criminal group. In this case, to arrest child pornography-related suspects, guerrilla investigation methods should be selected focusing on individual transactions.

III. CASE STUDIES: ANALYSES AND RESULTS

A. Case A

1) Management of the website

Benjamin Faulker and Patrick Falte hosted a child pornography website, Gift Box Exchange, from July 2015 to December 2016. They also ran another website, called Childs Play, which was the largest of its class on the darknet from April 2016 to September 2017[30]. In October 2016, they were arrested by the HIS of the US. Investigations into Gift Box Exchange resulted in arrests of a total of 158 people, of which 98 people were foreigners. Not all were arrested at the same time but were arrested sporadically in cooperation with other US or foreign law enforcement agencies.

It is difficult to see the website's management as a criminal organization. The management consisted of individuals with similar sexual taste. They never met off-line, and only the two organizers met two or three times until their arrests. The organizers met online, talked, exchanged opinions, made decisions, and eventually decided to create the Gift Box Exchange. Compared to widespread use of cryptocurrencies in marketplaces, this website did not rely on cryptocurrencies as a medium of transactions. Instead, users share and exchange their own sexual materials rather than buying and selling pornography. This way of transactions can be understood as a form of bartering. The Gift Box Exchange is designed to encourage interactions in forums so that users can communicate with each other while sharing child pornography. In the early days of its operation, the website was operated under the name of Pedos Giftbox, and had to upload child pornography for subscription and approval.

One important feature of the website was the star rating system. The operators measured the extent of participation of a user on the website and gave the corresponding number of stars to the user. The number of stars determined the position and status on the website. The best star rating, 7 stars, was given only to the two organizers and they had full access to all data. One was in Canada and the other was in Virginia, USA. Next, moderators were given six stars, granted administrative rights to the website, and managed forums for users to post their articles. The next was VIP status and VIPs were given 5 stars. To get VIP status, a user had to steadily upload new pornography. This requirement to get VIP status has provided a strong reason for users to engage in sexual abuse of children and to record them. In addition to uploading new child pornography, proactive interactions with other users were necessary to earn the VIP status. This kind of participation-based rating system was similar to common social media websites (e.g., Reddit). Examples include writing comments on posts, recommending other users, or providing operational or technical support. When this website opened, the number of registered users worldwide reached around 400,000. Because it was virtually impossible for the investigating authorities to track all of these users, they have prioritized and conducted investigations by selectively choosing users based on who could bring a great return on investment.

2) Profiling the website and suspects

When investigating a website where users engage in website operations and interact with each other, it is important to first look at the public profile of users. You need to check their basic information: How often they logged in, what local time they logged in, how many clicks (e.g., recommendations, thanks, or likes) they gave or received. In addition, investigators can check what they post or talk about, what they want, and how they communicate. Looking at these various aspects of the website will not only outline the profile of the organizers and key players, but also identify the general atmosphere of the darknet space.

Once the overall atmosphere of the website is examined, it is necessary to make the profile of the target user for identification and arrest. It is important to infer nationality, race, age, gender, occupation, range of actions, and so on.

If you look closely at what the user has written, user-generated information becomes a key clue. The time at which the article is posted can be used to infer what time zone the user belongs to. Or the user may have referred to his location, economic, political, or cultural issues in his/her locality. Looking at these public information, it is possible to configure the online persona of the target user.

3) Approaching a suspect

It is vital to form relationships with a suspect through continuous dialogues based on social engineering techniques. A software program does not necessarily locate exact whereabouts of the suspect. It is more important to draw a mistake from the suspect while building trust. Because they have avoided arrest from the authorities for years, they have psychological complacency which could lead to a single mistake. Therefore, their personal preference such as what they want or what they are uncomfortable with is invaluable information.

First, they were uncomfortable with the slow speed of the Tor browser, and this inconvenience was mentioned in conversations with others. To share materials, they typically upload and download child pornography from hundreds of megabytes to dozens of gigabytes. It takes several hours even to transfer a video of a few minutes. It is therefore important to persuade them to use open IP addresses, instead of Tor, after establishing trust through ongoing conversations. This website had the ability to send and receive private messages. You can use this feature to personalize the conversation between the target suspect and the undercover agent so that the suspect can be brought up to the surface. In the US, the manner in which investigators approach pedophiles is possible only within an ethical and legal scope. It is illegal for US federal investigators to manage child pornography sites or distribute pornography. Instead, they can be engaged in providing information on how to effectively exchange pornography with users on such websites. In contrast, some countries (e.g., Australia) to some extent allows investigators to manage pornographic websites or to distribute child sexual materials for the purpose of arresting perpetrators. Australian police faced a heavy criticism when it was revealed that a child pornography forum, Childs Play, was hosted by Task Force Argos of the Queensland Police Agency for almost a year[27].

Second, users were sensitive to maintaining their status on the website. In particular, VIPs were keen on keeping their status because VIPs have access to more child pornography. It was also important to build trust among users while maintaining a good reputation on the website. That way, you can get referrals from other users, and others will trust you to download the pornography you uploaded. This type of trust-based website management seems to be incongruent with an anonymous characteristic of the darknet. It is noteworthy, however, that users' status cannot be purchased via virtual currencies, but was based on reputation and trust from other users.

B. Case B

1) Management of the website

A suspect (website organizer) installed and operated a child pornographic dark website server at his home from July 2015 to March 2018. The number of registered users on the website was about 1.2 million worldwide, and the number of paying users was about 4,000. When a user pays a certain amount of Bitcoin, the website organizer gave the corresponding amount of points to the user so that the user can download child pornography materials. During the operation of the website, the suspect received 415 Bitcoins though transactions of 7,330 times from these paying users. After arresting the website operator in May 2017, separate investigations were conducted against domestic and international users. Before the media reports that the operator was arrested were released, the individual users were booked, and their houses were searched for confiscation. Most of the users were unmarried men in their twenties, most of whom were office workers and college students, including some with stable jobs such as teachers, government officials, and public health workers[2]. Most of them were first-time criminals, but some had criminal history of sexual offences of other types. These are summarized in Table 1.

Tabel 1. Summary of the overall trannsactions during the operation period[32]

Website operating period	Total users	Bitcoin transactions (users -> organizer)	Maximum amount of transaction	The number of uploaded videos	The number of downloads
2015. 7 – 2018. 3	1,283,255	415(BTC) 7,293 times	1.875 BTC 29 times	221,301	73,722 362,260 times

The website operator was familiar with IT and web programs. In 2015 he purchased a child pornography website with $5,000 through TorChat on the darknet. After this, he secured a large volume of child pornography and purchased a large-capacity HDD for storing those materials. He advertised the website in Hidden Wiki to attract users. After opening a Bitcoin account from a domestic exchange for transactions, transactions with users were carried out via Bitcoin. He allowed users to download videos by deducting points which could be bought by paying Bitcoins (100 points for 0.01 Bitcoin) and one point was deducted for one child pornography and unlimited access was granted for 6 months for users if they pay 0.03 Bitcoin as shown in Figure 2[24].

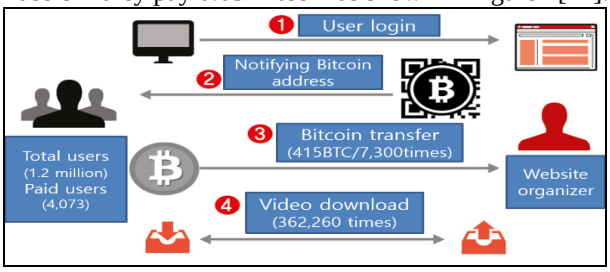

Fig. 2. Simplified diagram of the darknet website operation

2) Deanonymizing the website organizer

In September 2017, the HIS of the US requested an investigation into a darknet site "mt3plrzdi*******.onjon" dedicated to child sexual exploitation. Since the website sold child pornography

materials for profits, the police launched a criminal investigation into the website for violating the second clause of Article 11 of the Act on the Protection of Children and Juveniles from Sexual Abuse. The clause stipulates that a person who sells child pornography for profits could face imprisonment up to 10 years. At the outset of the investigation, investigators sent a small amount of Bitcoins to the address given on the website. After that, they looked at the transaction address using Chainanalysis and found transaction history between the organizer's bitcoin address and three domestic exchanges (i.e., Bithumb, CoinOne and Korbit) as shown in Figure 3.

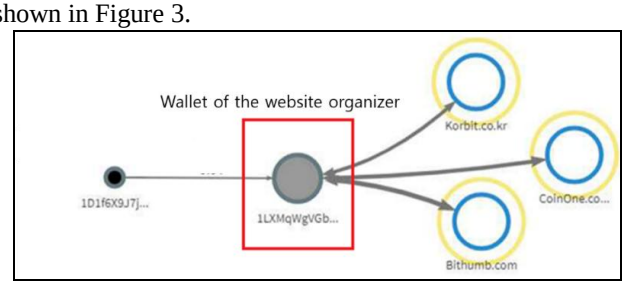

Fig. 3. Bitcoin flows between the organizer's wallet and domestic cryptocurrency exchanges

Although users transferred Bitcoins to various Bitcoin addresses, the Chainanalysis clustering technique found that those multiple addresses belonged to the operator's own wallet. This technique is a useful analysis method when multiple Bitcoin addresses are used in transactions. It can find that multiple addresses eventually belong to one wallet (cluster). In fact, Bitcoin transaction history is searchable from public web sites such as bitcoin.info, but it is difficult to analyze the flow of Bitcoin transactions if Bitcoins are traded on a large scale. However, with Chainanalysis, you can see the entire transaction details of a specific Bitcoin wallet and the transaction history between two wallets. Using these two features, investigators could extract details of the transactions from domestic exchange wallets to the organizer's personal wallet among the total transactions. Based on the details from this analysis technique, investigators asked a court for a search warrant against three major exchanges to seize personal information and transactional data in relation to the organizer's wallet. Requested information include membership information, access log, Bitcoin deposit and withdrawal history, details of buying and selling, and Korean currency deposit and withdrawal history.

3) Seizure of cryptocurrency and criminal proceeds

Collecting digital evidence in a crime scene is of importance. On the computer that has been seized, there were records of searching phrases such as "caught under the Act", "the Act my life", "the Act the end?" and "the Act sharing hard drive" through search engines. These phrases indicate that the organizer was aware that his online activities were illegal. This evidence could be submitted in a court against him. In particular, investigators should confiscate the files and printouts of the suspect's wallet and transfer cryptocurrencies of the suspect to an offline wallet owned by the investigation agency or ask for suspension of transactions if no agreement is granted. If the suspect uses an overseas exchange account, investigators must transfer it to an offline wallet owned by the investigation agency or confiscate it through the International Criminal Justice Assistance (MLAT) request. In addition, if cryptocurrencies were converted into financial assets, related financial account should be identified and suspension of transactions should be requested.

4) Judging whether a material is child pornography

In order to punish the suspect, videos distributed on the website must be judged as child pornography. In other words, the materials should be determined as "pornography of children and youths" as defined in Article 2 of the Act on the Protection of Children and Juveniles from Sexual Abuse. Firstly, among the total 221,301 uploaded video files 1,384 duplicate files were removed based on hash values. Secondly, hash values of the remaining 219,917 cases were compared with databases from Project VIC, MS Photo DNA, and MD5. Finally, the examination resulted in a total of 2,792 matches. Based on these 2,792 matching hash values, investigators examined thumbnail images of video files stored in the PC of the suspect and concluded that 3,055 video files expressed sexual acts with children or adolescents and these files can be presented as evidence to a court.

IV. DISCUSSIONS OF CASE STUDIES

Analyses on the two cases revealed some similarities and differences. Similarities were found in pre-arrest and after-arrest stages. Firstly, before arresting criminals, both agencies had the same goal of investigating child pornography websites. Secondly, after arresting criminals both agencies worked together with public and non-public organisations to demonstrate the accuracy of collected evidence. However, when both agencies approach and arrest the websites' organizers, they relied upon different investigation strategies to deanonymise them.

A. Similarity 1: Goal of child pornography investigations

The purpose of the investigation agencies in both countries was to eradicate production and distribution of child pornography. This could not be achieved by shutting down websites, but by arresting the organizers and VIPs of the child pornography website. If the investigation authorities arrest a small number of site administrators and close the website, it will create a vicious cycle in which a majority of users who are key players in the structure (for example, moderators and other active users) are scattered around to open or use other websites.

Thus, in both cases, efforts were made to identify and arrest as many child pornography website users as possible. In the HSI case, a total of 158 people whose IP addresses were identified were arrested and 98 of them were foreigners living abroad. In the Korean case, the police checked the details of Bitcoin remittance history and search warrants were issued to seize data on the target individuals from the domestic cryptocurrency exchanges. After all, 156 people were arrested. Both cases involved cooperation with domestic or overseas investigative agencies based on the jurisdiction of target users.

Both the US and Korean agencies did not shut down the websites after rounding up the operators. In the Korean case, the police displayed a notice on the website, saying that the website was under repair, so as not to be aware of the fact that the operator was arrested. On the other hand, the Gift Box Exchange was left in normal operation for one month for the same reason[30].

B. Similarity 2: Cross-border cooperation with public and non-public agencies

Most child pornography investigations are conducted in collaboration with Project VIC, an international child abuse eradication program. Project VIC was created with the aim of developing innovative technologies and victim-centered methodologies to rescue victims of child abuse and sexual violence and arrest the perpetrators. To this end, it works with law enforcement and private sector partners to provide solutions to real-world events. It has created a standardized form of database that enables sharing data (hashes, feature points) related to child pornography and cooperates with other organisations such as ICMEC, US Internet Crimes against Children Task Forces, and INTERPOL. The two cases studied in this paper also cooperated with the Project VIC. The HSI actually manages the Project VIC related child pornography database and provides hash values to law enforcement agencies around the world. Because NICMIC is not a law enforcement agency, it cannot manage seized child pornography. In order to judge whether or not pornography involved children and teenagers, both agencies had to make a comparison with Project VIC's Hash Value DB. This finding supports the argument that international cooperation is vital in addressing cybercrimes on the darknet[32]. In both cases suspects resided in foreign countries as well as in the country concerned, and were able to arrest more than 100 suspects by cooperating with the authorities in charge of national investigation. In the Korean case, a large number of users of the website were arrested in cooperation with the US Department of Homeland Security (HSI), the IRS, the Federal Attorney's Office, and the National Crime Agency of the UK.

C. Difference 1: Different investigation strategies due to different management styles of the websites

In the US HSI case, the Gift Box Exchange was a collection of users gathered for the purpose of sharing child pornography. The two operators were also pedophiles sharing the same intention with other users. On the other hand, in the Korean case, the website operator simply managed the website for profit. He was paid by Bitcoin to avoid attention from the police. However, the cryptocurrency itself became a crucial subject of criminal investigation. Also, after the arrest of the suspects, criminal justice procedures such as seizure and confiscation of criminal proceeds from personal wallet evolved around the cryptocurrency.

On the other hand, the HSI case in the US is not for profit but for the distribution and sharing of child pornography. This case did not involve any Bitcoin transactions, so it was impossible to track suspects through cryptocurrencies. Instead, it was necessary to identify target users through examination of public profiles, posts and comments, and dialogues between the users or the management and users. In order to arrest the suspects after the identification, investigators had to persuade them to reveal their IP addresses by continuing the conversations with the suspects through social engineering techniques. The most important strategy in this approach was to build trust through human relationships and interactions rather than technical interventions. It was primarily aimed at causing suspects to make mistakes. Users of child pornography websites have had some complacency because they have been using this sort of websites for years without receiving attention from law enforcement agencies or legal sanctions. Inducing the suspects to use the surface web is a challenging task and investigators needs to take needs of users and disadvantages of using the darknet into consideration.

V. CONCLUSION

Various crimes are occurring in the anonymous online space, and the investigation agencies should prepare against it from now on. In particular, child pornography websites have been operated and maintained with high resilience based on the anonymity that the darknet provides. In this paper, I examined the two pornography distribution websites among the various types of darknet websites. Although it appears that these two websites were quite similar in many ways (i.e., similar goal of distributing child pornography and operating in the same cyberspace), the structure and management style of the websites were different. The examination of the investigation cases of the US and South Korea pointed to some commonalities. First, it was found that the purpose of the investigation was not the closure of the website but eradicating child victimisation through mass arrests of users. Second, transnational cooperation is needed among law enforcement agencies and private organisations. On the other hand, it is noteworthy that the difference between the two cases was the difference in the investigation methods, and the difference in the manner of website operations contributed to disparate investigation methods. In the future, it is very likely that darknet websites will be managed in diverse manners, or that more anonymity and encryption will make pornography circulation structure invisible and unreachable. In this case studies, it was argued that perfect anonymity is not provided to the darknet users and that investigation agencies should make technical and social engineering efforts to deanonymise identities of criminals.

REFERENCES

1. Farrell P, Inside the darknet: where Australians buy and sell illegal goods. The Guardian, 4 July, 2017. Retrieved from https://www.theguardian.com/technology/2017/jul/04/inside-the-darknet-where-australians-buy-and-sell-illegal-goods
2. Jeong S, First arrest of the organizer of a darknet website. Korea Times, 1 May, 2018. Retrieved from http://www.hankookilbo.com/v/1be67abbf8b84905aecc0d83445ff199
3. Ko J, Arrested the organizer of a child pornography website on the darknet, a hot bed for cybercrimes. Asia Economy, 2 May, 2018. Retrieved from http://www.asiae.co.kr/news/view.htm?idxno=2018050215543463052

4. Dolliver DS, Kenney JL. “Characteristics of drug vendors on the Tor network: a cryptomarket comparison” Victims & Offenders. 11(4), 600-620, 2016.
5. Moore D, Rid T. “Cryptopolitik and the Darknet” Survival. 58(1), 7-38, 2016.
6. Buxton J, Bingham T. “The rise and challenge of dark net drug markets” Global Drug Policy Observatory 7, 1-24, 2015.
7. Owen G, Savage N. “The tor dark net” Global Commission on Internet Governance. 20, 1-9, 2015.
8. Chertoff M, Simon T. “The impact of the dark web on internet governance and cyber security”. Global Commission on Internet Governance. 6, 1-8, 2015.
9. Holm E. “The Darknet: A New Passageway to Identity Theft” International Journal of Information Security and Cybercrime. 6(1), 41-50, 2017.
10. Owen G, Savage N. “Empirical analysis of Tor hidden services” IET Information Security. 10(3), 113-118, 2016.
11. FBI. ‘Playpen’ Creator Sentenced to 30 Years. 2017. (Press release) Retrieved from https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years
12. Quayle E, Taylor M. “Child pornography and the Internet: Perpetuating a cycle of abuse” Deviant Behavior, 23(4), 331-361, 2002.
13. Maras MH. “Inside Darknet: the takedown of Silk Road: Marie-Helen Maras reports on the unexplored underworld of cyberspace” Criminal Justice Matters. 98(1), 22-23, 2014.
14. Spitters M, Verbruggen S, Van Staalduinen M. “Towards a comprehensive insight into the thematic organization of the tor hidden services” In Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint. 220-223, 2014.
15. Henri V. “The Dark Web: Some Thoughts for an Educated Debate” Canadian Journal of Law and Technology. 15(1), 85-98, 2017.
16. Weimann G. “Terrorist migration to the dark web” Perspectives on Terrorism 10(3), 40-44, 2016.
17. Oh HJ, Won DH, Kim C, Park, SH, Kim Y. “Design and implementation of crawling algorithm to collect deep web information for web archiving” Data Technologies and Applications. 52(2), 266-277, 2018.
18. Byrne JM, Kimball KA. Inside the Darknet: Techno-crime and criminal opportunity. In: Moriarty, L.J. ed. Criminal justice technology in the 21st century, 3rd ed. Illinois: Charles C Thomas. 206-232, 2017.
19. Watson KD. “The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks” Wash. U. Global Stud. L. Rev. 11, 715, 2012.
20. Department of Justice US. Attorney General Jeff Sessions Delivers Remarks at Press Conference Announcing AlphaBay Takedown. 2017. (Press release) Retrieved from https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-delivers-remarks-press-conference-announcing-alphabay
21. Baraniuk C. AlphaBay and Hansa dark web markets shut down. 2017. Retrieved from http://www.bbc.co.uk/news/technology-40670010
22. Popper N. AlphaBay, Biggest Online Drug Bazaar, Goes Dark, and Questions Swirl. New York Times, 6 July, 2017. Retrieved from https://www.nytimes.com/2017/07/06/business/dealbook/alphabay-online-drug-bazaar-goes-dark.html
23. Seto MC, Eke AW. “The criminal histories and later offending of child pornography offenders” Sexual abuse: a journal of research and treatment. 17(2), 201-210, 2005.
24. Lee J. Arrested the organizer of a child pornography website on the darknet, the first case in Korea. Herald Economy, 1 May, 2018. Retrieved from http://news.heraldcorp.com/view.php?ud=20180501000416
25. Taylor M. The nature and dimensions of child pornography on the Internet. Combating Child Pornography on the Internet, Vienna. 1999.
26. Wall D. Cybercrime: The transformation of crime in the information age (Vol. 4). Cambridge: Polity; 2007.
27. Knaus C. Australian police sting brings down pedophile forum on dark web. The Guardian, 7 October, 2017. Retrieved from https://www.theguardian.com/society/2017/oct/07/australian-police-sting-brings-down-paedophile-forum-on-dark-web
28. Wortley R K, Smallbone S. Child pornography on the internet. Washington, DC: US Department of Justice, Office of Community Oriented Policing Services; 2006.
29. Van Buskirk J, Roxburgh A, Bruno R, Naicker S, Lenton S, Sutherland R, Whittaker E, Sindicich N, Matthews A, Butler K, Burns L. “Characterising dark net marketplace purchasers in a sample of regular psychostimulant users” International Journal of Drug Policy. 35, 32-37, 2016.
30. VG. Breaking the darknet: why the police share abuse pics to save children. 7 October, 2017. Retrieved from https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en
31. National Police Agency. First arrest of a child pornography website organizer on the darknet. (Press release) 2018.
32. Şen S. “Organizational Solution Recommendations to the Problem of Child Pornography on the Internet”. Journal of Learning and Teaching in Digital Age. 3(1), 45-56, 2018.

AUTHORS PROFILE

Julak Lee Julak Lee is a professor in the Department of Security Management at Kyonggi University, South Korea. He received his Ph.D. in Criminal Justice at the University of Portsmouth. His primary interests are in security management and crime prevention. Currently, he is the president of the Korean Security Science Association.