116-0002
2-20-7 Arakawa Arakawaku Tokyo Japan

ISSN 2423-8783

International journal of criminal study

2019 4(1)

<Index>

1. Analysis and Responsive Measure of Smart Home SECURITY Threat in IoT.
/ Lee Jae-young
2. A Study on an Autonomous Committee for Countermeasures against School Violence for CRIME Prevention.
/ Kim Hak-bum
3. Research on Causes and Countermeasures of Juvenile SNS CYBER Verbal Abuse.
/ Kwon Hwa-suk

J-INSTITUTE

2019 4(1) 1-6

Submission: 2019/05/10, Peer review: 2019/05/20, Accepted: 2019/05/25, Published: 2019/06/30

International journal of criminal study

Publication state: Japan
ISSN: 2423-8783

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: klitie@semyung.ac.kr

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/criminal.2019.4.1.01

Analysis and Responsive Measure of Smart Home SECURITY Threat in IoT

Lee Jae-young

Semyung University, Jecheon, Republic of Korea

Abstract

Smart Home, also known as Home IoT, refers to the product, service and solution remotely moni-toring, controlling and operating domestic devices through the connection to the wireless network with mobile phones and computers. Smart Home has been developed into diverse versions, however its security still owns vulnerability in its device, network and privacy. Considering Smart Home security employs Public network, thus it is relatively more vulnerable than the ones, such as Smart Factory with Private network. Smart Home devised for convenience and safety of lifestyles may result in a disaster in private lives, if its security vulnerability is not resolved. The thesis examines past security threat cases in Smart Home environment, analyzes them in three different aspects – device, network and privacy – then would propose a counter-measure against the threats.

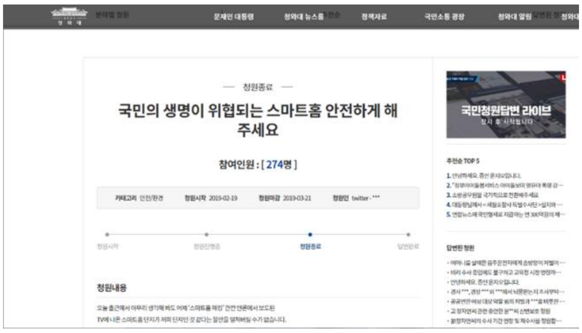
[Keywords] ***IoT, Smart Home, Hacking, CCTV, Security***

1. Introduction

On June 2015, an Internet website exposing 9,187 CCTV videos of 117 countries throughout the world was captured. Among the hacked CCTVs, 344 are installed in South Korea – on public streets, pathways around housing, significant government facilities, tuition centers, hospitals, offices and households. People, who know the website, could monitor the real-time CCTV videos everywhere in the world, and even could record and remotely control them[1]. Furthermore, household electricity charge had become 0 due to hacking on apartment management system of a metropolitan apartment, and another apartment doors had been disabled by the Internet malfunctioning[2]. Picture 1 is the petition content in National Petition Board of the Blue House on February 2019.

Thanks to the advancement of information and communication, and development of connectable devices to the network, development and distribution of distribution of IoT and Smart Home have been accelerated. From domestic electronic devices to security units, and heating or lighting system, various connectable devices to the Internet are devised, thus Smart Home is closely and specifically adhered to daily lives. Smart Home is domestically utilized – the most privately linked to a personal lifestyle – and is continuously being advanced, generating positive influences, however, its security is still vulnerable, and the users are exposed to diverse device, network and privacy threats[3]. If the security vulnerabilities of Smart Home, devised for convenience, life quality increase and safety, are not solved, then a huge disaster may be foreseen. As significance of privacy and safety of Smart Home are being highly raised, the thesis would analyze the security threats and suggest a responsive measure. The thesis consists as followings. Chapter 2 illustrates IoT and Smart Home, then observes Smart Home security threat cases. Chapter 3 analyzes Smart Home threats into device, network and privacy aspects. Chapter 4 proposes a responsive measure against the threats, then the chapter 5 draws a conclusion.

Figure 1. Petition of national.



— 청원종료 —

국민의 생명이 위협되는 스마트홈 안전하게 해 주세요

참여인원 : [274명]

카테고리 안전/환경 청원시작 2019-02-19 청원마감 2019-03-21 청원인 twitter - ***

청원내용

오늘 출근해서 아무리 생각해 봐도 어제 '스마트홈 해킹' 관련 언론에서 보도된
TV에 나온 스마트홈 단지가 저희 단지인 것 같다는 불안을 떨쳐버릴 수가 없습니다.

국민청원답변 라이브
잠시 후 시작됩니다

추천순 TOP 5

1. 안녕하세요. 증인 윤지오입니다.
2. "정부아이돌봄서비스 아이돌보미 영유아 폭행 갑···
3. 소방공무원을 국가직으로 전환해주세요
4. 대통령님께서 <세월호참사 특별수사단>설치해···
5. 연합뉴스에 국민혈세로 지급하는 연 300억원의 재···

답변된 청원

- [illegible]
- [illegible]
- 안녕하세요. 증인 윤지오입니다.
- [illegible]
- [illegible]
- [illegible]
- [illegible]

2. Relevant Research

2.1. IOT and smart home

IoT(Internet of Things) is a future Internet, and is an interoperable communication protocol with both physical and virtual identifier[4]. IoT, based on existing wireless communication, is an advanced model over the Internet or the mobile Internet, exchanges data without a human intervention, and processes information. Having no reliance on human control, but exchanging data among things, both Ubiquitous and M2M(Machine to Machine) are similar, however, M2M focuses on communication among things and humans. Therefore, IoT, having the notion of M2M as a basis, has developed into a concept to interoperate with things and all data in both physical and virtual world, by broadening the area into the Internet[4]. Areas of IoT application has expanded from wearable devices, attaching on a body or putting on a watch on the wrist, to home appliances, cooperative system, smart car, smart home and smart city – that is, from micro to macro environment[5].

3 major technologies applied in IoT is sensing, acquiring data from things and surrounding environment, wire or wireless communication and network infrastructure, supporting the connection between things and the Internet, and service interface, converging different technologies to manufacture and process data in accordance with adequacy of each service field and form[3]. <Table 1> is Service case of IoT[6].

Smart Home, also known as Home IoT, refers to product, service and solution which household domestic devices can remotely be monitored, controlled and operated by mobile devices or PC through an Internet interlinks[7]. Smart Home deals with various fields and its boundary has been broadened. Households with Smart Home services integrated home appliances, including TV, air conditioner and refrigerator, energy consumption units, such as water, electricity and cooling or heating, and security devices, - security lock, for example - into a single network, thus its monitoring, control and operation can be performed with no time or spatial restriction[7].

Table 1. Service case of IoT[6].

Field	Service content
Energy	Intellectual integration service of distributed generators to balance adequate consumption and demand, as well as providing data to power distribution company and customers, by constant measurement on new renewable energy, electrical grid, and electricity and energy consumption.
Transportation	Application technology to provide innovative service managing different transportation and their system with better safety and convenience by users.

Manufacturing	Real-time integrated processing system reforming and assembling required data in all-process for higher usefulness and application.
Medical	Establishment of public and personal medical system to improve accessibility of patients and medical teams to medical services via advanced application devices(mobile/smart device, sensor and actuator).
Public	Establishment of real-time information system to offer higher level of public service and data for civil safety.
Customer service	Provision of personal customized application service which can interoperate private life and technologies from purchase to entertainment.
Smart home	Application system relevant to buildings, which their lighting, heating and home appliances can remotely be controlled by smart-phones and mobile devices.
Finance	Intellectual integrates system that is applicable to various finance markets such as banking, insurance, real estate and loan.

1.2. Smart home security threat cases

Smart Home security, utilizing Public network, is respectively more vulnerable to threats than Smart Factory, using Private network. Followings are Smart Home security threat cases.

Figure 2. Smart home service.

1.2.1. Violation of iron and electric kettle case

An iron and an electric kettle made in China with a spy microchip installed were identified in Russia. Once the device is linked to the wireless network, malignant codes and span mails can be disseminated, and private information collected through tapping may be transmitted via the network. The number of the units identified reached over 30 and would be higher considering unidentified ones. If zombie PCs are produced via malignant codes distributed by the units, the PCs can be utilized for large-scale hacking attacks[3][6].

1.2.2. Violation of vulnerability abuse of thingbots

Thingsbots are the Smart TV, refrigerator and device that are linked to the Internet used for phishing and spam mail transmission due to hacking[8]. In 2016, a large-scale DDoS attack was committed to over 1200 US major agencies, including Twitter, Netflix and The New York Times. Thus, the websites had been disabled. The attacker sent the Mirai malignant code through Thingbots, the code infected IoT devices with their initial ID/PW unchanged by acquiring the administrator access[6][8][9].

1.2.3. Violation of monitor camera case

According to BBC in the United Kingdom, an obscene sound was output from a household monitoring camera designed for toddlers in Texas, the United States, and this was a case of vulnerability abuse of FOSCAM product to produce obscene noise. The case was a violation case of abusing firmware and software weaknesses discovered[6].

1.2.4. Violation of home appliance case

Referring to Proofpoint, a US security company, since 2013 to the early 2014, 750 thousands of phishing and spam mail were transmitted via IoT home appliances such as home networking router, smart TV and refrigerator throughout the world. Attackers abused the mailing function installed in IoT home appliances connected to the Internet and sent phishing and malicious mails. In addition, smart TV was hacked and live-broadcasted inside of an entire household through a camera installed in its home appliance. There were other cases, which order number of TV home-shopping has randomly been changed, and collecting and changing significant data such as image, video, sound, credit card number, bank account number and location data – leading to further damages[10].

1.2.5. Privacy infringement case via CCTV

Over 73000 personal CCTVs throughout the world were hacked and broadcasted in real-time. Over 6000 CCTVs hacked were placed in South Korea, which was found to be the second largest in the number of victims in the world. It was, at last, discovered to be an intention of the website operator to emphasize the importance of security, however, the case proved that not only restaurant, café and streets, but also personal privacy may be looked through if one wishes to[6].

2. Smart Home Security Threat

2.1. Device security threat

Attackers disguise unauthorized device into an authorized one, thus can input malignant code into wireless network and counterfeit or falsify data tapped from authorized devices. Smart device with malignant code becomes a zombie device, generating DDoS attack, then other smart devices linked to the same home network with the PC get infected, hence secondary damage occurs. Counterfeiting or falsifying data from authorized device may enable further counterfeiting of device authorization process and outcome, thus inadequate service may be practiced. Furthermore, by tapping data between devices via wireless network, an attacker can capture important data from Smart Home.

2.2. Network security threat

Smart Home, utilizing wireless network, controls home appliances, thus should establish a password to prevent risk of its data being tapped. IP Spoofing is a method to attack system to disguise unauthorized user as an authorized one by pirating the data origin, transferred from internal to external network, threatening Confidentiality of data. The Internet fundamentally is operated based on a client/server structure. User accesses to the central server and received data, the data set is not entirely transferred at once, but by small units segmented, so-called packet. The segregated packets go through several devices till its reception to the user, and the devices may tap and counterfeit the packet content. This is called Man-in-the-Middle attack. Attacker located in-between smart TV and web-server may try unauthorized reading, data counterfeit and falsification attacks by approaching to the data being transmitted.

2.3. Private information-related security threat

As convenience offered by Smart Home, controlling home appliances connected to the wireless Internet, gets enhanced, concerns on privacy violation by hacking and information leakage are growing. As IoT develops, the number of smart devices to collect personal data increased, thus considering the large amount of accumulated private information and its broad application in many directions, growing demand in privacy protection is inevitable[11]. Home appliances for Smart Home collect and store situational data(any human movement inside the housing, room temperature, humidity, lighting brightness, CCTV, gas valve detection, electricity consumption, absence state and list of home appliances) inside households via attached sensors. Likewise, all devices used for Smart Home can be exposed to security threats – personal information leakage and privacy infringement.

3. Responsive Measure against Smart Home Security Threat

3.1. Measure against device vulnerability

Security issues in devices are access by an unauthorized device, data counterfeit and falsification, and personal information leakage. To cope with such device security threats, first, only authorized device must be allowed for an access to Smart Home network. Cross-certification is executed with all devices used for Smart Home, all users using the devices go through a user authentication. Second, prevent any device access with its integrity damaged via integrity check. Integrity of all data transmitted and received between devices are confirmed by applying one-way hash function. Third, by using the intrusion detection technique for Smart Home service, any device attempting an irregular access is forcibly blocked out. Monitoring Smart Home, detection for any device with irregular action is performed. Fourth, a password is set for all devices as a basic step, then the established password is periodically changed. Fifth, all data transferred to the network is encrypted based on a public-key cryptosystem.

3.2. Measure to ensure network security

To ensure security between networks in Smart Home, devices connected to the network should be trustworthy to each other, tapping by a 3rd party should be prevented during their data transmission, and even if they are exposed to tapping attacks, the attacker must not be able to know the tapped contents. To deal with the network security threats, first, for non-repudiation of data transmission-reception among devices, digital signature or electronic envelop methods are used. Second, for integrity of data being transmitted, one-way hash function is applied, and practice symmetric-key algorithm or public-key cryptosystem to preserve the data confidentiality. To safely perform data encryption, different password key is utilized in each session, and any key, considered significant for the encryption, is distributed in advance and stored in devices.

3.3. Measure for private information protection

Measure to protect personal information stored in Smart Home device as followings. First, authority to access to Smart Home devices must be restricted. By employing various user authentication techniques based on IP, ID and biometrics to users attempting an access to devices, only authorized users can access to the devices. Second, all devices connected to Smart Home should utilize a password. Password is the most basic way to protect privacy. The password should periodically be changed, complicatedly structured, thus its stability must be enhanced. Third, personal information stored in devices should be stored in compliance with public-key cryptosystem. If attackers cannot decrypt the acquired private information from devices, it the data becomes useless. Fourth, access history of users to devices should be kept and managed. Storing and managing the history is to identify any access or action by attackers, attempting an illegal access to devices via counterfeiting as users.

4. Conclusion

Due to development of information and communications and commercialization of smart devices, Smart Home technology and service, using IoT, has more rapidly been developed and distributed. Smart Home enables a wide range of devices – from home appliances to security devices, heating and lighting system – be connected to the Internet, thus human life quality has been enhanced. However, Smart Home security technology is still insufficient, hence individuals and households using Smart Home are being exposed to security threats in many aspects, including device, network and privacy infringement. The thesis observed the actual security threat cases, in terms of Smart Home uses, analyzed any probable security threats in Smart Home environment into device, network and private information prevention categories, then suggested their sequent responsive measures.

First, to cope with device security threats, 1. Cross-certification to devices. 2. Blocking any device with damaged integrity. 3. Blocking any irregular access to devices. 4. Set a password. 5. Encryption of all data. are proposed.

Second, to deal with network security threats, 1. Application of digital signature and electronic envelop for non-repudiation of data transmission. 2. Application of one-way has function to protect data integrity and maintain data confidentiality by using encrypted data. 3. Change the key for encryption at every session, and distribution of significant key in advance. are suggested.

Lastly, to protect private information, 1. Restrict authorities to access device. 2. Manage the password. 3. Full encryption of all data stored in devices. 4. Manage and store all device access history. are proposed.

Smart Home, devised for convenience and constantly being advanced over time, has become an important part of daily lives of human beings. In the light of Smart Home security threats, affecting individuals and households, security has become a necessity, not an option. To enjoy Smart Home and its convenience to the full extent, consistent investment and research on the security should be conducted.

5. References

5.1. Journal articles

[7] Lee MY & Park JP. Analysis and Study on Invasion Threat and Security Measures for Smart Home Service in IoT Environment. *The Journal of the Institute of Internet, Broadcasting and Communication*, 16(5), 27-32 (2016).

[8] Um JY. Security Technology for Home IoT / Connected Appliances. *Journal of the Korean Institute of Communication Sciences*, 34(10), 10-16 (2017).

[11] Pyo CS. Technology Trend of Internet of Things. *Journal of Electromagnetic Engineering and Science*, 25(4), 49-58 (2014).

5.2. Thesis degree

[3] Bang SS. A Study on Security Threats and Information Protection in Smart Home IoT Service Environment. KonKuk University, Master’s Thesis (2017).

[4] Jung JW. A Study on the Information Security Factors Affecting of Smart Home IoT Services. Soongsil University, Master’s Thesis (2018).

[6] Park KS. A Study on the Direction of Cyber Infringement Response in Smart Home Environment. AJou University, Master’s Thesis (2019).

[10] Shin DH. An Analysis of Security Vulnerability by Wireless Home Network Environment. Soongsil University, Master’s Thesis (2008).

5.3. Additional references

[1] https://www.boannews.com/ (2015).

[2] https://n.news.naver.com/ (2019).

[5] http://www.epnc.co.kr/ (2019).

[9] https://cafe.naver.com/ (2019).

Author

Lee Jae-young / Semyung University Assistant Processor
B.A. Semyung University
M.A. Semyung University
Ph.D. Chungbuk National University

Research field
- A Study on Improvement of Device Removal Processes from ZigBee Network, Journal of Engineering and Applied Sciences, 13(1) (2016).
- A Study on Utilizing IoT for Preventing Approach Restraining Order Violation, International Journal of Police and Policing, 2(1) (2017).

Major career
- 2012~2016. Semyung University, Assistant Processor in Department of Liberal Education
- 2016~2019. Semyung University, Assistant Processor in School of Information & Communication Systems
- 2019~ present. Semyung University, Assistant Processor in Department of Liberal Education

2019 4(1) 7-13 Submission: 2019/05/10, Peer review: 2019/05/20, Accepted: 2019/05/25, Published: 2019/06/30

International journal of criminal study

Publication state: Japan
ISSN: 2423-8783

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: kojet2@naver.com

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/criminal.2019.4.1.07

A Study on an Autonomous Committee for Countermeasures against School Violence for CRIME Prevention

Kim Hak-bum

Semyung University, Jecheon, Republic of Korea

Abstract

Recently, a growing number of cases of school violence at school sites have become contentious and become legal problems, and the phenomenon is deepening beyond what teachers can solve. In line with these social changes, the Act on the prevention of and countermeasures against violence in schools was enacted in 2004.

However, a number of complementary points are being discussed regarding the formation and operation of an autonomous committee for countermeasures against school violence under the current law. As the autonomous committee, which plays the most direct role as a response to school violence, needs to operate efficiently, the study explored the development direction through the analysis of current statutes and prior studies. The preceding studies presented various conclusions, but in common they suggested a lack of expertise in the formation of autonomous committees. It also said it lacked counseling and other support for the victims.

Based on these problems, the study presented the following improvement directions. The first is the strengthening of the professionalism of the autonomous committee. The results of the preceding studies show that non-professional parent representatives include a majority, weakening their professionalism. Therefore, the need to expand the participation of external members in order to secure expertise is recognized.

The second is the expansion of exclusion and recusal and the broad-basedization of the autonomous committee. It will be necessary to expand the system of exclusion and recusal in conjunction with the strengthening of professionalism. In order to eventually resolve this issue, the broad-basedization of the autonomous committee should also be considered.

The third, parents' education closest to students should be required so that education can be conducted within the home. However, since such parents' education cannot be enforced under the current law, there is a need to establish a rule to supplement it.

Finally, it is necessary to bring the victims' support to reality. In order to make the support of the victims a reality, it may be possible to activate the counseling function, including professional social workers, in the form of autonomous committees. Another is the use of the expertise of the Korea Crime Victim support Center.

This improvement will serve as a positive aspect of the autonomous committee's activities to reduce school violence.

[Keywords] ***Criminal, School Violence, Autonomous Committee, Crime Prevention, Strengthening of the Professionalism***

1. Introduction

At present, our society is becoming longer, more violent and less aged, with sexual violence occurring between teenagers, bullying by friends, bullying by school violence, which leads to serious illness or death. Moreover, with the development of smartphones and the Internet, the forms of school violence are becoming diverse[1].

Recently, a growing number of cases of school violence at school sites have become contentious and become legal problems, and the phenomenon is deepening beyond what teachers can solve. In line with these social changes, the Act on the Prevention of and Countermeasures against Violence in Schools(hereinafter referred to as School Violation Prevention Act) was enacted in 2004[2].

With the enactment of the law, countermeasures for efficient and open handling of school violation problems without concealing them, but school violation still exists in various forms[1].

Many contents of the school violence prevention law have been revised and supplemented through 22 revisions, including the revision of other laws and the revision of the school violence prevention law, until the revision in 2017. The need for such a revision shows the importance of understanding and preventing more essential school violence through the law[3].

However, a number of complementary points are being discussed regarding the formation and operation of an autonomous committee for countermeasures against school violence(hereinafter referred to as "autonomous committee") under the current law. As the autonomous committee, which plays the most direct role as a response to school violence, needs to operate efficiently, the study will explore the development direction through the analysis of current statutes and prior studies.

2. Analysis of Previous Studies

Previous studies generally share the need for an autonomous committee. However, there are features that suggest a variety of improvement measures.

First, Kim LJ(2013) proposed a revision to the composition of the autonomous committee in his study on prevention of school violence. She said it would be desirable to use the autonomous committee as a kind of advisory body consisting of parents and some experts. It also suggested giving much power to elected superintendent of offices of education. It also said that because there is a lack of professional counseling personnel for school violence and limited protection measures, the government should seek ways to strengthen support for the victims[1].

And Chang MH(2014) conducted an analysis of elementary school teachers' perception of the operation of the autonomous committee. The study first suggested that teachers should be required to provide education on the operational regulations of the autonomous committee. She suggested for the second time that there was a problem with the rule that requires a majority of the autonomous committee members to be parents, and finally reported a lack of consultation bodies and professional counselors to protect the victims[2].

Lee CB(2015) studies surveyed school resource officers about their perception towards the function of the autonomous committee, its member, and the response of the principal to school violence.

The results indicated that the officers thought the autonomous committee did not very well for the function of protecting the victim’s rights. In addition, he believed that the participation of parents needs to be limited in the membership, and more experts should be included in the membership of the autonomous committee. He also thought the principals should be tough in dealing with school violence. The discussion includes ideas about improving professionalism of the membership and making changes on the related regulations[4].

In the study by Jung HG(2017), the following points were presented.

First, it needs to establish regulations of system and operation for improvement of dedicated organizations and to strengthen the support and counseling activities for healing students to protect the victims.

Second, it is necessary to improve the dispute conciliation system to transfer the tasks related to the dispute mediation and to ensure professionalism of the autonomous committee as well as clearly define the functions and roles of the autonomous committee.

Third, in the case of victims' protection and guidance and education for aggressors rather than punishment, the dedicated organization must handle it without opening the autonomous committee if it is judged that there is no problem as a result of the violence or damage[3].

And Han JK(2018) analyzed the procedures for handling school violence in order to prevent school violence. The analysis results are as follows:

First, in case of Non-serious violence school violence, it is necessary to give an opportunity to terminate the matter through the period of conflict adjustment between stakeholders at the stage of the Exclusive Units for School Violence, which is the stage before the autonomous committee.

Second, in order to ensure the fairness and professionalism of the school violence handling procedure, the current regulation, which consists of a majority of the members of the autonomous committee, should be revised. In addition, she proposes a plan to establish the autonomous committee at the Education Support Office instead of installing it at each school. This will enable school teachers to focus on education, and the committee will be able to maintain a consistent process based on uniform standards[5].

There are also studies that have been approached in terms of restorative justice. Yun TH(2017) argued the present efforts cannot be free from some negative evaluation that the measures to prevent school bullying taken so far by the government seem to be too formal and slipshod to take effect. He also stressed that both perpetrators and victims, through their own self-reflection efforts, should establish a system to safely return to society, forming a new paradigm in the field of general criminal justice[6].

In Lee HJ(2017)' study, the procedure of school violence prevention, the detailed standard and the autonomous committee were examined, and the following improvement measures and legislative examples were presented based on the problems.

She argued that the autonomous committee should be fair and professional, however there was a problem that parental committee accounts for a majority, and it is difficult to appoint specialists at the unit school. Therefore, she insisted that the committee should be established by the Education Support Agency to secure fairness and professionalism and to reduce the burden on the unit school[7].

The above preceding studies presented various conclusions, but in common they suggested a lack of expertise in the formation of autonomous committees. It also said it lacked counseling and other support for the victims. Based on this awareness of the problem, I am looking at the current statutes and am trying to find ways to improve them.

3. The Act on the Prevention of and Countermeasures against Violence in Schools

3.1. Purpose and definition

The purpose of the School Violation Prevention Act is to protect the human rights of students and raise students as healthy members of society through the protection of victim students, the guidance and education of aggressor students, and mediation between victim students and aggressor students, by providing for matters necessary for the prevention of and countermeasures against violence in schools[8].

The school violence means any action committed against students inside or outside of school premises resulting in a physical or mental injury, or damage to property through a battery, assault, confinement, threat, kidnapping, abduction, defamation, insult, extortion, coercion, forced errand, sexual violence, bullying, or cyber-bullying, or with obscene or violent information via an information and communications network[8].

3.2. Establishment and functions of autonomous committees

Each school shall establish an autonomous committee for countermeasures against school violence to deliberate on matters related to the prevention of and countermeasures against school violence: provided, that at least two schools may establish a joint autonomous committee after filing a report with the superintendent of the relevant office of education on any ground prescribed by Presidential Decree. Ground prescribed by Presidential Decree means where the victim student and the aggressor student in a school violence case are enrolled in different schools[9].

Each autonomous committee shall deliberate on the following matters for the prevention of and countermeasures against school violence.

- Establishing a school system to prevent school violence and to develop countermeasures against school violence;

- Protecting victim students;

- Guiding and punishing aggressor students;

- Mediating disputes between victim students and aggressor students;

- Other matters prescribed by Presidential Decree. Other matters prescribed by Presidential Decree means measures suggested by the responsible teacher or the representative of the student council regarding prevention of and countermeasures against school violence.

Each autonomous committee may request the head of the relevant school and the chief of the competent police station to provide data concerning school violence that has occurred in the relevant area.

3.3. Composition and operation of autonomous committees

An autonomous committee shall be comprised of at least five to up to ten members, including one chairperson; a majority of the total members shall be commissioned from among representatives of parents directly elected at a parents conference, as prescribed by Presidential Decree: Provided, That if it is impracticable to elect representatives of parents at a parents conference due to any extenuating circumstance, representatives of parents may be elected at a conference consisting of representatives of every class.

Members of an autonomous committee shall be appointed or commissioned by the head of the relevant school, from among the following persons:

- The deputy head of the relevant school;

- Teachers with work experience in student guidance and counseling, among teachers of the relevant school;

- Representatives of parents elected in accordance with Article 13(1) of the Act;

- Judges, prosecutors, and attorneys-at-law;

- Police officers of the police station having jurisdiction over the relevant school;

- Licensed physicians;

- Other persons who have abundant knowledge and experience in prevention of school violence and protection of juveniles[9].

Meetings of an autonomous committee shall be held at least once a quarter, and the chairperson of an autonomous committee shall call a meeting under any of the following circumstances:

- Where requested by at least 1/4 of the members registered with the autonomous committee;

- Where requested by the head of a school;

- Where requested by a victim student or his/her parents;

- Where the occurrence of school violence is notified or reported to the committee;

- Where the fact that an aggressor student has threatened or retaliated against a victim student is notified or reported to the committee;

- Other cases deemed necessary by the chairperson.

Each autonomous committee shall prepare and keep meeting minutes stating the date, place, members present, discussion and matters for resolution of the meeting.

3.4. Composition and operation of autonomous committees

If an autonomous committee deems it necessary for the protection of a victim student, it may request the head of the relevant school to take any of the following measures(or several concurrent measures) for the victim student: Provided, That the head of a school may take any measure under subparagraph 1, 2, or 6 before the autonomous committee requests such measure, if he/she deems that an urgent measure is required for the protection of a victim student or receives a request for urgent protection from a victim student:

1)Psychological counseling or advice by experts from within and outside school;

2)Temporary protection;

3)Treatment and recuperation for treat ment;

4)Change of class;

5)Other measures necessary for the pro tection of a victim student.

3.5. Mediation of disputes

An autonomous committee may mediate a dispute arising in connection with school violence. The duration of mediation of a dispute shall not exceed one month.

The mediation of a dispute arising in connection with school violence shall include the following matters:

- Mediation for settlement of damages between the victim student and the aggressor student or his/her guardian;

- Other matters the autonomous committee deems necessary.

If an autonomous committee deems it necessary for the mediation of a dispute, it may investigate into the facts relevant to a case of school violence with the cooperation of related authorities. Also, if an autonomous committee intends to mediate a dispute, it shall notify its intention to the victim student, the aggressor student and his/her guardian.

4. The Direction of Improvement of the Autonomous Committee

Based on the above preceding studies and current laws, I intend to present the development direction of the operation of the autonomous committee.

4.1. The strengthening of the professionalism of the autonomous committee

The results of the preceding studies show that non-professional parent representatives include a majority, weakening their professionalism[1][10][11]. Therefore, the need to expand the participation of external members in order to secure expertise is recognized. In order to make participation of outside experts a reality, the committee should be formed with experts in criminal justice, including professors in relevant departments. To this end, the government should revise the rules for the composition of the autonomous committees, which comprise a majority of the committee members as parents. Specifically, more than two-thirds of the experts will have to be organized. This should include the person with the relevant degree.

4.2. Expansion of exclusion and recusal and the broad-basedization of the autonomous committee

It will be necessary to expand the system of exclusion and recusal in conjunction with the strengthening of professionalism. Many parents in the same area are linked to school ties and delays. This is because it is difficult to expect fairness from the committee members who are highly relevant to the perpetrators and the victims even if they are not linked by blood.

In order to eventually resolve this issue, the broad-basedization of the autonomous committee should also be considered. It can be expected that there will be less likelihood of recusal among members of the broadened autonomous committee. It would be appropriate to open it as a unit of the Educational Support Agency.

4.3. The strengthening of parental education

The beginning of students' violence and flight often comes from families, not from their school days. And with current education taking place in a short period of time, it is hard to expect the effect of reducing school violence. Therefore, parents' education closest to students should be required so that education can be conducted within the home. However, since such parents' education cannot be enforced under the current law, there is a need to establish a rule to supplement it. The effectiveness of the system should be ensured by introducing the contents of the crime not prosecuted against objection[5] as claimed in some studies or by including parental education condition measures.

4.4. The Realization of victims' support

In order to make the support of the victims a reality, it may be possible to activate the counseling function, including professional social workers, in the form of an autonomous committees[12].

Another is the use of the expertise of the Korea Crime Victim support Center. Using the Korea Crime Victim support Center, which is set up by region, could achieve the realization of support for victims. These points should be further defined in the law.

5. Conclusion

The reality of Korean education is that despite various efforts being made on the issue of school violence, the seriousness of it has not decreased. To reduce school violence, the School Violation Prevention Act was enacted in 2004 in line with these social changes.

Although the autonomous committee under the law is in operation, various operational problems are being discussed.

The preceding studies presented various conclusions, but in common they suggested a lack of expertise in the formation of autonomous committees. It also said it lacked counseling and other support for the victims.

Based on these problems, the study presented the following improvement directions.

The first is the strengthening of the professionalism of the autonomous committee. The results of the preceding studies show that non-professional parent representatives include a majority, weakening their professionalism. Therefore, the need to expand the participation of external members in order to secure expertise is recognized.

The second is the expansion of exclusion and recusal and the broad-basedization of the autonomous committee. It will be necessary to expand the system of exclusion and recusal in conjunction with the strengthening of professionalism. In order to eventually resolve this issue, the broad-basedization of the autonomous committee should also be considered.

The third, parents' education closest to students should be required so that education can be conducted within the home. However, since such parents' education cannot be enforced under the current law, there is a need to establish a rule to supplement it.

Finally, it is necessary to bring the victims' support to reality. In order to make the support of the victims a reality, it may be possible to activate the counseling function, including professional social workers, in the form of an autonomous committee. Another is the use of the expertise of the Korea Crime Victim support Center.

Through the improvement of school violence procedures, such as the above, the current school violence prevention law will be able to secure practical validity and procedural equity, and will positively affect the recovery of the victims' damages.

6. References

6.1. Journal articles

[4] Lee CB. School Resource Officers' Perception toward the Function and Role of the Local Board against School Violence. *Korean Security Science Review*, 44, 117-137 (2015).

[5] Han JK. A Study on the School Violence Handling Procedure in Act on the Prevention of and Countermeasures against Violence In Schools. *Journal of Public Society*, 8(1), 131-161 (2018).

[6] Yun TH. A Study on the Measures to Prevent and Cope with School Violence through Restorative Justice. *Korean Juvenile Protection Review*, 30(2), 89-122 (2017).

[7] Lee HJ. The Problems and Improvements of the Procedures for School Violence. *Studies on American Constitution*, 28(3), 215-251 (2017).

[10] Han YK & Lee JY & Park JH. An Analysis of School Violence Issues in Schools. *Journal of Educational Studies*, 44(4), 73-97 (2013).

[11] Lee SH. Revised Contents and Improvements of the Act on the Prevention and Countermeasures against Violence in Schools. *Korean Criminological Review*, 23(2), 157-190 (2012).

6.2. Thesis degree

[1] Kim LJ. Study on Law Related to Prevention of School Violation. Dongeui University, Doctoral Thesis (2013).

[2] Chang MH. An Analysis of Elementary School Teachers' Perception on the Local Board against School Violence. Gyeongin National University of Education, Master's Thesis (2014).

[3] Jung HG. A Legal Study on the Problems and Improvement of School Violence Prevention System. Donga University, Doctoral Thesis (2017).

[12] Kim JH. Comparison on the Role of the School Social Worker and the Local Board against School Violence. Korea International Culture University, Master's Thesis (2007).

6.3. Additional references

[8] Act on the Prevention of and Countermeasures against Violence in Schools.

[9] Enforcement Decree of the Act on the Prevention of and Countermeasures against Violence in Schools.

Author
Kim Hak-bum/ Semyung University Associate Professor
B.A. Hankuk University of Foreign Studies
M.A. Dongkuk University
Ph.D. Dongkuk University

Research field
- A Study on the Music Therapy Approach for the Internet Addiction Crime, Korean Association of Addiction Crime Review, 2(2), (2012).
- A Study on Regulation Plan of Games, Korean Association of Addiction Crime Review, 7(1), (2017).

Major career
- 2010~present. Semyung University, Professor
- 2011~present. Korea Association of Addiction Crime, Director

2019 4(1) 14-19

Submission: 2019/05/10, Peer review: 2019/05/20, Accepted: 2019/05/25, Published: 2019/06/30

International journal of criminal study

Publication state: Japan
ISSN: 2423-8783

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: klaces7@naver.com

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/criminal.2019.4.1.14

Research on Causes and Countermeasures of Juvenile SNS CYBER Verbal Abuse

Kwon Hwa-suk

Semyung University, Jecheon, Republic of Korea

Abstract

Teenage SNS cyber verbal abuse affect not only mental but also physical features of daily lives, bringing experiences of rage, demoralization and senses of outrage and humiliation. Juvenile SNS cyber verbal abuse may induce mental. physical in daily lives, as well as in school lives, critically harming the personality of a victim.

The thesis aims at contemplating causes and countermeasures of cyber verbal abuse in juvenile SNS language uses in such a mobility society.

Thus, observing the juvenile SNS usage state, the notion and types of cyber verbal abuse is proposed. Further, based on the context, causes and countermeasures of the juvenile SNS cyber verbal abuse are considered.

The thesis suggests the causes of juvenile SNS cyber verbal abuse in terms of SNS media feature, internal characteristic of the juvenile and educational aspect.

In addition, a campaign to eliminate school verbal abuse by the police, mentoring curriculum associated with each social institution and character education are revised in a societal manner, and langage education to prevent juvenile SNS verbal abuse in an educational manner as countermeasures against the juvenile SNS cyber verbal abuse.

Guiding an appropriate direction for juvenile SNS language use in the mobility society, the thesis would contribute to discover a meaning in educational and sociocultural aspects. Moreover, the thesis would contribute to counteracting against juvenile SNS verbal abuse and to an adequate guidance of juvenile language uses.

[Keywords] ***Mobile, SNS, Cyber Verbal Abuse, Law Enforcement, Crime Prevention***

1. Introduction

Verbal abuse refers to communication inducing severe humiliation either by an individual or a community[1], and to linguistic expression to harm and assault identity of others, committing intentional insult, contempt, critics, belittlement, sarcasm, mockery, condemnation, threat, oppression and assault.

Verbal abuse, in accordance with ways to harm identities of others, condemns appearance, character and background, and is a malicious behavior expecting others to go amiss, a harassing behavior to make others raged or threatening behaviors taking an advantage of weaknesses and flaws of others[2].

Most victims of verbal abuse counteract passively, assuming their own fault as the causes or falling into hesitation due to fear and anxiety, rather than actively[3], and result in experiencing mental damage without any proper counteract against the abuses. Being consistently exposed to verbal abuse in conflicting situations, the assailant depicts oneself negative and hostile, being tied to such emotions, hence relies on verbal assaults, particularly focusing on self-concept of others, rather than objective logic - that is, a negative result[4]. Emotional·verbal abuses may cause various psychological·mental damages, and even bring serious issues if the abuses are chronically neglected[5].

Likewise, verbal abuse induces serious damage to identity of others, thus influence not only psychological but also physical aspects of daily lives, bringing experiences of rage, demoralization and senses of outrage and humiliation.

Owing to technological development and commercialization of smartphones, people use SNS. Utilization of SNS helps formation of human interaction through its online platforms, enabling establishment of private networks. As use of mobile increases, communication with diverse people via SNS(Social Network Service), but without spatial and time constraints, has been enabled. Communication vis mobile messengers is committed as Mediated Communication, a character of SNS communication. At this stage, SNS cyber verbal abuse is often easily generated.

The research aims at contemplating causes and countermeasures of juvenile SNS language uses in mobility society. First, juvenile SNS usage state would be observed and the notion and type of cyber verbal abuse would be proposed. Then, based on the context, causes and countermeasures of juvenile SNS cyber verbal abuses would be considered.

2. Juvenile SNS Language Use State

SNS(Social Network Service), an online service enabling network establishment among people with shared activities and particular interests, has emerged as a sociological and academic hot potato, recently, - for example, Facebook and Twitter. SNS with functions of disclosure of personal information, network establishment and its disclosure, posting opinions and information, and mobile support, has its distinctive characteristics, and their each aspect obtains attention from different perspectives. SNS is placed at the center of controversies due to its consequences and issues. SNS serves functions to generate and spread social issues, to share experiences via expansion of human network and cultivation of quantitative·qualitative performance by collective power, hence is superior over other media. In a situation, which 100.0% of Korean juveniles are using the Internet, juvenile SNS addiction will significantly be discussed. According to the data from the National Statistical Office[6] and the Ministry of Gender Equality and Family[7], 77.2% of 10-19 juvenile was in over-reliance on smartphone and used SNS. In particular, middle and high school students utilized SNS at a high ratio. Furthermore, juvenile with over 200 acquaintances conncected through SNS was 21.6%, and their purposes to use SNS were seeking for information and pleasure, and friendship. As SNS performs interaction with others and allows self-expression simultaneously, thus its relationship function is clearly distinct. Such a function is closely linked to the development stage of the juvenile who value peer relationship[8].

It is notable that the linguistic life of the juvenile is mainly held in SNS. SNS is a private space, but is accessible by anyone. Within the space, the juvenile presents their private characteristics, communicate with others and diverse linguistic cultures. Such a SNS feature interlocks with dynamic and progressiveness of the juvenile, hence their writing and images are disclosed to the society and affect on daily lives of their own and others.

3. Notion and Types of Cyber Verbal Abusing

Cyber verbal abusing refers to insulting, slandering, or spreading false information to others via online bulletin boards, chatrooms, email, and others. This kind of action is also called as ‘Flaming’. Flaming is defined in various ways, but its definition is described as constantly discussing in an extreme, mocking way, and this is typically accompanied with insults, personal attack alongside expressing rude and extreme hostility[9].

Cyber verbal abusing is being considered as a less-severe issue since this issue is included in the same context with minor issues like encountering explicit content and other inappropriate activities instead of hacking virus spreading, personal information hacking spam email spreading, cyber gambling and other major cyber-crimes[10]. However, this notion only makes sense to the verbal abusing part.

Cyber-crimes are divided into multiple factors, and typical cyber-crimes like hacking virus spreading, personal email hacking spam email spreading, cyber gambling, cyber theft, piracy, cyber sexual assault, cyber slandering, cyber verbal abusing are also included. In a bigger array, crimes can be divided into new types of terrorism-related hacking crime, property asset fraud and burglary in cyberspace, old-fashioned cyber assault and related violent crimes, and sexual assault along with slandering.

In the bigger array context, verbal abusing can be defined as a behavior related to violence crime, and has three different kind of variations. The first one is simple insult, second is spreading rumors or false information, and the last one is committing sexual harassment via posting obscene conversations or sexually inappropriate posts. In other words, according to the first variation, the term ‘cyber verbal abusing’ only includes the hostile concept the insults and inappropriate language connotes. However, if cyber verbal abusing is defined in a larger array, this can be interpreted as cyber assault, which means that the second and third variation can also be discussed in the same criterion. Therefore, cyber verbal abusing turned out to be a severe act of crime which cannot be considered as a minor problematic behavior if we interpret this kind of behavior with a larger array rather than a smaller array.

4. Causes and Countermeasures of Juvenile SNS Cyber Verbal Abuse

This chapter would monitor causes and countermeasures of juvenile SNS cyber verbal abuses.

4.1. Causation of juvenile cyber verbal abuse

Juvenile SNS cyber verbal abuse tends to occur due to several reasons. Causation of juvenile SNS cyber verbal abuses can be categorized into undeniable nature of the social network service, environmental reasons, and interpersonal reasons, and lastly educational reason. These reasons will be examined throughout following clause.

4.1.1. Natural trait of SNS media

1)Anonymity and Disinhibition

Within the subject of cyber verbal abuse, one of the most frequently mentioned cause of the problem is cyber anonymity. Anonymity of cyberspace not only brings down self-consciousness but also interferes with self-regulation causing disinhibition.

2)Lack of Control within Cyberspace and Insufficient Punishment

Once the information gets sent out to the unspecified individuals, according to the principle anyone can have access to the information has been released. Due to the open nature it is hard to regulate cyber verbal abuse. On top of that due to anonymity of the cyberspace it is not only hard to pinpoint the suspect. Since cyber verbal abuses do not have direct correlated with physical abuses therefore the awareness of the abuse is comparably lower than other crimes. Since cyber verbal abuses are considerably small compared to other matters, police perform passively towards the matter. Also, if the victim fails to gather up the evidence it is hard to advance forward with the case. Moreover, in reality due to the lack of investigators it is hard to expose the criminal.

3)Relation between Internet Usage Time and Possibility of Being Exposed to Potential Violence

The fact that accidental cyber verbal abuse happens is a proof that those who spend majority of their time online and internet addicts have higher expose rate to violence and exposure has direct correlation with cybercrime rate.

4.1.2. Socio-environmental reasons

1)Manifest in Group Identity

Although cyberspace is created to share different opinions the truth is that it attracts those with similar perspectives and mindset and excludes those with different thoughts.

Cyber verbal abuse happens due to the friction caused during the elimination process within the cyberspace.

2)Cyber Cultural Environment

Cultural aspect of internet is one of the causations of cyber verbal abuse. Cultural norms within the cyberspace has crucial effect on users. If Juveniles, spend most of their time online. They will be influenced by all the criticisms and comments from cyberspace. Which will eventually lead to potential cyber verbal abuse.

3)Individual Attitudes and Lack of Ethical Sense

Increased usage of internet will slowly reform not only one's attitude towards cyber verbal abuse but also increase their chance in partaking in cyber verbal abuse. Since cyberspace has a notion of artificial environment, meditated society, lack of realization of reality, it decreases user's understanding of severity of cyber verbal abuse. Therefore, Individual attitudes and lack of ethical sense can be considered one of the main causes of cyber verbal abuse.

4.1.3. Cyber verbal abuse caused by personal characteristics of juvenile

Juvenile's personal characteristics and has close relationship with cyber verbal abuse.

1)Fun and curiosity

Cyber verbal abuses are often caused due to simple curiosity and for lack of fun. Juvenile tend to view cyberspace as a play area. Therefore instead of using it for web searching and for work, they tend to use the internet for gaming purposes. However, once they get addicted to the environment where there is no restriction juveniles will act based upon their emotions. Also, this will lead them to commit a cyber-crime without them knowing. Existing researches reviled that some hackers tend to hack solely base on curiosity without any guilt cyber sexual harassments are caused in order to entertain certain users.

2)To boast Oneself

Those who frequently go thought cyber verbal abuse often lack in self-confidence, lack in achievement, therefore they suffering from inferiority disorder. The concept of boasting undermines the idea of exposing their ego to the public in order to relieve their inferiority.

3)Release of Daily Stress

Cyber verbal abuse can be seen as a reaction created while exposing and releasing stress. There are lack of sense of reality in cyberspace and it is meditated society users us cyber verbal abuse as a scapegoat to release their stress and tension. Therefore, cyber verbal abuse can be seen as a way to release juveniles stress and tension.

4)Lack of Self-Control

Out of all the categories accidental and impulsive reasons take up the majority of the reason for the cyber verbal abuse. Regarding the data ability to control oneself is directly correlated to cyber verbal abuse[11].

4.1.4. Cause derived from educational aspects

The cause of juvenile SNS cyber verbal abusing can also be approached in the educational aspect as well.

First of all, home education and parent-related aspects are related to educational aspect. The modern society can be described to be in a severe state of lacking home education due to parents' aspirational value, change of family structure, and increase in number of dual-income families. Due to these changes, if juveniles do not receive efficient amount of home education from their parents along with lacking proper household environment, then these juveniles have potential to expose their extremely unstable mentality, desire via SNS.

The linguistic environment of all families inflict substantial influence to children and juveniles' development. Inappropriate language environment within families can act as a crucial cause to juvenile delinquency and violent behavior, and especially among linguistic environment within the family, if insults were involved during parent-child communication, these experiences can negatively affect juveniles and cause them to commit cyber verbal abusing. On the other hand, juveniles' experience of being insulted by their parents can be the major cause of causing juvenile SNS cyber verbal abusing.

Besides this, parental monitoring and juvenile SNS cyber verbal abusing is strongly connected. According to C. Kim and K. Rim[12], one of the major causes of negative factors which affect juvenile deviation is lack of parental monitoring and lack of communication. Like this, parent-related aspects and home education is strongly connected to juveniles' problematic behaviors.

Also, lack of linguistic education at school along with home education and family-related aspects can also be a cause of calling juvenile SNS cyber verbal abusing.

4.2. Solutions for counteracting to juvenile SNS cyber verbal abusing

This clause will attempt to propose the solution for counteracting to juvenile SNS cyber verbal abusing by approaching this issue through an educational aspect and a social aspect.

4.2.1. Solutions when approaching issue via educational aspect

In order to counteract to juvenile SNS cyber verbal abusing, home education must be properly conducted by parents to juveniles. Parents must conduct home education along with setting an example to juveniles with firm values so that juveniles can develop the emotion of caring and respect.

Along with home education, education regarding proper language must be conducted at school as well based on home education and practical education. For this, there is the need to seek solutions for developing teaching programs targeting juveniles to conduct proper language and cultivate humanistic knowledge. Furthermore, debate sessions for juveniles' self-reflection of their rhetoric is required so that they can fix their mistakes and apply their new attitude into action. Along with these requirements mentioned above, schools have to conduct language and characteristics education in a more systematic method and endorse juveniles to have a more considerate and cooperative attitude.

4.2.2. Solutions when approaching issue via social aspect

In the social aspect, juvenile SNS cyber verbal abusing must be countered with a full collaboration between social organizations along with related activities. Also, cyber ethnics education sessions need to be conducted in collaboration with the government, social organizations, media organizations, and more so on.

For example, the police and related law enforcement agencies need to conduct guidance campaigns for exterminating school verbal violence to multi-cultural family children in collaboration with schools and other related social organizations in a regular basis. Along with collaboration programs, there is the need for juveniles to be warned about juvenile SNS cyber verbal abusing and the legal punishment for related acts. To continue, there are some speculations that there is also the need for social organizations over all fields to collaborate and create programs like proper language sessions so that juveniles can realize the importance of proper conversation themselves and indicate the problems and dangers of cyber verbal abusing.

Besides this, student-to-student or student-to-social organization mentoring sessions for preventing SNS cyber verbal abusing can also be a meaningful solution. Also, schools and social organizations regardless of their field affiliation must collaborate and initiate a basic and regular personality education on a society level.

5. Conclusion

To conclude, this research has classified the cause of juvenile cyber verbal abusing into cause derived from the characteristic of SNS, sociological cause, juvenile's internal characteristic-related cause, and educational cause. Also, this research also scoped on solutions to juvenile SNS cyber verbal abusing in educational and social aspects.

Juvenile SNS cyber verbal abusing inflicts a critical damage to the victim's personality, and this can affect the not only the victim's school life, but also incur psychological and physical problems.

Hereupon, there are expectations for this research to be able to contribute in providing guidance to juvenile's appropriate language culture, and counteracting to juvenile SNS cyber verbal abusing.

6. References

6.1. Journal articles

[1] Anderson LN & Clarke JT. De-escalating Verbal Aggression in Primary Care Settings. *The Nurse Practitioner*, 21(10), 95-107 (1996).

[2] Infante DA & Wigley CJ. Verbal Aggressiveness: An Interpersonal Model and Measure. *Communications Monographs*, 53(1), 61-69 (1986).

[3] Sofield L & Salmond SW. Workplace Violence: A Focus on Verbal Abuse and Intent to Leave the Organization. *Orthopaedic Nursing*, 22(4), 274-283 (2003).

[4] Martin M & Anderson C. Argumentativeness and Verbal Aggressiveness. *Journal of Social Behavior and Personality*, 11(3), 547-554 (1996).

[6] Engel F & Marsh S. Helping the Employee Victim of Violence in Hospitals. *Psychiatric Services*, 37(2), 159-162 (1986).

[9] Lee CS. A Study for Flaming in Virtual Community. *Korea Marketing Review*, 18(1), 3-30 (2003).

[10] Cheon JW. A Study on the Characteristics of Youth Deviance in Cyberspace. *Korean Journal of Youth Studies*, 7(2), 97-116 (2000).

[11] Kim KS & Kim JH. A Study on Adolescent`s Level of Internet Addiction by Their Perceived Relationships with Parents. *Korean Journal of Human Ecology*, 6(1), 15-25 (2003).

[12] Kim C & Rim K. Causes of School Violence and Solutions. *Law Research*, 38, 173-198 (2010).

6.2. Thesis degree

[5] Lee OH. The Effects of Psychological Violence by Husbands on the Depression and Psychological Well-being of Wives: Mediating Effect of Dysfunctional Thoughts. Daegu University, Doctoral Thesis (2011).

[8] Kang JH. The Effects of Social Anxiety and Self-presentational Motivation on SNS Addiction Proneness of Male and Female Middle School Students. Myongji University, Master's Thesis (2014).

6.3. Additional references

[6] http://kostat.go.kr/ (2017).

[7] http://www.mogef.go.kr/ (2017).

Author

Kwon Hwa-suk / Semyung University Professor
B.A. Kyungpook National University
M.A. Hankuk University of Foreign Studies
Ph.D. Hankuk University of Foreign Studies

Research field
- A Study of Measures to Teach Korean History Based on Content-based Teaching Method for Academic-purpose Korean Language Learners, Korean Language & Literature, 102 (2017).
- A Study on Reasons of School Maladjustment of Multicultural Background Learners and Responding Measures, International Journal of Police and Policing, 2(2), 26-31 (2017).

Major career
- 2013~present. Semyung University, Professor
- 2013~present. The Korean Language and Culture Education Society, Editing Director